



System i
Redes
Correo electrónico

Versión 6 Release 1





System i
Redes
Correo electrónico

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en: "Avisos", en la página 57.

Esta edición atañe a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761-SS1) y a todos los releases subsiguientes hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni tampoco se ejecuta en los modelos CISC.

© Copyright International Business Machines Corporation 1998, 2008. Reservados todos los derechos.

Contenido

Correo electrónico	1	
Novedades de la V6R1	1	
Archivo PDF del tema Correo electrónico.	2	
Conceptos relacionados con el correo electrónico	2	
Protocolo simple de transferencia de correo en i5/OS.	3	
Protocolo de oficina postal (POP) en i5/OS	4	
Escenario: Correo electrónico	5	
Escenario: enviar y recibir correo electrónico localmente	5	
Escenario: configurar la API		
QtmsCreateSendEmail para que utilice S/MIME	7	
Planificar el correo electrónico	10	
Controlar el acceso al correo electrónico	11	
Controlar el acceso del protocolo simple de transferencia de correo (SMTP)	11	
Controlar el acceso del protocolo de oficina postal (POP)	12	
Impedir el acceso al correo electrónico	13	
Impedir el acceso del protocolo simple de transferencia de correo (SMTP)	13	
Impedir que se inicie el protocolo simple de transferencia de correo (SMTP) cuando se inicia TCP/IP.	13	
Impedir el acceso a los puertos del protocolo simple de transferencia de correo (SMTP)	13	
Retener colas de servicios de distribución de arquitectura de sistemas en red (SNADS)	14	
Impedir el acceso del protocolo de oficina postal (POP)	14	
Impedir que se inicie el protocolo de oficina postal (POP) cuando se inicia TCP/IP.	14	
Impedir el acceso a los puertos del protocolo de oficina postal (POP)	14	
Configurar el correo electrónico	15	
Acceder a servidores de correo electrónico con System i Navigator	15	
Configurar TCP/IP para correo electrónico	15	
Configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) para correo electrónico	16	
Configurar el servidor de protocolo simple de transferencia de correo (SMTP)	17	
Habilitar SSL entre el servidor y el cliente SMTP en el sistema del destinatario	17	
Habilitar SSL entre el servidor y el cliente SMTP en el sistema del remitente	18	
Instalar el certificado de la entidad emisora de certificados (CA) del receptor en el sistema del remitente.	19	
Configurar el servidor de protocolo de oficina postal (POP)	19	
Asociar un certificado al servidor de protocolo de oficina postal (POP)	20	
Inscribir usuarios de correo electrónico	20	
Iniciar y detener los servidores de correo electrónico.	21	
Iniciar los servidores de correo electrónico	22	
Detener los servidores de correo electrónico	22	
Configurar un perfil de conexión de correo por acceso telefónico.	22	
Asistente para configurar la conexión por línea telefónica de ISP.	23	
Planificar trabajos de correo electrónico por lotes de ISP	24	
Configurar el servidor SMTP para recuperar correo por acceso telefónico	24	
Soporte para múltiples dominios	25	
Proteger el correo electrónico	25	
Enviar correo electrónico a través de un direccionador o un cortafuegos	26	
Prerrequisitos para un direccionador de correo electrónico.	26	
Autenticar correo electrónico local y para retransmitir	27	
Rastrear el remitente de correo electrónico	27	
Restringir la retransmisión de mensajes	28	
Aceptar mensajes de retransmisión de los clientes de protocolo de oficina postal (POP)	29	
Utilizar conjuntamente las funciones de restricción de retransmisión y de restricción de conexión	30	
Restringir conexiones	31	
Filtrar el correo electrónico para impedir la proliferación de virus	31	
Enviar y recibir correo electrónico	32	
Configurar clientes de correo electrónico de protocolo de oficina postal (POP)	32	
JavaMail	33	
Enviar archivos en spool como archivos PDF	34	
Utilizar el protocolo ligero de acceso a directorio (LDAP) para las direcciones	34	
Enviar correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)	35	
Configurar cabeceras para diferenciar entre destinatarios	35	
Soporte de sistema de direcciones de Internet para el mandato SNDDST	36	
Adjuntar archivos	37	
Recibir correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)	37	
Gestionar el correo electrónico	38	
Comprobar servidores de correo electrónico	38	
Eliminar usuarios de correo electrónico de protocolo de oficina postal (POP)	39	

Impedir que se dividan los mensajes de correo electrónico largos	39	Resolver problemas relacionados con el correo electrónico.	51
Recibir estado de entrega de correo electrónico	39	Determinar problemas relacionados con el correo electrónico.	51
Hospedar un servidor Domino y un servidor SMTP en el mismo sistema	40	Comprobar los diarios de componentes	53
Hospedar LDAP Domino y el servidor de directorio en el mismo sistema	41	Hacer un seguimiento del correo electrónico no entregado	54
Gestionar el rendimiento del servidor de protocolo simple de transferencia de correo (SMTP).	41	Resolver problemas relacionados con la API QtmmSendMail	54
Cambiar valores del servidor de protocolo simple de transferencia de correo (SMTP)	42	Comprobar la llamada de API	54
Cambiar valores para el cliente de protocolo simple de transferencia de correo (SMTP)	43	Comprobar el archivo MIME (Multipurpose Internet Mail Extension)	55
Seleccionar un subsistema nuevo para los trabajos del servidor de protocolo simple de transferencia de correo (SMTP)	43	Comprobar los trabajos de la infraestructura de servidor de correo (MSF).	55
Información de consulta relacionada con el correo electrónico.	44	Información relacionada con el temario Correo electrónico.	55
Entradas de diario del servidor de correo	44	Apéndice. Avisos 57	
Protocolo simple de transferencia de correo (SMTP).	49	Información de la interfaz de programación	59
Protocolo de oficina postal (POP)	50	Marcas registradas	59
		Términos y condiciones	59

Correo electrónico

Utilice la siguiente información para planificar, configurar, usar, gestionar y resolver problemas relacionados con el correo electrónico en el sistema.

En esta información se presupone que ya ha trabajado con el sistema operativo i5/OS, que posee conocimiento suficiente para el uso de TCP/IP y del protocolo simple de transferencia de correo (SMTP), y que está familiarizado con los conceptos relacionados con el correo electrónico.

Novedades de la V6R1

Aquí encontrará la información nueva o la que ha cambiado sustancialmente en el temario Correo electrónico en la V6R1.

Soporte S/MIME de SMTP

El protocolo S/MIME (secure/Multipurpose Internet Mail Extensions) permite verificar los remitentes de correo electrónico cuando hay múltiples transacciones en una entrega del protocolo simple de transferencia de correo (SMTP). Con el protocolo, el documento de correo electrónico puede estar firmado o cifrado. Hay una nueva API QtmsCreateSendEmail que proporciona soporte S/MIME.

Para obtener una definición de S/MIME y para conocer los pasos de configuración al utilizar la nueva API en un escenario, lea estos temas:

- “Conceptos relacionados con el correo electrónico” en la página 2
- “Escenario: configurar la API QtmsCreateSendEmail para que utilice S/MIME” en la página 7

Autenticación SMTP y soporte SSL/TLS

Con la autenticación SMTP, ahora puede rastrear un originador de correo electrónico. El servidor SMTP de i5/OS también soporta las sesiones que están protegidas por la capa de sockets seguros (SSL) o por la seguridad de capa de transporte (TLS).

- “Controlar el acceso del protocolo simple de transferencia de correo (SMTP)” en la página 11
- “Rastrear el remitente de correo electrónico” en la página 27

Soporte SSL/TLS de POP

Ahora el servidor de protocolo de oficina postal (POP) de i5/OS también soporta sesiones SSL/TLS. El servidor puede cifrar los ID de usuario y las contraseñas.

- “Configurar clientes de correo electrónico de protocolo de oficina postal (POP)” en la página 32

Cómo ver las novedades o los cambios

Para ayudarle a ver dónde se han realizado cambios técnicos, en este documento se utiliza:

- La imagen  para marcar donde empieza la información nueva o cambiada.
- La imagen  para marcar donde acaba la información nueva o cambiada.

En los archivos PDF, verá barras de revisión (|) en el margen izquierdo de la información nueva o cambiada.

Para obtener más información sobre las novedades o los cambios de este release, vea el memorándum para los usuarios.

Archivo PDF del tema Correo electrónico

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF de este documento, seleccione Correo electrónico (alrededor de 692 KB).

Cómo guardar los archivos PDF

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. En el navegador, pulse el enlace del PDF con el botón derecho del ratón.
2. Pulse la opción destinada a guardar el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

Para poder ver o imprimir estos archivos PDF, debe tener Adobe Reader instalado en su sistema. Puede descargar una copia gratuita desde el sitio Web de Adobe ([www.adobe.com/products/acrobat/](http://www.adobe.com/products/acrobat/readstep.html)

[readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

Referencia relacionada

“Información relacionada con el temario Correo electrónico” en la página 55

Manuales del producto, publicaciones IBM Redbooks, sitios Web y otros temarios de Information Center que contienen información relacionada con el temario Correo electrónico. Puede ver o imprimir cualquiera de los archivos PDF.

Conceptos relacionados con el correo electrónico

El correo electrónico constituye una herramienta de gestión empresarial esencial. El sistema operativo i5/OS usa protocolos, como el protocolo simple de transferencia de correo (SMTP) y el protocolo de oficina postal (POP), que permiten que el correo electrónico funcione en la red de manera continua y eficaz.

Métodos de distribución

Estos conceptos adicionales sobre el correo electrónico se refieren a otros métodos de distribución de correo electrónico:

- Multipurpose Internet Mail Extensions (MIME)

MIME es un método estandarizado para organizar formatos de archivos divergentes. SMTP está limitado a texto ASCII de 7 bits con una longitud máxima de línea de 1000 caracteres. MIME se ha desarrollado para admitir tipos de archivos más avanzados como, por ejemplo, archivos de texto enriquecido, de imágenes y de audio o vídeo. MIME codifica archivos de datos de tipo binario de modo que aparezcan como datos SMTP simples, utilizando cabeceras para distinguir tipos de archivos diferentes dentro del mensaje antes de enviarlo con SMTP. Luego el cliente de correo recibe el mensaje y lo decodifica en los tipos de archivos adecuados, interpretando las cabeceras MIME para leer el archivo.

- | • S/MIME

| Secure/MIME es una versión segura del protocolo MIME que permite a los usuarios enviar mensajes cifrados y firmados electrónicamente, incluso si los usuarios tienen programas de correo diferentes.

- Infraestructura AnyMail/400

La infraestructura AnyMail/400 procesa todo el correo entrante de SMTP para usuarios locales (usuarios con cuentas de correo en este sistema). La infraestructura de servidor de correo es una

estructura de distribución de correo que permite distribuir correo electrónico. La infraestructura de servidor de correo llama a los snap-in o programas de salida para que manejen tipos de correo específicos.

- Servicios de distribución de arquitectura de sistemas en red (SNADS)

SNADS es un servicio de distribución asíncrono de IBM que define un conjunto de reglas para recibir, direccionar y enviar correo electrónico en una red de sistemas. En este tema, SNADS hace referencia a un perfil de usuario en el que la **Dirección preferida** está establecida en **ID de usuario/Dirección**. La dirección preferida indica a la infraestructura de servidor de correo qué campos debe utilizar en el directorio de distribución del sistema para la dirección.

Conceptos relacionados

“Enviar y recibir correo electrónico” en la página 32

Su sistema es un servidor de correo y tiene usuarios de correo electrónico (usuarios de SNADS, POP o Lotus) inscritos en él. Los usuarios de correo electrónico pueden enviar, recibir y leer correo electrónico utilizando un cliente POP o un cliente SNADS.

Tareas relacionadas

“Retener colas de servicios de distribución de arquitectura de sistemas en red (SNADS)” en la página 14

Puede retener colas de distribución de los servicios de distribución de arquitectura de sistemas en red (SNADS), que la aplicación SMTP utiliza para distribuir el correo electrónico. De esta manera, tendrá una mayor protección para limitar la distribución de correo electrónico.

Protocolo simple de transferencia de correo en i5/OS

El protocolo simple de transferencia de correo (SMTP) es el protocolo que permite al sistema operativo enviar y recibir correo electrónico.

Básicamente, SMTP es la entrega de correo de extremo a extremo desde un servidor de correo a otro. Existe una conexión directa entre un emisor SMTP (el cliente) y el receptor SMTP destino (el servidor). El cliente SMTP conserva el correo en el emisor hasta que lo transmite y lo copia satisfactoriamente en el receptor SMTP (servidor).

En este sistema operativo, SMTP soporta la distribución de notas, mensajes y documentos de texto ASCII. SMTP, además del texto sin formatear, puede admitir otros formatos mediante el protocolo MIME (Multipurpose Internet Mail Extensions). MIME es el estándar Internet para enviar correo con cabeceras en las que se describe el contenido de los mensajes de correo para el cliente receptor. Estos mensajes pueden contener componentes de vídeo, audio o binarios.

Acerca de la entrega de correo electrónico de SMTP

Para que el correo electrónico llegue a su destino, SMTP debe poderlo entregar al host correcto y al ID de usuario que reside en ese host. Supongamos que se envía correo a bobsmith@mycompany.com.

En primer lugar, SMTP comprueba si el destinatario del correo electrónico (bobsmith) es un usuario del servidor local. Si SMTP determina que no es así, reenvía el correo electrónico al siguiente servidor de hospedaje (host). El siguiente host podría ser o no ser el host final. SMTP determina el nombre del host a partir de la información del sistema de direcciones que se encuentra en el protocolo SMTP.

Entonces, SMTP resuelve la dirección del host, ya sea utilizando el servidor del sistema de nombres de dominio (DNS) o la tabla de hosts locales. El nombre de host forma parte de la cuenta de correo electrónico (mycompany.com), y la dirección IP es lo que utiliza SMTP para buscar el servidor de correo correcto al que enviar el correo (192.1.1.10).

1. Las direcciones IPv6 se ignoran cuando el servidor SMTP busca las direcciones del nombre de host en la tabla de hosts locales.

2. Si un servidor DNS configurado tiene direcciones IPv6, todos los servidores DNS configurados deben soportar la recursión con el fin de resolver los dominios de correo electrónico para los que los servidores configurados no son una autoridad.

En estos temas se indica la relación que hay entre DNS y SMTP:

- Configuración de dominios en el sistema de nombres de dominio (DNS)
- Registros de correo y de intercambiador de correo (MX)

En el caso del correo electrónico de entrada, el servidor SMTP primero convierte el nombre de host destino en una dirección de protocolo Internet (IP). Debido a la función de asignación de alias, el servidor puede tener varios nombres de host. Por lo tanto, el servidor SMTP utiliza la interfaz de sockets para determinar si la dirección IP es una de las que las interfaces utilizan para el host local.

Conceptos relacionados

DNS

Registros de correo y de intercambiador de correo (MX)

Tareas relacionadas

Configuración de dominios en el sistema de nombres de dominio (DNS)

“Configurar el correo electrónico” en la página 15

Para configurar el correo electrónico en el sistema, debe configurar TCP/IP, configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP), e iniciar los servidores de correo electrónico.

Protocolo de oficina postal (POP) en i5/OS

El servidor de protocolo de oficina postal (POP) es la implementación i5/OS de la interfaz de correo del Protocolo de Oficina Postal Versión 3.

El servidor POP proporciona buzones de correo electrónico en este sistema operativo, de donde los clientes pueden recuperar su correo. Cualquier cliente de correo que ofrezca soporte para el protocolo POP3 puede utilizar este servidor, como Netscape Mail, Outlook Express o Eudora. Los clientes se pueden ejecutar en cualquier plataforma, como Windows, Linux, AIX o Macintosh.

El servidor POP funciona a modo de área de retención temporal para el correo hasta que el cliente de correo lo recupera. El cliente de correo, cuando se conecta al servidor, consulta el contenido del buzón para ver si tiene algún mensaje de correo que recuperar. Si lo hay, recupera los mensajes de uno en uno. Después de haber recuperado un mensaje, el cliente indica al servidor que marque el mensaje para suprimirlo al finalizar la sesión del cliente. El cliente recupera todos los mensajes del buzón y emite un mandato que indica al servidor que suprima todos los mensajes marcados para supresión y se desconecte del cliente.

Los clientes de correo POP utilizan *verbos* para comunicarse con el servidor POP. Los verbos soportados por el servidor de protocolo de oficina postal (POP) para este sistema operativo se describen en el tema Protocolo de oficina postal (POP).

Tareas relacionadas

“Acceder a servidores de correo electrónico con System i Navigator” en la página 15

Puede utilizar System i Navigator para configurar y gestionar servidores de correo electrónico de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP).

“Configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) para correo electrónico” en la página 16

Para utilizar el correo electrónico, debe configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) en su sistema.

Referencia relacionada

“Protocolo de oficina postal (POP)” en la página 50

La interfaz de correo Protocolo de oficina postal (POP) Versión 3 está definida en la solicitud de comentarios (RFC) 1939 (POP3), en la RFC 2449 (Mecanismo de extensión POP3) y en la RFC 2595 (Utilizar TLS con IMAP, POP3 y ACAP). Las solicitudes de comentarios (RFC) son el mecanismo que se utiliza para definir los estándares de Internet en evolución.

Información relacionada

 Índice de RFC

Escenario: Correo electrónico

Estos escenarios ilustran cómo se procesa el correo electrónico entre los usuarios locales y cómo se puede configurar la API `QtmsCreateSendEmail` para usar S/MIME.

Escenario: enviar y recibir correo electrónico localmente

En este escenario se hace una demostración de cómo se procesa el correo electrónico entre usuarios locales.

Situación

Jane Smith, directora de Recursos Humanos, debe enviar un mensaje a Sam Jones del departamento jurídico. Ambos trabajan en las oficinas centrales de MyCompany. Siguiendo este proceso, puede ver cómo se maneja el correo electrónico en el sistema.

Los objetivos a largo plazo de este ejemplo son:

- Demostrar cómo se relacionan entre sí los clientes y los servidores de correo electrónico y cómo se procesa un mensaje
- Utilizar el servidor SMTP para enviar correo
- Entregar correo a un usuario de POP

Detalles

Jane utiliza el cliente de correo Netscape. Escribe un mensaje y se lo envía a `SamJones@mycompany.com`. El siguiente ejemplo muestra la ruta que sigue el mensaje por la red.

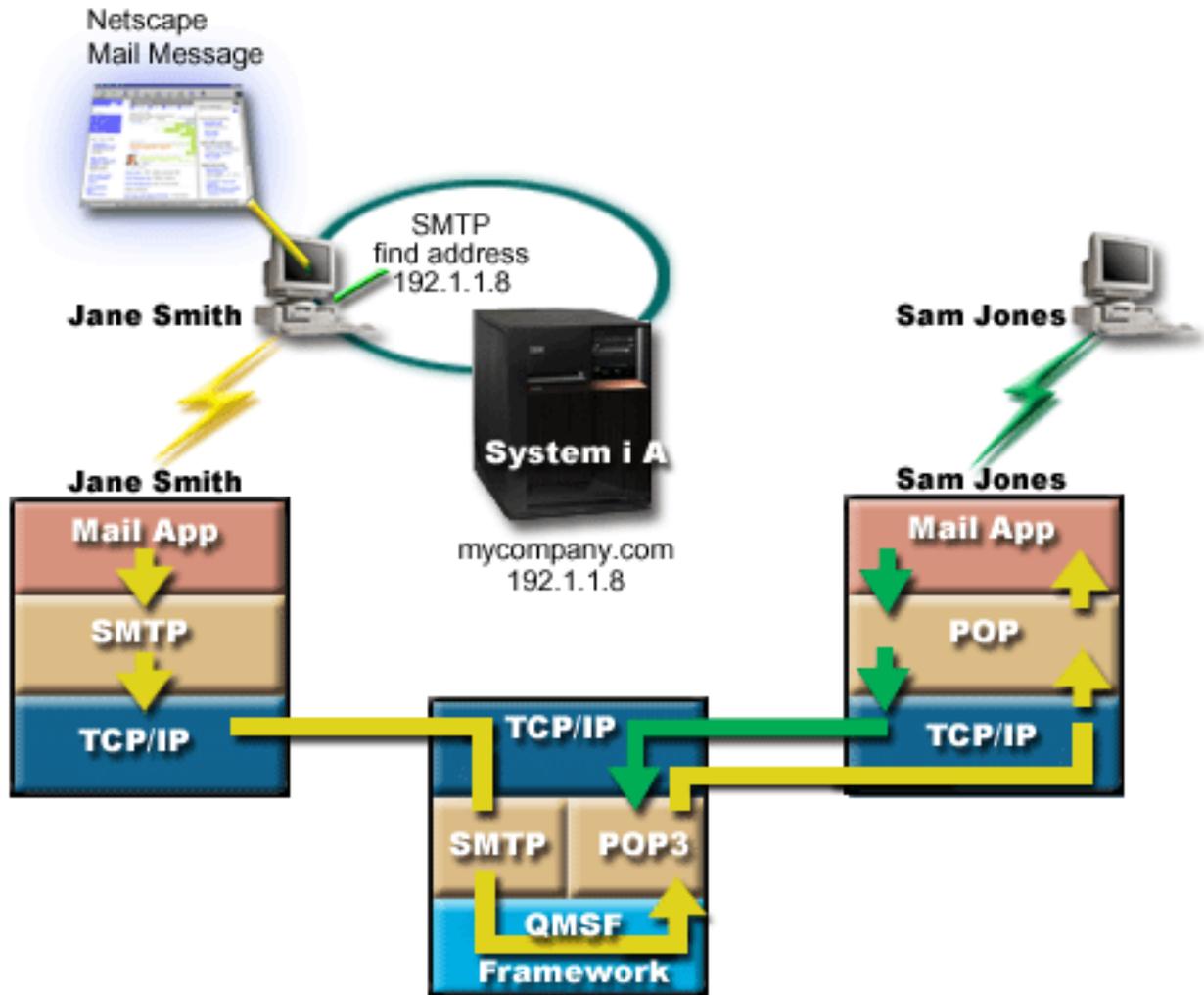


Figura 1. Configuración de red de ejemplo

El siguiente texto describe cada fase de la ruta que sigue el mensaje de correo por la red.

Fase 1: de cliente SMTP a servidor SMTP

El cliente SMTP del PC de Jane utiliza los datos de configuración que se han entrado para la identidad y el servidor de correo saliente. El campo de identidad se utiliza para la dirección De. El servidor de correo saliente es el host contactado por el cliente SMTP del PC. Puesto que la dirección se entra como dominio, el cliente SMTP consulta el sistema de nombres de dominio (DNS) para obtener la dirección IP del servidor SMTP, y descubre que es 192.1.1.8.

Ahora el cliente SMTP contacta con el servidor SMTP en el puerto SMTP (Puerto 25 en 192.1.1.8). El diálogo que se utiliza entre el cliente y el servidor es el protocolo SMTP. El servidor SMTP acepta la entrega del correo, y el mensaje se transmite del cliente al servidor utilizando TCP/IP.

Fase 2: el servidor SMTP entrega el mensaje al servidor POP

El servidor SMTP prueba el dominio del destinatario para comprobar si es local. Como es local, el correo se escribe en un archivo del sistema de archivos integrado, y se utiliza la interfaz de programación de aplicaciones (API) Crear mensaje de infraestructura QMSF para poner la información del mensaje en la

cola QMSF. La infraestructura QMSF permite distribuir el correo electrónico, llamando a programas de salida o snap-in para manejar tipos de correo específicos. La información del mensaje identifica la dirección de Sam como formato SMTP, por lo que la infraestructura llama al programa de salida de resolución de direcciones SMTP. Este programa vuelve a comprobar si se trata de un mensaje local. Al verificar que sí, utiliza el directorio de distribución del sistema (datos entrados mediante WRKDIRE) para buscar la dirección SMTP del destinatario. Localiza la dirección de Sam y averigua que el nivel de servicio de correo es el almacén de mensajes del sistema en la entrada de directorio para este usuario; entonces lo reconoce como una cuenta POP. La resolución de direcciones de SMTP añade la información del perfil a la información del mensaje. Marca la información como entrega local de POP. Luego, la infraestructura QMSF llama al programa de salida de entrega local de POP, que encuentra la información del perfil y el nombre del archivo del sistema de archivos integrado y entrega el correo en el buzón de Sam.

Fase 3: el cliente POP recupera el mensaje para Sam Jones del servidor POP

Más tarde, Sam decide utilizar su cliente de correo (Netscape) para ver si tiene mensajes de correo electrónico en su buzón. El cliente POP de su PC está configurado para buscar en el servidor POP de mycompany.com el nombre de usuario SamJones y la contraseña (*****). El nombre de dominio se vuelve a cambiar por una dirección IP (utilizando DNS). El cliente POP se pone en contacto con el servidor POP utilizando el puerto POP y el protocolo POP3. El servidor POP del sistema operativo comprueba si el nombre del usuario del buzón de correo y la contraseña coinciden con el perfil y la contraseña de un usuario de i5/OS. Una vez que se ha validado, se utiliza el nombre del perfil para localizar el buzón de Sam. El cliente POP carga el mensaje y envía una solicitud de nuevo al servidor POP para que suprima el correo del buzón POP. El mensaje se visualiza en Netscape para que Sam lo lea.

Conceptos relacionados

“Planificar el correo electrónico” en la página 10

Antes de configurar el correo electrónico, debe elaborar un plan básico sobre cómo utilizar el correo electrónico en su sistema.

Referencia relacionada

“Protocolo simple de transferencia de correo (SMTP)” en la página 49

El protocolo simple de transferencia de correo (SMTP) es un protocolo TCP/IP que se utiliza para enviar y recibir correo electrónico. Normalmente se utiliza con POP3 o con el protocolo de acceso a mensajes de Internet (IMAP) para guardar mensajes en un buzón del servidor y descargarlos periódicamente del servidor para el usuario.

“Protocolo de oficina postal (POP)” en la página 50

La interfaz de correo Protocolo de oficina postal (POP) Versión 3 está definida en la solicitud de comentarios (RFC) 1939 (POP3), en la RFC 2449 (Mecanismo de extensión POP3) y en la RFC 2595 (Utilizar TLS con IMAP, POP3 y ACAP). Las solicitudes de comentarios (RFC) son el mecanismo que se utiliza para definir los estándares de Internet en evolución.

| Escenario: configurar la API QtmsCreateSendEmail para que utilice S/MIME

| Este ejemplo muestra cómo se puede configurar la API QtmsCreateSendEmail para que utilice secure/MIME (S/MIME).

| Situación

| El usuario John Smith cuyo ID es jsmith quiere configurar la API QtmsCreateSendEmail para que utilice S/MIME. S/MIME es una manera más segura de enviar correo electrónico programáticamente que cuando se emplea la API QtmmSendMail.

| Detalles

| Para enviar correo electrónico firmado y cifrado, John necesita tener instaladas las opciones siguientes en el sistema que ejecuta i5/OS V6R1:

- | • i5/OS PASE (5761-SS1 opción 33)
- | • Digital Certificate Manager (5761-SS1 opción 34)
- | • OpenSSL (5733-SC1 opción 1)

| Crear un almacén de certificados de usuario

| Para utilizar S/MIME se necesita un repositorio de los certificados de usuario, que se llama almacén de certificados de usuario. En el sistema operativo, los certificados de los usuarios utilizan el convenio de denominación *idusuario.usrcrt*. Los certificados están en el directorio `/qibm/userdata/icss/cert/download/client`.

| John debe configurar el almacén de certificados de usuario para su propio perfil de usuario, bajo el que se ejecuta el trabajo de crear y enviar mensajes de correo. Para gestionar el almacén de certificados de usuario, puede usar el gestor de certificados digitales (DCM).

| Para crear un almacén de certificados de usuario, siga estos pasos:

- | 1. Cree un subdirectorío utilizando el nombre del perfil de usuario:

```
| cd /qibm/userdata/icss/cert/download/client  
| mkdir jsmith
```

- | 2. Mediante el navegador Web, vaya a la página Tareas de System i en su sistema, en `http://nombre_del_sistema: 2001`.

- | 3. Seleccione **Gestor de certificados digitales (DCM)** en la lista de productos, en la página Tareas de System i, para acceder la interfaz de usuario de DCM. En el panel izquierdo pulse **Crear almacén de certificados nuevo**.

- | 4. En la página Crear almacén de certificados nuevo, seleccione **Otro almacén de certificados del sistema** y pulse **Continuar**.

- | 5. En la página Crear un certificado en el almacén de certificados nuevo, seleccione **No - No crear un certificado en el almacén de certificados**.

- | 6. En la página Nombre y contraseña de almacén de certificados, establezca el nombre de la vía de acceso del almacén de certificados y la contraseña. Establezca la vía de acceso del almacén de certificados para que incluya el ID de usuario. Por ejemplo, John establece su vía de acceso de almacén como `/qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb`.

| Exportar el certificado de usuario del remitente a System i

| El navegador Web de John es Internet Explorer (IE) 6. El certificado de usuario del remitente se obtiene de la entidad emisora de certificados (CA) y se instala en IE 6.

| Para exportar el certificado de usuario del remitente a la plataforma System i, se le indica a John que realice estos pasos:

- | 1. En la ventana de IE, seleccione **Herramientas** → **Opciones de Internet**.
- | 2. En la pestaña **Contenido** pulse **Certificados**.
- | 3. En la pestaña **Personal**, seleccione el certificado de remitente y pulse **Exportar**.
- | 4. En la página Bienvenida al asistente de exportación de certificado, pulse **Siguiente**.
- | 5. En la página Exportar clave privada, seleccione **Sí, exportar la clave privada** y pulse **Siguiente**.
- | 6. Para la página Formato de archivo de exportación, seleccione **Habilitar protección fuerte (requiere IE 5.0, NT 4.0 SP4 o superior)** bajo **Intercambio de información personal - PKCS n° 12 (.PFX)**.

- | 7. En la página Contraseña, teclee la contraseña del certificado.
- | 8. En la página Archivo a exportar, especifique el nombre del archivo que desea exportar, por ejemplo, C:\temp\jsmithcert.pfx, y pulse **Siguiente**.
- | 9. En la página Completar el asistente de exportación de certificado, pulse **Finalizar**.
- | 10. Envíe el certificado de usuario remitente jsmithcert.pfx en modalidad ASCII, mediante FTP, a la plataforma System i. En este ejemplo, se presupone que este archivo se envía al directorio /home/jsmith del sistema de archivos integrado de System i. Para obtener detalles sobre cómo importar este certificado, consulte: “Importar el certificado del remitente a System i”.

| **Exportar los certificados de usuario del destinatario a System i**

| Para exportar el certificado de usuario del destinatario a la plataforma System i, se le indica a John que realice estos pasos:

- | 1. En la ventana de IE, seleccione **Herramientas** → **Opciones de Internet**.
- | 2. Pulse la pestaña **Contenido** de la página Opciones de Internet, y luego pulse **Certificados**.
- | 3. En la pestaña **Personal** de la página Opciones de Internet, seleccione el certificado y pulse **Exportar**. Si existe más de un certificado, debe repetir los pasos del 3 al 7 para todos los certificados.
- | 4. En la página Bienvenido al asistente de exportación de certificado, pulse **Siguiente**.
- | 5. En la página Formato de archivo de exportación, seleccione **X.509 codificación binaria DER (.CER)**.
- | 6. En la página Archivo a exportar, especifique el nombre del archivo que desea exportar, por ejemplo, C:\temp\receiveruser.cer, y pulse **Siguiente**.
- | 7. En la página Completar el asistente de exportación de certificado, pulse **Finalizar**.
- | 8. Envíe el certificado de usuario del destinatario receiver.cer en modalidad ASCII, mediante FTP, a la plataforma System i. En este ejemplo, se presupone que este archivo se envía al directorio /home/jsmith del sistema de archivos integrado de System i. Para obtener detalles sobre cómo importar el certificado del destinatario, consulte: “Importar el certificado de destinatario a System i” en la página 10.
- | 9. Repita todos los pasos anteriores para cada destinatario que se utilice en S/MIME.

| **Importar el certificado del remitente a System i**

| Luego, John necesita importar el certificado de usuario y la clave privada al almacén de certificados mediante DCM. La contraseña del certificado importado debe coincidir con la del almacén de claves. También necesita importar todos los certificados de los usuarios a los que desea enviar correo electrónico.

- | 1. Mediante el navegador Web, vaya a la página Tareas de System i en su sistema, en http://nombre_del_sistema:2001.
- | 2. Seleccione **Gestor de certificados digitales (DCM)** en la lista de productos, en la página Tareas de System i, para acceder la interfaz de usuario de DCM.
- | 3. En la página Seleccionar un almacén de certificados, seleccione **Otro almacén de certificados del sistema** y pulse **Continuar**.
- | 4. En la página Nombre y contraseña del almacén de certificados, teclee el nombre de archivo y la vía de acceso del almacén de certificados y la contraseña, y pulse **Continuar**. En el caso de John, el nombre del archivo es /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.
- | 5. Expanda **Gestionar certificados** → **Importar certificado**. Seleccione **Servidor o cliente** para importar el certificado del remitente. Pulse **Continuar**.
- | 6. En la página Importar certificado de cliente o servidor, teclee el directorio del sistema de archivos integrado y el nombre de archivo del certificado del remitente y pulse **Continuar**. En “Exportar el certificado de usuario del remitente a System i” en la página 8, el directorio y el archivo del sistema de archivos integrado es /home/jsmith/ jsmithcert.pfx.

- | 7. Especifique la etiqueta del certificado, es decir, la dirección de correo electrónico del remitente en minúsculas. Pulse **Continuar**.
- | 8. Pulse **Aceptar**.

| **Importar el certificado de destinatario a System i**

| Para importar el certificado del destinatario a la plataforma System i, siga estos pasos:

- | 1. Mediante el navegador Web, vaya a la página Tareas de System i en su sistema, en `http://nombre_del_sistema: 2001`.
- | 2. Seleccione **Gestor de certificados digitales (DCM)** en la lista de productos, en la página Tareas de System i, para acceder la interfaz de usuario de DCM.
- | 3. En la página Seleccionar un almacén de certificados, seleccione **Otro almacén de certificados del sistema** y pulse **Continuar**.
- | 4. En la página Nombre y contraseña del almacén de certificados, teclee el nombre de archivo y la vía de acceso del almacén de certificados y la contraseña, y pulse **Continuar**. En el caso de John, el nombre del archivo es `/qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb`.
- | 5. Expanda **Gestionar certificados** → **Importar certificado**. Seleccione **Entidad emisora de certificados (CA)** para importar el certificado del destinatario. Pulse **Continuar**.
- | 6. En la página de Importar certificado de entidad emisora de certificados (CA), teclee el directorio y el nombre de archivo del sistema de archivos integrado del certificado del destinatario, y pulse **Continuar**. En “Exportar los certificados de usuario del destinatario a System i” en la página 9 el directorio y el archivo del sistema de archivos integrado del destinatario es `/home/jsmith/receiveruser.cer`.
- | 7. Especifique la etiqueta del certificado de CA, es decir, la dirección de correo electrónico del remitente en minúsculas. Pulse **Continuar**.
- | 8. Repita todos los pasos anteriores para cada uno de los certificados del destinatario que el remitente deba utilizar.

| **Conceptos relacionados**

| Gestor de certificados digitales (DCM)

| **Referencia relacionada**

| API Crear y enviar correo electrónico MIME (QtmsCreateSendEmail)

Planificar el correo electrónico

Antes de configurar el correo electrónico, debe elaborar un plan básico sobre cómo utilizar el correo electrónico en su sistema.

Antes de empezar a configurar el correo electrónico, responda a las siguientes preguntas:

- 1. ¿Cómo van a ser mis direcciones de correo electrónico?
- 2. ¿Cuál es la dirección IP de mi servidor de nombres de dominio (DNS)?
- 3. ¿Tengo un cortafuegos? Si la respuesta es afirmativa, ¿cuál es su dirección IP?
- 4. ¿Tengo un proxy de correo, un direccionador de correo o una retransmisión de correo? Si la respuesta es afirmativa, ¿cuál es su dirección IP?
- 5. ¿Voy a utilizar una base de datos de Domino?
- 6. ¿Voy a utilizar el servidor POP de i5/OS para recibir correo?

Si lo desea, puede consultar el escenario de correo electrónico para obtener información básica acerca del funcionamiento del correo electrónico.

Si se propone utilizar el servidor Domino y el servidor SMTP de i5/OS, consulte el tema: Hospedar un servidor Domino y un servidor SMTP en el mismo sistema. Para obtener información adicional sobre Domino, consulte el tema: Domino, o el sitio Web de Lotus Domino para i5/OS.

Si no piensa utilizar los servidores SMTP o POP, inhabílitelos para asegurarse de que no se utilizan sin que usted lo sepa.

Conceptos relacionados

“Escenario: enviar y recibir correo electrónico localmente” en la página 5

En este escenario se hace una demostración de cómo se procesa el correo electrónico entre usuarios locales.

Domino

Tareas relacionadas

“Configurar el correo electrónico” en la página 15

Para configurar el correo electrónico en el sistema, debe configurar TCP/IP, configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP), e iniciar los servidores de correo electrónico.

“Hospedar un servidor Domino y un servidor SMTP en el mismo sistema” en la página 40

Si ejecuta Domino y el protocolo simple de transferencia de correo (SMTP) en el mismo sistema, le sugerimos que configure cada uno para que se enlace a una dirección IP específica.

Información relacionada



Lotus Domino para i5/OS

Controlar el acceso al correo electrónico

Debe controlar quién accede a su sistema mediante correo electrónico para proteger sus datos de los ataques maliciosos.

Esta sección proporciona sugerencias para proteger los servidores de correo electrónico contra ataques de inundación y correo masivo.

Conceptos relacionados

Ejemplos de agrupaciones de discos independientes

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Tareas relacionadas

“Restringir la retransmisión de mensajes” en la página 28

Para impedir que otras personas utilicen el servidor de correo electrónico para el correo masivo o para enviar grandes cantidades de mensajes de correo electrónico no deseado, puede utilizar la función de restricción de retransmisión y especificar quién puede usar su sistema para retransmitir mensajes. Sin embargo, cuando restringe la retransmisión de mensajes, no puede autenticar el correo electrónico.

“Restringir conexiones” en la página 31

Para garantizar la seguridad del sistema, debe impedir la conexión de usuarios que podrían abusar del servidor de correo electrónico.

Información relacionada



AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet

Controlar el acceso del protocolo simple de transferencia de correo (SMTP)

Para evitar que el sistema sea atacado por correo malicioso o no solicitado (spam), debe controlar el acceso del protocolo simple de transferencia de correo (SMTP).

Si desea permitir que clientes SMTP accedan al sistema, debe proteger el sistema de posibles ataques, realizando estas tareas:

- Si es posible, evite utilizar una entrada *ANY *ANY en el directorio de distribución del sistema. Cuando el sistema no tiene ninguna entrada *ANY *ANY, es más difícil que alguien pueda intentar utilizar SMTP para saturar el sistema o la red. La saturación se produce cuando el almacenamiento auxiliar se llena con correo no deseado que se direcciona a través de su sistema a otro sistema.
- Establezca límites de umbral adecuados para las agrupaciones de almacenamiento auxiliar (ASP) para impedir que un usuario pueda saturar el sistema con objetos no deseados. Puede visualizar y establecer los umbrales de las ASP utilizando las herramientas de servicio del sistema (SST) o las herramientas de servicio dedicado (DST).
- Ajuste el número máximo de trabajos de prearranque que se pueden crear, utilizando el mandato Cambiar entrada de trabajo de prearranque (CHGPJE). Esto limita el número de trabajos creados durante un ataque de denegación de servicio. Para el umbral máximo, el valor predeterminado es 256.
- Impida que los intrusos utilicen su conexión para enviar correo electrónico no solicitado (correo masivo) restringiendo retransmisiones y conexiones.
- En los sistemas que ejecutan i5/OS V6R1, puede impedir el correo masivo exigiendo la autenticación para enviar correo electrónico. Si un servidor remoto exige autenticación, puede configurarla en su servidor local.

Referencia relacionada

Mandato Cambiar atributos de SMTP (CHGSMTPA)

Controlar el acceso del protocolo de oficina postal (POP)

Para garantizar la seguridad del sistema, debe controlar el acceso del protocolo de oficina postal (POP).

- Puede especificar si el servidor POP utiliza el cifrado para proteger las corrientes de datos de POP, incluidos los ID de usuario y las contraseñas. Se proporciona cifrado con la capa de sockets seguros (SSL) y con la seguridad de capa de transporte (TLS). Para indicar si se soportan las sesiones POP seguras, establezca el parámetro ALWSSL en el mandato CL Cambiar atributos de servidor POP (CHGPOPA).

Si desea permitir que clientes POP accedan al sistema, tenga en cuenta las siguientes consideraciones sobre seguridad:

- El servidor de correo POP proporciona autenticación para clientes que intentan acceder a los buzones de correo. El cliente envía al servidor una contraseña y un ID de usuario.
El servidor de correo POP verifica el ID del usuario y la contraseña comparándolo con el perfil de usuario y contraseña de i5/OS de ese usuario. Puesto que no tiene control sobre el modo en que se almacenan el ID y la contraseña del usuario en el cliente POP, le interesará crear un perfil especial que tenga autorización limitada en el sistema. Para impedir que se pueda utilizar el perfil de usuario para una sesión interactiva, puede establecer los valores siguientes en el perfil de usuario:
Establezca el menú inicial (INLMNU) en *SIGNOFF
Establezca el programa inicial (INLPGM) en *NONE
Establezca Limitar posibilidades (LMTCPB) en *YES
- Para evitar que un intruso inunde el servidor con objetos no deseados, asegúrese de que establece los límites de umbral adecuados para las agrupaciones de almacenamiento auxiliar (ASP). El umbral de almacenamiento de ASP impide que el servidor se detenga debido a que el sistema operativo no tenga suficiente espacio de trabajo. Puede visualizar y establecer los umbrales de ASP utilizando las herramientas de servicio del sistema (SST) o las herramientas de servicio dedicado (DST).
- Aunque debe asegurarse de que el umbral de ASP impide que el sistema se desborde, también debe asegurarse de que el sistema tiene espacio adecuado para almacenar y enviar correo adecuadamente. Puede constituir un problema de integridad para los usuarios que el servidor de correo no pueda entregar correo porque el sistema no dispone de almacenamiento adecuado para el correo transitorio. Cuando el uso del almacenamiento del sistema es alto, se detiene la ejecución del correo.
Normalmente, el espacio de almacenamiento no es un problema significativo. Cuando el cliente recibe el correo, el servidor lo borra del sistema.

Conceptos relacionados

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Impedir el acceso al correo electrónico

En función de cómo utilice el sistema, es posible que le interese impedir que los usuarios accedan al correo electrónico a través de los servidores SMTP y POP. Puede impedir totalmente el acceso al correo electrónico o puede permitir el acceso en determinadas ocasiones.

Impedir el acceso del protocolo simple de transferencia de correo (SMTP)

Si no quiere que se utilice indiscriminadamente el protocolo simple de transferencia de correo (SMTP) para distribuir correo a su sistema o desde él, debe impedir que se ejecute el servidor SMTP.

SMTP se configura por defecto para que se inicie automáticamente cuando se inicia TCP/IP. Si no tiene ninguna intención de utilizar SMTP, no lo configure en el sistema (o no permita que nadie más lo configure).

Impedir que se inicie el protocolo simple de transferencia de correo (SMTP) cuando se inicia TCP/IP:

Es posible que en alguna ocasión necesite utilizar el protocolo simple de transferencia de correo (SMTP), pero que desee limitar la cantidad de usuarios que tienen acceso al servidor SMTP.

Para impedir que los trabajos del servidor SMTP se inicien automáticamente cuando se inicia TCP/IP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Deseleccione **Iniciar cuando se inicia TCP/IP**.

Impedir el acceso a los puertos del protocolo simple de transferencia de correo (SMTP):

Con el fin de proteger el servidor de protocolo simple de transferencia de correo (SMTP) contra aplicaciones desconocidas, quizás le interese impedir el acceso a los puertos SMTP.

Para impedir que SMTP se inicie y que alguien asocie una aplicación de usuario (como una aplicación de socket) al puerto que el sistema utiliza normalmente para SMTP, lleve a cabo los pasos siguientes:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la ventana Propiedades de configuración de TCP/IP, pulse la pestaña **Restricciones de puerto**.
4. En la página Restricciones de puerto, pulse **Añadir**.
5. En la página Añadir restricción de puerto, especifique los siguientes valores:
 - **Nombre de usuario:** especifique un nombre de perfil de usuario que esté protegido en su sistema. (Perfil de usuario protegido es aquel que no es propietario de programas que adopten autorización y cuya contraseña no conocen los demás usuarios). Al restringir el puerto a un usuario específico, excluye automáticamente a los demás usuarios.
 - **Puerto inicial:** 25
 - **Puerto final:** 25
 - **Protocolo:** TCP
6. Pulse **Aceptar** para añadir la restricción.
7. En la página **Restricciones de puerto**, pulse **Añadir** y repita el procedimiento para UDP.

8. Pulse **Aceptar** para guardar las restricciones de puerto y cerrar la ventana **Propiedades de configuración de TCP/IP**. La restricción de puerto entrará en vigor la próxima vez que inicie TCP/IP. Si TCP/IP está activo cuando establece las restricciones de puerto, debe finalizar TCP/IP y volver a iniciarlo.

Retener colas de servicios de distribución de arquitectura de sistemas en red (SNADS):

Puede retener colas de distribución de los servicios de distribución de arquitectura de sistemas en red (SNADS), que la aplicación SMTP utiliza para distribuir el correo electrónico. De esta manera, tendrá una mayor protección para limitar la distribución de correo electrónico.

Para retener las colas de distribución, teclee los siguientes mandatos en la interfaz basada en caracteres:

```
HLDDSTQ DSTQ(QSMTPQ)PTY(*NORMAL)
HLDDSTQ DSTQ(QSMTPQ)PTY(*HIGH)
```

Conceptos relacionados

“Conceptos relacionados con el correo electrónico” en la página 2

El correo electrónico constituye una herramienta de gestión empresarial esencial. El sistema operativo i5/OS usa protocolos, como el protocolo simple de transferencia de correo (SMTP) y el protocolo de oficina postal (POP), que permiten que el correo electrónico funcione en la red de manera continua y eficaz.

Impedir el acceso del protocolo de oficina postal (POP)

Si no quiere que se utilice indiscriminadamente el protocolo de oficina postal (POP) para acceder a su sistema, debe impedir que se ejecute el servidor POP.

Si no tiene ninguna intención de utilizar POP, no lo configure en el sistema (o no permita que nadie más lo configure).

Impedir que se inicie el protocolo de oficina postal (POP) cuando se inicia TCP/IP:

Es posible que en alguna ocasión necesite utilizar el protocolo de oficina postal (POP), pero que desee limitar la cantidad de usuarios que tienen acceso al servidor POP.

El servidor POP se configura por defecto para que se inicie automáticamente cuando se inicia TCP/IP. Para impedir que los trabajos del servidor POP se inicien automáticamente cuando se inicia TCP/IP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **POP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Deseleccione **Iniciar cuando se inicia TCP/IP**.

Impedir el acceso a los puertos del protocolo de oficina postal (POP):

Con el fin de proteger el servidor de protocolo de oficina postal (POP) contra aplicaciones desconocidas, quizás le interese impedir el acceso a los puertos POP.

Para impedir que el servidor POP se inicie y que alguien asocie una aplicación de usuario (como una aplicación de socket) al puerto que el sistema utiliza normalmente para POP, lleve a cabo los pasos siguientes:

1. En System i Navigator, conéctese al sistema y expanda **Red** → **Servidores** → **TCP/IP**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la ventana Propiedades de configuración de TCP/IP, pulse la pestaña **Restricciones de puerto**.
4. En la página Restricciones de puerto, pulse **Añadir**.
5. En la página Añadir restricción de puerto, especifique los siguientes valores:

- **Nombre de usuario:** especifique un nombre de perfil de usuario que esté protegido en su sistema. (Perfil de usuario protegido es aquel que no es propietario de programas que adopten autorización y cuya contraseña no conocen los demás usuarios). Al restringir el puerto a un usuario específico, excluye automáticamente a los demás usuarios.
- **Puerto inicial:** 110 995
- **Puerto final:** 110 995
- **Protocolo:** TCP

6. Pulse **Aceptar** para añadir la restricción.
7. En la página Restricciones de puerto, pulse **Añadir** y repita el procedimiento para UDP.
8. Pulse **Aceptar** para guardar las restricciones de puerto y cerrar la ventana Propiedades de configuración de TCP/IP.

La restricción de puerto entrará en vigor la próxima vez que inicie TCP/IP. Si TCP/IP está activo cuando establece las restricciones de puerto, debe finalizar TCP/IP y volver a iniciarlo.

Configurar el correo electrónico

Para configurar el correo electrónico en el sistema, debe configurar TCP/IP, configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP), e iniciar los servidores de correo electrónico.

Conceptos relacionados

“Protocolo simple de transferencia de correo en i5/OS” en la página 3

El protocolo simple de transferencia de correo (SMTP) es el protocolo que permite al sistema operativo enviar y recibir correo electrónico.

“Planificar el correo electrónico” en la página 10

Antes de configurar el correo electrónico, debe elaborar un plan básico sobre cómo utilizar el correo electrónico en su sistema.

Acceder a servidores de correo electrónico con System i Navigator

Puede utilizar System i Navigator para configurar y gestionar servidores de correo electrónico de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP).

Para acceder a POP o SMTP en System i Navigator, siga estos pasos:

1. Pulse dos veces en la carpeta **Client Access Express**.
2. Pulse dos veces en **System i Navigator**. Si esta es la primera vez que utiliza System i Navigator, pulse el icono de **Conexión nueva** para establecer una conexión con su sistema.
3. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
4. Pulse dos veces en **SMTP** para abrir el diálogo Propiedades de SMTP, o pulse dos veces en **POP** para abrir el diálogo Propiedades de POP.

Conceptos relacionados

“Protocolo de oficina postal (POP) en i5/OS” en la página 4

El servidor de protocolo de oficina postal (POP) es la implementación i5/OS de la interfaz de correo del Protocolo de Oficina Postal Versión 3.

Configurar TCP/IP para correo electrónico

Debe configurar el TCP/IP antes de configurar el correo electrónico en su sistema.

Si está configurando el correo electrónico en el sistema por primera vez, realice los pasos siguientes. Si ya ha configurado TCP/IP en el sistema, puede ir directamente a Configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) para correo electrónico.

1. En System i Navigator, expanda *su sistema* → **Red** → **Configuración de TCP/IP**.

2. Pulse **Interfaces** con el botón derecho del ratón, seleccione **Interfaz nueva** y el tipo de red que representa la nueva interfaz. Siga las instrucciones del asistente para crear una nueva interfaz TCP/IP. El asistente le solicita que proporcione la información siguiente:

- Tipo de conexión
- Recurso de hardware
- Descripción de línea
- Dirección IP
- Nombre de host
- Nombre de dominio

El nombre de host y el nombre de dominio que utiliza para el asistente constituyen el nombre de dominio completo. SMTP requiere un nombre de dominio completo para comunicarse con otros hosts SMTP.

Por ejemplo, si el nombre de host local es ASHOST y el nombre de dominio local es DOMAIN.COMPANY.COM, el nombre del dominio completo es ASHOST.DOMAIN.COMPANY.COM.

- Servidores que hay que iniciar
3. Cuando haya acabado de utilizar el asistente, pulse **TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**. Aparece el diálogo Propiedades de TCP/IP.
4. Pulse la pestaña **Tabla de hosts**.
5. Pulse **Añadir**. Aparece el diálogo Entrada de tabla de hosts TCP/IP.
6. Entre la dirección IP y el nombre de host que utilizó en el asistente Nueva interfaz de TCP/IP.
7. Pulse **Aceptar** para cerrar el diálogo Entrada de tabla de hosts TCP/IP.
8. Pulse **Aceptar** para cerrar el diálogo Propiedades de TCP/IP.

Conceptos relacionados

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Tareas relacionadas

“Configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) para correo electrónico”

Para utilizar el correo electrónico, debe configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) en su sistema.

Configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) para correo electrónico

Para utilizar el correo electrónico, debe configurar los servidores de protocolo simple de transferencia de correo (SMTP) y de protocolo de oficina postal (POP) en su sistema.

Nota: Ambos servidores, SMTP y POP, deben estar correctamente configurados.

Conceptos relacionados

“Protocolo de oficina postal (POP) en i5/OS” en la página 4

El servidor de protocolo de oficina postal (POP) es la implementación i5/OS de la interfaz de correo del Protocolo de Oficina Postal Versión 3.

Tareas relacionadas

“Configurar TCP/IP para correo electrónico” en la página 15

Debe configurar el TCP/IP antes de configurar el correo electrónico en su sistema.

Configurar el servidor de protocolo simple de transferencia de correo (SMTP)

Cuando configuró TCP/IP, el sistema configuró SMTP automáticamente. Sin embargo, aún debe cambiar algunas propiedades SMTP para asegurarse de que el servidor SMTP funciona correctamente para el correo electrónico.

Para cambiar las propiedades de SMTP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.

2. Pulse dos veces en **SMTP**.

3. Pulse las pestañas que figuran en la tabla siguiente para establecer los valores de campo indicados en la columna Y realice la siguiente acción.

Pulse esta pestaña	Y realice la siguiente acción
General	Seleccione Iniciar cuando se inicia TCP/IP . ¹
General	Seleccione Sin máximo para el campo Tamaño de división de mensaje .
General	Si dispone de un direccionador de correo, entre el nombre del mismo, por ejemplo, mailrouter.company.com. El nombre del direccionador de correo es el nombre del servidor al que SMTP dirige el correo si el correo electrónico no es correo local. Para obtener información detallada, vea la ayuda de System i Navigator.
General	Si tiene una configuración de cortafuegos, seleccione Reenviar el correo saliente al direccionador a través del cortafuegos .
General	Si intercambia correo electrónico con servidores Domino, deselectione el campo Interpretar el signo de porcentaje como carácter de direccionamiento .
General	Si se desea reenviar todo el correo electrónico no local a otro servidor SMTP, especifique el nombre de dominio de intercambio de correo completo en el campo Reenviar dominio de correo .
General	Si quiere que el servidor SMTP soporte el salto de línea (LF) escueto o el salto de línea de retorno de carro (CRLF), seleccione Permitir salto de línea escueto . Si desea que el servidor SMTP soporte solo CRLF, quite la marca del recuadro de selección Permitir salto de línea escueto .
Registro automático	Si utiliza el mandato SNDDST para enviar correo electrónico y el mandato RCVDST para recibir correo electrónico, y además utiliza el sistema de direcciones SNADS en lugar del de Internet, marque el recuadro de selección Añadir automáticamente usuarios remotos al directorio de distribución del sistema .
Registro automático	Si utiliza el mandato SNDDST para enviar correo electrónico y el mandato RCVDST para recibir correo electrónico, pulse Tabla de alias del sistema en el campo Añadir usuarios a .

¹ Este cambio entrará en vigor la próxima vez que se inicie el servidor SMTP.

4. Pulse **Aceptar** para aceptar los cambios.

Tareas relacionadas

“Autenticar correo electrónico local y para retransmitir” en la página 27

Ahora puede impedir la entrada de correo masivo en el servidor exigiendo autenticación para enviar correo electrónico. No puede exigir autenticación si quiere restringir la retransmisión de mensajes. Le recomendamos que configure la autenticación para su servidor.

Habilitar SSL entre el servidor y el cliente SMTP en el sistema del destinatario:

Para habilitar SSL entre el servidor y el cliente SMTP en el sistema del destinatario, realice estos pasos. Se presupone que ya se ha creado un certificado de servidor en el servidor SMTP.

Para realizar esta tarea, asegúrese que está conectado al sistema del destinatario.

Iniciar y configurar DCM

1. En el navegador Web, conéctese al servidor SMTP: `http://su_sistema: 2001/`
2. En la página Tareas de i5/OS, seleccione **Gestor de certificados digitales (DCM)** y luego pulse **Seleccionar un almacén de certificados**.
3. En la página Seleccionar un almacén de certificados, seleccione ***SYSTEM** y pulse **Continuar**.
4. En la página Almacén de certificados y contraseña, teclee la contraseña del almacén de certificados.
5. Expanda **Gestionar aplicaciones** → **Actualizar asignación de certificado** y seleccione **Servidor**.
6. Seleccione **Servidor SMTP TCP/IP de i5/OS** y pulse **Actualizar asignación de certificado**, si es necesario.

Configurar el servidor SMTP

Para habilitar el soporte SSL, establezca que el parámetro ALWAUTH sea igual a *LCLRLY o *RELAY con el mandato Cambiar atributos de SMTP (CHGSMTPA).

- Si establece que el parámetro sea igual a *RELAY, solo se puede usar SSL para el correo electrónico enviado desde el otro servidor SMTP.
- Si establece que el parámetro sea igual a *LCLRLY, también se habilitan los parámetros Verificar mensajes MSF (VFYMSFMSG) y Verificar desde usuario (VFYFROMUSR). El valor predeterminado también puede provocar el rechazo de ciertos mensajes de correo electrónico. Determine si desea que el soporte de rechazos esté habilitado.

Configurar el cliente SMTP

Debe configurar el cliente SMTP de System i para que pueda iniciar sesión en el servidor SMTP destinatario de System i. Utilice el mandato CL Añadir entrada de lista SMTP (ADDSMTPLE) para añadir una entrada a la lista de autenticación de hosts:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(susistema.realm.com) USERNAME(receiver) PASSWORD(xxxx)
```

El nombre de host, que se almacena en mayúsculas, debe coincidir con la dirección de correo electrónico. Si la dirección de correo electrónico es myemail@susistema, hay que añadir la entrada:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(YOURSYSTEM) USERNAME(receiver) PASSWORD(xxxx)
```

Habilitar SSL entre el servidor y el cliente SMTP en el sistema del remitente:

Debe estar conectado al sistema del remitente para llevar a cabo esta tarea.

1. En el navegador Web, conéctese al servidor SMTP: `http://su_sistema: 2001/`
2. En la página Tareas de i5/OS, seleccione **Gestor de certificados digitales (DCM)** y luego pulse **Seleccionar un almacén de certificados**.
3. En la página Seleccionar un almacén de certificados, seleccione ***SYSTEM** y pulse **Continuar**.
4. En la página Almacén de certificados y contraseña, teclee la contraseña del almacén de certificados y pulse **Continuar**. Si no tiene un certificado de usuario o si desea crear uno, realice los pasos del 5 al 8; en caso contrario, vaya directamente al paso 9.
5. En la página Crear certificado, seleccione **Certificado de usuario** y pulse **Continuar**.
6. En la página Crear certificado de usuario, especifique los campos necesarios para la información del certificado y pulse **Continuar**.
7. En la ventana Violación potencial de scripts, pulse **Sí**.
8. En la página Crear certificado de usuario, pulse **Aceptar**. El sistema utilizará el certificado de usuario del cliente.
9. Expanda **Gestionar aplicaciones** → **Actualizar asignación de certificado** y seleccione **Certificado de servidor o de cliente**.
10. En la página Actualizar asignación de certificado, seleccione **Cliente** y pulse **Continuar**.
11. Seleccione **Cliente TCP/IP de i5/OS** y pulse el botón **Actualizar asignación de certificado**.

| **Instalar el certificado de la entidad emisora de certificados (CA) del receptor en el sistema del remitente.:**

| Si el certificado digital del receptor lo ha emitido una entidad emisora de certificados (CA) desconocida para el sistema del remitente, instale el certificado digital correspondiente a la entidad emisora de certificados en el sistema del remitente.

| **Exportar el certificado de CA local y enviarlo al sistema del remitente**

| Se supone que la entidad emisora de certificados es local; sin embargo, puede utilizar este procedimiento para exportar cualquier certificado de CA que sea desconocido para el sistema del remitente.

| Para exportar el certificado de CA local, siga estos pasos:

- | 1. Pulse **Seleccionar un almacén de certificados** y seleccione **Entidad emisora de certificados (CA) local**. Pulse **Continuar**.
- | 2. En la página Almacén de certificados y contraseña, teclee la contraseña.
- | 3. Expanda **Gestionar CA local** → **Exportar** y seleccione **Archivo - Exportar a un archivo**. Pulse **Continuar**.
- | 4. En la página Exportar certificado, teclee el directorio y la ubicación del nombre de archivo donde se almacenará el certificado de la CA. Si todavía no existe un directorio, utilice el mandato mkdir para crear uno.
- | 5. En la página Exportar certificado satisfactoriamente, pulse **Aceptar**.
- | 6. Utilice FTP en modalidad ASCII para enviar el certificado de CA del sistema receptor al sistema emisor.

| **Instalar el certificado de la CA en el sistema emisor**

- | 1. En la página Seleccionar un almacén de certificados, seleccione ***SYSTEM** y pulse **Continuar**.
- | 2. En la página Almacén de certificados y contraseña, teclee la contraseña y pulse **Continuar**.
- | 3. Expanda **Gestionar certificados** → **Importar certificados**, seleccione **Entidad emisora de certificados (CA)** y pulse **Continuar**.
- | 4. En la página Importar certificado de entidad emisora de certificados (CA), teclee el directorio en donde está almacenado el certificado de CA del destinatario. Pulse **Continuar**.
- | 5. Asigne una etiqueta de certificado al certificado y pulse **Continuar**. Se muestra un mensaje como este:
El certificado se ha importado.
- | 6. Pulse **Aceptar**.

Configurar el servidor de protocolo de oficina postal (POP)

Debe configurar el servidor de protocolo de oficina postal (POP) si desea utilizarlo para entregar mensajes de correo a los clientes POP.

El servidor POP entrega correo a un cliente POP desde el buzón del usuario, cuando este lo solicita. Debe configurar el servidor POP para que el sistema esté completamente preparado para correo electrónico.

Para configurar el servidor POP para un programa de correo, como Netscape Mail o Eudora Pro, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **POP**.
3. Consulte la tabla siguiente para establecer los valores de los campos.

Pulse esta pestaña	Y realice la siguiente acción
General	Seleccione Iniciar cuando se inicia TCP/IP .

Pulse esta pestaña	Y realice la siguiente acción
General	Si desea autorizar ambos tipos de sesiones (sesiones TLS/SSL y sesiones POP no seguras), seleccione Tanto seguro como no seguro para el campo Soporte de capa de sockets que se iniciará con el servidor .
Configuración	Seleccione Sin máximo para el campo Tamaño de división de mensaje .
Configuración	Si los clientes POP inician sesión a través de líneas de acceso telefónico y reciben fragmentos grandes de correo, aumente el Valor de tiempo de espera de inactividad .
Correlaciones	Seleccione Utilizar solo cuando se indica CCSID no soportado .

4. Pulse **Aceptar** para aceptar los cambios.

Asociar un certificado al servidor de protocolo de oficina postal (POP):

Realice esta tarea si no ha asignado un certificado a la aplicación del servidor de protocolo de oficina postal (POP) durante la creación de la entidad emisora de certificados (CA) local o si ha configurado su sistema para que solicite un certificado de una CA pública.

1. Inicie IBM Digital Certificate Manager. Si necesita obtener o crear certificados, o bien establecer o cambiar su sistema de certificados, hágalo ahora. Para obtener más información sobre cómo configurar un sistema de certificados, consulte: Configurar DCM.
2. Pulse **Seleccionar un almacén de certificados**.
3. Seleccione ***SYSTEM**. Pulse **Continuar**.
4. Teclee la contraseña pertinente para el almacén de certificados ***SYSTEM**. Pulse **Continuar**.
5. Cuando se recargue el menú de navegación de la izquierda, expanda **Gestionar aplicaciones**.
6. Pulse **Actualizar asignación de certificados**.
7. Seleccione **Aplicación de servidor**. Pulse **Continuar**.
8. Seleccione **Servidor POP TCP/IP de i5/OS**.
9. Pulse **Actualizar asignación de certificado** para asignar un certificado a este servidor POP.
10. Seleccione un certificado en la lista para asignarlo al servidor.
11. Pulse **Asignar certificado nuevo**.
12. Cuando termine de configurar los certificados para el servidor POP, pulse **Terminado**.

Inscribir usuarios de correo electrónico

Debe crear perfiles de usuario para inscribir usuarios de correo electrónico.

Los perfiles de usuario indican qué hace el sistema operativo i5/OS para identificar un destinatario o un remitente de correo electrónico. Todos los usuarios que desea que formen parte del sistema de correo electrónico deben tener un perfil de usuario en el sistema.

Al crear un perfil de usuario para cada usuario, los inscribe automáticamente al directorio de distribución del sistema. El protocolo simple de transferencia de correo (SMTP) utiliza el directorio de distribución del sistema para determinar dónde hay que entregar el correo electrónico local.

Para crear perfiles de usuario para usuarios de correo electrónico de los servicios de distribución de arquitectura de sistemas en red (SNADS) y del protocolo de oficina postal (POP), siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Usuarios y grupos**.
2. Pulse **Todos los usuarios** con el botón derecho del ratón y seleccione **Usuario nuevo**.
3. Escriba un nombre de usuario y su contraseña.

Nota: Los usuarios de POP utilizan esta contraseña para acceder a sus buzones de POP.

4. Pulse el botón **Posibilidades**.
5. Pulse la pestaña **Privilegios**. Asegúrese de que la clase de privilegio es **Usuario**.
6. Pulse **Aceptar**.
7. Pulse el botón **Personal**.
8. Pulse la pestaña **Correo**.
9. Elija el **Nivel de servicio de correo**.
 - Si es un usuario de SNADS, seleccione **Índice de usuarios**.
 - Si es un usuario de correo POP3, seleccione **Buzón de correo del sistema**.
10. Elija **Tipo de dirección preferida**.
 - Si es un usuario de SNADS, seleccione **ID de usuario y dirección**.
 - Si es un usuario de correo POP3, seleccione **Nombre SMTP**.
11. Verifique que se muestra el nombre de dominio necesario para el dominio de correo electrónico de SMTP. Generalmente, el nombre predeterminado es correcto, pero si tiene múltiples dominios locales es posible que deba cambiarlo.
12. Pulse **Aceptar**. Si está inscribiendo un usuario de SNADS, la inscripción ha finalizado. Si está inscribiendo un usuario de POP que utilizará el servidor POP de i5/OS solo para recuperar correo electrónico, siga en el próximo paso.
13. Pulse el botón **Trabajos**.
14. Pulse la pestaña **Inicio de sesión**.
15. Para el campo **Menú inicial**, seleccione **Finalizar sesión**. Con esta configuración, cualquier intento de iniciar sesión en el sistema, que no sea para recuperar correo electrónico o para cambiar una contraseña, finaliza automáticamente la sesión del usuario.
16. Pulse **Aceptar**.
17. Pulse **Aceptar**.
18. Repita estas instrucciones hasta que todos los usuarios de correo electrónico dispongan de perfiles de usuario.

Conceptos relacionados

“Enviar y recibir correo electrónico” en la página 32

Su sistema es un servidor de correo y tiene usuarios de correo electrónico (usuarios de SNADS, POP o Lotus) inscritos en él. Los usuarios de correo electrónico pueden enviar, recibir y leer correo electrónico utilizando un cliente POP o un cliente SNADS.

Tareas relacionadas

“Enviar correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)” en la página 35

Puede enviar correo electrónico desde su sistema usando el programa de cliente de servicios de distribución de arquitectura de sistemas en red (SNADS). El remitente del correo electrónico debe ser un usuario local de SNADS.

Iniciar y detener los servidores de correo electrónico

Inicie los servidores necesarios para asegurarse de que todo funciona como es debido y de que todos los cambios de configuración que realizó entran en vigor. A veces, podría ser necesario reiniciar los servidores. Puede hacerlo deteniendo los servidores y luego siguiendo los pasos para volver a iniciarlos.

Tareas relacionadas

“Comprobar servidores de correo electrónico” en la página 38

Uno de los problemas más comunes en relación al correo electrónico es que no se inician los correspondientes servidores. Antes de utilizar los servidores de correo electrónico, debe verificar su estado y asegurarse de que todos ellos se están ejecutando.

Iniciar los servidores de correo electrónico

Puede iniciar los servidores y hacer que el sistema sea un servidor de correo electrónico con usuarios de correo electrónico inscritos.

Para iniciar los servidores, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**. Se abre el diálogo Propiedades de configuración de TCP/IP.
 - Si el estado de TCP/IP es Iniciado, pulse **Aceptar** y vaya al paso siguiente.
 - Si no es así, pulse **Cancelar** para cerrar el diálogo Propiedades de configuración de TCP/IP; luego pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Iniciar**. Cuando haya terminado, pulse **Aceptar**.
3. Expanda **Servidores** → **TCP/IP**. Si los servidores SMTP y POP no se han iniciado, siga estos pasos para iniciarlos:
 - a. Pulse **SMTP** con el botón derecho del ratón y seleccione **Iniciar**.
 - b. Pulse **POP** con el botón derecho del ratón y seleccione **Iniciar**.
4. Para iniciar la infraestructura de servidor de correo (MSF), abra una interfaz basada en caracteres y escriba STRMSF.
5. Si utiliza SNADS, escriba STRSBS QSNADS para iniciar el subsistema QSNADS.

Ha iniciado los servidores y ahora el sistema ejecuta un servidor de correo electrónico con usuarios de correo electrónico inscritos.

Detener los servidores de correo electrónico

Puede utilizar System i Navigator para detener los servidores de correo electrónico.

Para detener los servidores, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**. Si los servidores SMTP y POP ya se han iniciado, siga estos pasos para detenerlos:
 - a. Pulse **SMTP** con el botón derecho del ratón y seleccione **Detener**.
 - b. Pulse **POP** con el botón derecho del ratón y seleccione **Detener**.
2. Para detener la infraestructura del servidor de correo, abra la interfaz basada en caracteres y escriba ENDMSF.
3. Si utiliza SNADS, escriba ENDSBS QSNADS para finalizar el subsistema QSNADS.

Configurar un perfil de conexión de correo por acceso telefónico

Si no dispone de soporte de AT&T Global Network, primero debe configurar un perfil de conexión de correo.

Para crear un perfil de conexión por línea telefónica de forma manual, siga estos pasos:

Nota: Si dispone de soporte de AT&T Global Network, puede saltarse el paso del asistente Configurar la conexión por línea telefónica de ISP.

1. En System i Navigator, expanda *su sistema* → **Red** → **Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión de receptor** con el botón derecho del ratón y seleccione **Perfil nuevo**.
3. Seleccione **PPP** para el **Tipo de protocolo**.
4. Seleccione **Línea conmutada** para **Tipo de conexión**.
5. Expanda **Configuración de TCP/IP** y seleccione **Conexiones**.
6. Expanda **Servidores** → **TCP/IP**.
7. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.

8. Pulse la pestaña **Planificador**. Marque el recuadro de selección **Iniciar el planificador al iniciar SMTP** y especifique el perfil de conexión que ha creado.
9. Pulse la página ETRN y marque el recuadro de selección **Soportar ETRN (Recuperación de correo por acceso telefónico)**. Pulse **Añadir** para especificar el nombre de dominio para la dirección del servidor de correo saliente del ISP.
10. Habilite el cortafuegos y señale hacia al servidor de correo saliente del proveedor de servicios de Internet (ISP).
11. Continúe con el asistente para configurar una nueva conexión por línea telefónica de ISP.

Tareas relacionadas

“Asistente para configurar la conexión por línea telefónica de ISP”

Debe configurar un perfil de conexión por línea telefónica antes de utilizar la función del planificador de protocolo simple de transferencia de correo (SMTP) para enviar grandes cantidades de correo electrónico a través de un proveedor de servicios de Internet (ISP).

Asistente para configurar la conexión por línea telefónica de ISP

Debe configurar un perfil de conexión por línea telefónica antes de utilizar la función del planificador de protocolo simple de transferencia de correo (SMTP) para enviar grandes cantidades de correo electrónico a través de un proveedor de servicios de Internet (ISP).

Para configurar el perfil de conexión por línea telefónica de ISP, puede utilizar el asistente de conexión por línea telefónica del proveedor de servicios de Internet (ISP).

Requisitos previos:

Si no tiene soporte de AT&T Global Network, consulte: Configurar un perfil de conexión de correo por acceso telefónico, donde hallará un paso preliminar. El asistente de conexión le proporciona las direcciones IP de los servidores de correo (SMTP y POP), así como el nombre de dominio, el nombre de cuenta y la contraseña asignados a cada uno.

Para ejecutar el asistente y configurar el planificador de SMTP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión de originador** con el botón derecho del ratón y seleccione **Nueva conexión por línea telefónica de AT&T Global Network**.
3. En el panel de bienvenida, pulse **Siguiente** para empezar.
4. En el panel **Tipo de aplicación**, seleccione **Aplicación de intercambio de correo** y pulse **Siguiente**.
5. Continúe con el asistente para configurar una nueva conexión por línea telefónica de AT&T Global Network.

Cuando haya configurado la conexión por línea telefónica, puede planificar trabajos de correo electrónico de ISP por lotes.

Tareas relacionadas

“Configurar un perfil de conexión de correo por acceso telefónico” en la página 22

Si no dispone de soporte de AT&T Global Network, primero debe configurar un perfil de conexión de correo.

“Planificar trabajos de correo electrónico por lotes de ISP” en la página 24

Para limitar el tiempo necesario para establecer una conexión, puede planificar los trabajos de acceso telefónico de correo para que se conecten con el proveedor de servicios de Internet (ISP) a intervalos regulares. Utilice el planificador SMTP para establecer los intervalos de tiempo en los que desea que el sistema se conecte con el ISP y envíe el correo electrónico de la empresa.

Planificar trabajos de correo electrónico por lotes de ISP

Para limitar el tiempo necesario para establecer una conexión, puede planificar los trabajos de acceso telefónico de correo para que se conecten con el proveedor de servicios de Internet (ISP) a intervalos regulares. Utilice el planificador SMTP para establecer los intervalos de tiempo en los que desea que el sistema se conecte con el ISP y envíe el correo electrónico de la empresa.

Requisitos previos:

Utilice el asistente de conexión por línea telefónica de ISP para configurar la conexión.

Para establecer que el planificador de SMTP envíe el correo electrónico a un ISP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **SMTP**.
3. Pulse la pestaña **Planificador**.
4. Marque el recuadro de selección **Iniciar el planificador al iniciar SMTP**.
5. Seleccione el **Perfil de conexión punto a punto** que ha configurado con el asistente de configuración del marcador telefónico de AT&T Global Network, o bien, seleccione un **Perfil de conexión punto a punto** configurado manualmente.
6. Establezca el **Intervalo de transferencia de correo** en los minutos que desea que SMTP tarde en entregar el correo electrónico que se encuentra en la cola.
7. Si el ISP no es AT&T Global Network, marque el recuadro de selección **Emitir ETRN al conectar al servidor remoto**.
8. Teclee la dirección IP del servidor de correo entrante en la red del ISP, y escriba el valor de host.dominio de ISP registrado para el que este servidor SMTP va a emitir un ETRN.
9. Pulse **Aceptar**.

Tareas relacionadas

“Asistente para configurar la conexión por línea telefónica de ISP” en la página 23

Debe configurar un perfil de conexión por línea telefónica antes de utilizar la función del planificador de protocolo simple de transferencia de correo (SMTP) para enviar grandes cantidades de correo electrónico a través de un proveedor de servicios de Internet (ISP).

“Configurar el servidor SMTP para recuperar correo por acceso telefónico”

Puede utilizar el servidor de protocolo simple de transferencia de correo (SMTP) para recibir correo de sucursales remotas por acceso telefónico.

Configurar el servidor SMTP para recuperar correo por acceso telefónico

Puede utilizar el servidor de protocolo simple de transferencia de correo (SMTP) para recibir correo de sucursales remotas por acceso telefónico.

El sistema debe tener una dirección IP fija y estar registrado en un DNS. Cada host.domain (pareja de valores de host y dominio) del que los servidores de acceso telefónico remotos recuperarán correo también debe tener entradas MX en el DNS que señalen hacia este sistema. El sistema también debe tener alias para los valores host.domain en la tabla de hosts local. Si los servidores de acceso telefónico remotos se ejecutan en el sistema operativo i5/OS, deben estar configurados para trabajos de correo electrónico de ISP planificados por lotes.

Para recibir las solicitudes de correo electrónico de los servidores de correo de acceso telefónico remotos, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **SMTP**.
3. Pulse la pestaña **ETRN**.

4. Marque el recuadro de selección **Soportar ETRN (Recuperación de correo por acceso telefónico)**.
5. Pulse **Añadir** para especificar el nombre de dominio y el host del ISP. Puede hacerlo varias veces si hay varios servidores de correo que soliciten su correo.
6. Pulse **Aceptar**.

Tareas relacionadas

“Planificar trabajos de correo electrónico por lotes de ISP” en la página 24

Para limitar el tiempo necesario para establecer una conexión, puede planificar los trabajos de acceso telefónico de correo para que se conecten con el proveedor de servicios de Internet (ISP) a intervalos regulares. Utilice el planificador SMTP para establecer los intervalos de tiempo en los que desea que el sistema se conecte con el ISP y envíe el correo electrónico de la empresa.

Soporte para múltiples dominios

Puede configurar el servidor de protocolo simple de transferencia de correo (SMTP) para que dé soporte a múltiples dominios con el fin de hospedar funciones del proveedor de servicios de Internet (ISP).

Para que el servidor SMTP pueda hospedar funciones del ISP, es necesario que parezca que el SMTP opera en múltiples dominios. El cliente SMTP usa esta información de configuración para saber a qué interfaz se debe enlazar cuando envía correo electrónico y qué correo se debe considerar local (o sea, que debe resolver y enviar por su cuenta) o qué correo debe reenviar a un daemon de correo configurado con cortafuegos.

1. En System i Navigator, expanda *su sistema* → **TCP/IP** → **Red**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la pestaña **Múltiples dominios**.
4. Pulse **Añadir** para especificar los dominios y las interfaces que desea admitir.
5. Pulse **Aceptar**.

Conceptos relacionados

“Prerrequisitos para un direccionador de correo electrónico” en la página 26

En este tema se explica lo que hay que hacer antes de configurar un direccionador de correo electrónico.

Proteger el correo electrónico

Para ayudar a proteger el correo electrónico, puede utilizar cortafuegos, restringir las retransmisiones y las conexiones, y filtrar los virus.

Es importante promocionar un entorno seguro en el servidor de protocolo simple de transferencia de correo (SMTP). Debe proteger el servidor SMTP y también a los usuarios ante los posibles ataques internos y externos.

Conceptos relacionados

“Conceptos relacionados con el correo electrónico” en la página 2

El correo electrónico constituye una herramienta de gestión empresarial esencial. El sistema operativo i5/OS usa protocolos, como el protocolo simple de transferencia de correo (SMTP) y el protocolo de oficina postal (POP), que permiten que el correo electrónico funcione en la red de manera continua y eficaz.

Referencia relacionada

API Crear y enviar correo electrónico MIME (QtmsCreateSendEmail)

Información relacionada

Seguridad en el correo electrónico

Enviar correo electrónico a través de un direccionador o un cortafuegos

El direccionador de correo electrónico es un sistema intermedio al que el servidor de protocolo simple de transferencia de correo (SMTP) entrega el correo cuando no puede localizar la dirección IP exacta del destinatario.

El direccionador de correo electrónico direcciona el correo electrónico a la dirección IP o a otro direccionador. Direcciona el correo electrónico saliente a un sistema alternativo si el servidor local no puede entregar el correo electrónico al sistema. Si tiene un cortafuegos, puede utilizarlo como direccionador.

Antes de seguir estos pasos para configurar un direccionador, consulte: “Prerrequisitos para un direccionador de correo electrónico”.

Para establecer el direccionador, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **SMTP**.
3. Pulse la pestaña **General**.
4. Teclee el nombre del direccionador de correo.

Para direccionar el correo electrónico a través de un cortafuegos, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **SMTP**.
3. Pulse la pestaña **General**.
4. Teclee el nombre del cortafuegos; por ejemplo, FWAS400.company.com en el campo **Direccionador de correo**.
5. Seleccione **Reenviar el correo saliente al direccionador a través del cortafuegos**.

Prerrequisitos para un direccionador de correo electrónico

En este tema se explica lo que hay que hacer antes de configurar un direccionador de correo electrónico.

Antes de configurar un direccionador de correo electrónico, debe tener en cuenta los aspectos siguientes:

- No hace falta que el servidor intermedio tenga el sistema operativo i5/OS. El direccionador de correo solo necesita una tabla de hosts que contenga todos los servidores de hospedaje a los que deba direccionar correo electrónico. Si el sistema operativo i5/OS es el direccionador de correo, no requiere ningún nivel de sistema particular.
- Solo puede configurar un servidor intermedio para direccionar entre el servidor origen y el servidor destino. No puede anidar direccionadores de correo.
- El protocolo simple de transferencia de correo (SMTP) debe poder obtener una dirección IP para el direccionador de correo cuando se inicia, ya sea de la tabla de hosts locales o mediante el servidor de sistema de nombres de dominio (DNS). SMTP, si no puede obtener una dirección IP para el direccionador de correo, se ejecuta sin utilizar un direccionador.
- El soporte de cortafuegos del cliente SMTP utiliza el direccionador de correo para reenviar correo electrónico destinado a un host que se encuentre fuera del dominio local (protegido). Para entregar correo electrónico, el direccionador de correo debe ser un servidor que tenga autorización para reenviar correo electrónico a través del cortafuegos. Además, los destinatarios de correo cuyo dominio no esté en el sistema operativo i5/OS pasan a través del direccionador cuando usted activa el soporte de cortafuegos de SMTP. El sistema operativo i5/OS V5R1 o posterior admite múltiples dominios locales. Puede configurar múltiples dominios que no envíen correo a través del cortafuegos.

Tareas relacionadas

“Soporte para múltiples dominios” en la página 25

Puede configurar el servidor de protocolo simple de transferencia de correo (SMTP) para que dé soporte a múltiples dominios con el fin de hospedar funciones del proveedor de servicios de Internet (ISP).

Autenticar correo electrónico local y para retransmitir

Ahora puede impedir la entrada de correo masivo en el servidor exigiendo autenticación para enviar correo electrónico. No puede exigir autenticación si quiere restringir la retransmisión de mensajes. Le recomendamos que configure la autenticación para su servidor.

Para habilitar la autenticación en el servidor, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **SMTP**.
3. Pulse la pestaña **Autenticación** y establezca los campos según los valores indicados en la columna Y realice la siguiente acción:

Pulse esta pestaña	Y realice la siguiente acción
Autenticación	Si desea que el servidor use TLS/SSL para autenticar localmente y al retransmitir los mensajes, seleccione Requerir TLS/SSL y autenticar localmente y al retransmitir .
Autenticación	Si desea que el servidor use TLS/SL para autenticar solo cuando utiliza la función retransmitir, seleccione Requerir TLS/SSL y autenticar solo al retransmitir .
Autenticación	Si desea permitir que únicamente los usuarios que figuran en la lista de autorizados puedan iniciar sesión en SMTP, seleccione Verificar los ID en las entregas locales .
Autenticación	Si desea que el servidor SMTP permita que las funciones de complemento de la infraestructura del servidor de correo (MSF) rechacen un correo electrónico no verificado, seleccione Verificar originador de mensaje .
Autenticación	Si desea que el servidor SMTP verifique si la dirección de correo electrónico del remitente figura en el directorio de distribución del sistema y si la dirección concuerda, seleccione Usuarios o Usuarios que no están en la lista de aceptados . Se rechazarán los usuarios cuyas direcciones de correo electrónico no concuerden.

4. Pulse **Aceptar** para aceptar los cambios.

Tareas relacionadas

“Restringir la retransmisión de mensajes” en la página 28

Para impedir que otras personas utilicen el servidor de correo electrónico para el correo masivo o para enviar grandes cantidades de mensajes de correo electrónico no deseado, puede utilizar la función de restricción de retransmisión y especificar quién puede usar su sistema para retransmitir mensajes. Sin embargo, cuando restringe la retransmisión de mensajes, no puede autenticar el correo electrónico.

“Configurar el servidor de protocolo simple de transferencia de correo (SMTP)” en la página 17

Cuando configuró TCP/IP, el sistema configuró SMTP automáticamente. Sin embargo, aún debe cambiar algunas propiedades SMTP para asegurarse de que el servidor SMTP funciona correctamente para el correo electrónico.

Rastrear el remitente de correo electrónico

Ahora, puede establecer que el servidor SMTP rechace un remitente de correo electrónico que no esté autenticado. Además, puede establecer que las funciones de complementos de la infraestructura de servidor de correo (MSF) SMTP rechacen un mensaje de correo electrónico que no esté verificado.

Para rechazar un remitente o un mensaje de correo electrónico que no esté verificado, debe habilitar el cifrado de las transacciones, es decir, los protocolos TLS/SSL.

Rechazar un remitente de correo que no esté verificado

- | Para rechazar un remitente de correo electrónico que no esté verificado, siga estos pasos:
- | 1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - | 2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
 - | 3. Pulse la pestaña **Autenticación**.
 - | 4. Si desea verificar todos los remitentes de correo electrónico, vaya al campo **Verificar correo de usuario** y seleccione **Todo**. Si desea verificar solamente los usuarios que no están en la lista de aceptados, seleccione **Usuarios que no están en la lista de aceptados**.
 - | 5. Pulse **Aceptar**.

| El servidor SMTP comprueba si el remitente está en el directorio de distribución del sistema y si la dirección de correo concuerda con la que hay en el directorio. Si hay una discrepancia, el usuario se rechaza.

| **Rechazar un correo electrónico que no esté verificado**

- | Para rechazar un correo electrónico que no esté verificado, siga estos pasos:
- | 1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - | 2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
 - | 3. Pulse la pestaña **Autenticación**.
 - | 4. Seleccione **Requerir TLS/SSL y autenticar localmente y al retransmitir** para el campo **Permitir autenticación**.
 - | 5. Seleccione **Verificar originador de mensaje MSF**.
 - | 6. Pulse **Aceptar**.

| Si el correo electrónico no proviene de una fuente autenticada, el usuario que emitió la API QzmfCrtMailMsg() debe ser el originador del mensaje MSF. De lo contrario, las funciones de complemento de SMTP rechazarán los mensajes de correo electrónico.

Restringir la retransmisión de mensajes

| Para impedir que otras personas utilicen el servidor de correo electrónico para el correo masivo o para enviar grandes cantidades de mensajes de correo electrónico no deseado, puede utilizar la función de restricción de retransmisión y especificar quién puede usar su sistema para retransmitir mensajes. Sin embargo, cuando restringe la retransmisión de mensajes, no puede autenticar el correo electrónico.

Dispone de seis opciones para permitir la retransmisión:

- Permitir todos los mensajes de retransmisión
- Bloquear todos los mensajes de retransmisión
- Aceptar mensajes de retransmisión solo para los destinatarios de la lista de dominios próximos
- Aceptar mensajes de retransmisión que solo procedan de la lista de direcciones de retransmisión
- Aceptar mensajes de retransmisión que utilizan ambas listas, la de dominios próximos y la de direcciones de retransmisión
- Aceptar mensajes de retransmisión procedentes de los clientes POP durante un tiempo especificado

| Ahora puede restringir las retransmisiones solo cuando selecciona la opción **No TLS/SSL y no se hará autenticación**. En System i Navigator, la opción está en la página Autenticación que aparece cuando especifica las propiedades de SMTP.

Para especificar los usuarios que pueden enviar correo electrónico a Internet, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.

3. Pulse la pestaña **Restricciones de retransmisión**.
4. Seleccione la restricción de retransmisión pertinente en la lista de opciones que aquí se ofrecen.

Nota: Si elige **Aceptar mensajes de retransmisión solo para destinatarios de la lista de dominios próximos** o **Aceptar mensajes de retransmisión que utilizan ambas listas de dominios próximos y de direcciones de retransmisión**, debe pulsar la pestaña **General** para obtener una lista de los dominios próximos de los que acepta retransmisiones.

5. Pulse **Aceptar**.

Conceptos relacionados

“Controlar el acceso al correo electrónico” en la página 11

Debe controlar quién accede a su sistema mediante correo electrónico para proteger sus datos de los ataques maliciosos.

Tareas relacionadas

“Autenticar correo electrónico local y para retransmitir” en la página 27

Ahora puede impedir la entrada de correo masivo en el servidor exigiendo autenticación para enviar correo electrónico. No puede exigir autenticación si quiere restringir la retransmisión de mensajes. Le recomendamos que configure la autenticación para su servidor.

“Utilizar conjuntamente las funciones de restricción de retransmisión y de restricción de conexión” en la página 30

El sistema operativo i5/OS le permite utilizar la función restricción de retransmisión junto con la de restricción de conexión para controlar de forma precisa quien puede acceder al servidor de correo electrónico.

Referencia relacionada

Mandato Cambiar atributos de SMTP (CHGSMTPA)

Aceptar mensajes de retransmisión de los clientes de protocolo de oficina postal (POP)

Una de las opciones para restringir las retransmisiones consiste en permitir que los clientes de protocolo de oficina postal (POP) retransmitan mensajes a través del protocolo simple de transferencia de correo (SMTP) durante un tiempo especificado después de que hayan iniciado sesión en el servidor POP.

A esta función se la suele llamar POP antes que SMTP. Es una función especialmente útil en el caso de los empleados móviles que emplean direcciones IP dinámicas, porque las funciones de comprobación de seguridad que utilizan direcciones IP fijas no son eficaces para comprobar las direcciones IP dinámicas. Puede permitir que un empleado móvil se autentique una vez ante el servidor POP y envíe correo electrónico durante un tiempo designado (de 15 a 65535 minutos) sin tener que volver a autenticarse.

Por ejemplo, puede configurar el sistema para que permita que los usuarios remotos retransmitan mensajes a través del servidor SMTP durante cuatro horas (240 minutos) después de que hayan iniciado sesión en el servidor POP. En este ejemplo, un trabajador móvil inicia sesión en el servidor POP para recuperar su correo electrónico. El servidor POP registra la dirección IP del usuario y una indicación horaria en una cola. Una hora más tarde, el usuario decide enviar un mensaje de correo electrónico. Cuando el usuario envía el mensaje de correo electrónico utilizando SMTP, el servidor SMTP comprueba la cola para verificar que el usuario ha accedido al servidor POP para recuperar correo electrónico en algún momento dentro del tiempo configurado. Una vez que se ha verificado el usuario, el servidor SMTP retransmite el mensaje de correo electrónico al cliente SMTP para entregarlo al destinatario de correo electrónico.

Nota: Para controlar de forma más precisa los usuarios que pueden acceder al servidor de correo electrónico, puede utilizar conjuntamente la función de restricción de retransmisión y la función de restricción de conexión. Por ejemplo, quizás desee restringir la conexión de grupos concretos de usuarios al servidor de correo electrónico y a la vez permitir que determinados clientes POP de dicho grupo utilicen el servidor SMTP para enviar mensajes de correo electrónico.

Si desea habilitar clientes POP para que retransmitan mensajes durante un tiempo especificado, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la pestaña **Restricciones de retransmisión**.
4. Para **Permitir retransmitir mensajes**, seleccione **Especificado**.
5. Seleccione **Del cliente POP durante el tiempo siguiente (15 - 65535)** y teclee un valor de tiempo para especificar el número de minutos durante los que un cliente puede enviar correo utilizando el servidor SMTP.
6. Pulse **Aceptar**.

Utilizar conjuntamente las funciones de restricción de retransmisión y de restricción de conexión

El sistema operativo i5/OS le permite utilizar la función restricción de retransmisión junto con la de restricción de conexión para controlar de forma precisa quien puede acceder al servidor de correo electrónico.

Puede restringir la conexión de grupos concretos de usuarios al servidor de correo electrónico y a la vez permitir que determinados clientes de protocolo de oficina postal (POP) de dicho grupo utilicen el servidor SMTP para enviar mensajes de correo electrónico.

Por ejemplo, usted sabe que los usuarios de un rango específico de direcciones IP envían habitualmente correo masivo. Por tanto, desea restringir la conexión de las direcciones de dicho rango a su servidor de correo electrónico. Sin embargo, varias direcciones IP del rango de direcciones IP representan usuarios de i5/OS de confianza y desea permitir que dichos usuarios con perfiles de usuario i5/OS retransmitan mensajes durante un tiempo especificado después de que hayan iniciado sesión en el servidor POP.

Afortunadamente, puede utilizar la función de restricción de conexión para restringir las conexiones de un rango específico de direcciones IP y utilizar la función de restricción de retransmisión para permitir que determinados usuarios de confianza (clientes POP) del rango restringido envíen correo electrónico utilizando el servidor de protocolo simple de transferencia de correo (SMTP). El sistema operativo i5/OS comprueba primero si ha configurado el sistema para permitir que los clientes POP retransmitan mensajes durante un tiempo especificado. A continuación, comprueba las conexiones restringidas. Esta prestación de i5/OS le permite controlar de forma precisa quién puede utilizar el servidor SMTP para retransmitir mensajes y quién puede conectarse al servidor de correo electrónico.

- | Si elige utilizar juntas ambas funciones, la de restricción de conexión y la de restricción de retransmisión, debe especificar OVRRTNNL(*YES) (Alterar temporalmente lista de conexiones rechazadas) en el mandato CL Cambiar atributos de SMTP (CHGSMTPA). Este parámetro habilita la prestación de autenticación del servidor POP para alterar temporalmente la configuración de restricción de conexión.
- | En una fecha posterior, podría interesarle eliminar la restricción de retransmisión que permite a los clientes POP del grupo restringido utilizar el servidor de correo electrónico. En ese caso, debe especificar OVRRTNNL(*NO) en el mandato CHGSMTPA.

Tareas relacionadas

“Restringir la retransmisión de mensajes” en la página 28

Para impedir que otras personas utilicen el servidor de correo electrónico para el correo masivo o para enviar grandes cantidades de mensajes de correo electrónico no deseado, puede utilizar la función de restricción de retransmisión y especificar quién puede usar su sistema para retransmitir mensajes. Sin embargo, cuando restringe la retransmisión de mensajes, no puede autenticar el correo electrónico.

“Restringir conexiones” en la página 31

Para garantizar la seguridad del sistema, debe impedir la conexión de usuarios que podrían abusar del servidor de correo electrónico.

Referencia relacionada

Restringir conexiones

Para garantizar la seguridad del sistema, debe impedir la conexión de usuarios que podrían abusar del servidor de correo electrónico.

Usuarios no deseados podrían conectarse al sistema y enviar correo no solicitado. Este correo electrónico no solicitado ocupa mucho espacio y ciclos de unidad de proceso. Además, si el sistema permite que otros usuarios retransmitan correo no solicitado, otros sistemas podrían bloquear el correo que procede de su sistema.

Puede especificar direcciones IP de usuarios no deseados conocidos, o bien conectarse a un host que contenga un servidor de listas de agujeros negros en tiempo real (RBL). Las listas de agujeros negros en tiempo real proporcionan un listado de las direcciones IP conocidas que envían correo no solicitado.

Para especificar direcciones IP conocidas o un host con una lista de agujeros negros en tiempo real (RBL), siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la página Restricciones de conexión.
4. Pulse **Añadir** para añadir nombres de hosts de los servidores con listas de agujeros negros en tiempo real que desea utilizar.
5. Pulse **Añadir** para añadir direcciones IP específicas que restrinjan las conexiones intentadas.
6. Pulse **Aceptar**.

Conceptos relacionados

“Controlar el acceso al correo electrónico” en la página 11

Debe controlar quién accede a su sistema mediante correo electrónico para proteger sus datos de los ataques maliciosos.

Tareas relacionadas

“Utilizar conjuntamente las funciones de restricción de retransmisión y de restricción de conexión” en la página 30

El sistema operativo i5/OS le permite utilizar la función restricción de retransmisión junto con la de restricción de conexión para controlar de forma precisa quien puede acceder al servidor de correo electrónico.

Filtrar el correo electrónico para impedir la proliferación de virus

Para impedir la propagación de un virus que podría infiltrarse en el servidor de correo electrónico, puede crear filtros que busquen un determinado asunto, tipo, nombre de archivo o dirección del originador en el correo electrónico entrante. Entonces el correo electrónico se puede descartar o poner en cuarentena.

Gracias al filtrado de virus, los mensajes de correo electrónico dudosos se colocan en cuarentena o se descartan automáticamente basándose en los parámetros establecidos por el administrador. Los mensajes de correo electrónico se pueden filtrar según uno o todos los criterios siguientes:

1. **Dirección**-individuar o de dominios
2. **Asunto** - ILOVEYOU
3. **Nombre de archivo adjunto** - lovebug.vbs o *.vbs
4. **Tipo MIME** - image/* o image/jpg

Los valores pueden contener caracteres comodín. Un carácter comodín es un asterisco (*), que especifica que puede haber uno o más caracteres arbitrarios en la posición del comodín. Por ejemplo, se puede

utilizar *.vbs para comprobar nombres de archivo con una extensión .vbs. Un originador de *@us.ibm.com filtra todo el correo de IBM en los Estados Unidos y un filtro image/* filtra la imagen de tipo para todos los subtipos.

Para crear un filtro, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Seleccione la página Filtros.
4. Seleccione **Conservar el mensaje** o **Descartar el mensaje**. Si selecciona **Conservar el mensaje**, se guarda una copia del mensaje, que no se entrega al destinatario.
5. Pulse **Añadir** para especificar los criterios de mensajes que identifiquen el posible virus. Los mensajes que coincidan con estos criterios no se entregarán al destinatario.
6. Pulse **Aceptar** para guardar los cambios.

Además de estas herramientas, debe implementar soluciones antivirus adicionales.

Enviar y recibir correo electrónico

Su sistema es un servidor de correo y tiene usuarios de correo electrónico (usuarios de SNADS, POP o Lotus) inscritos en él. Los usuarios de correo electrónico pueden enviar, recibir y leer correo electrónico utilizando un cliente POP o un cliente SNADS.

- | Los usuarios pueden utilizar la API Enviar correo MIME (QtmmSendMail) o la API Crear y enviar correo electrónico MIME (QtmsCreateSendEmail) para enviar correo electrónico desde un programa de i5/OS.
- | Con la API QtmsCreateSendEmail, los usuarios pueden firmar y cifrar el documento MIME mediante secure/MIME, que es una versión segura del protocolo MIME. La API QtmsCreateSendEmail es la forma preferida de enviar correo electrónico programáticamente.
- | Además, los usuarios pueden enviar y recibir correo electrónico de las formas siguientes.

Conceptos relacionados

“Conceptos relacionados con el correo electrónico” en la página 2

El correo electrónico constituye una herramienta de gestión empresarial esencial. El sistema operativo i5/OS usa protocolos, como el protocolo simple de transferencia de correo (SMTP) y el protocolo de oficina postal (POP), que permiten que el correo electrónico funcione en la red de manera continua y eficaz.

Tareas relacionadas

“Inscribir usuarios de correo electrónico” en la página 20

Debe crear perfiles de usuario para inscribir usuarios de correo electrónico.

Referencia relacionada

API Crear y enviar correo electrónico MIME (QtmsCreateSendEmail)

API Enviar correo MIME (QtmmSendMail)

Configurar clientes de correo electrónico de protocolo de oficina postal (POP)

Si desea recibir y almacenar mensajes de correo electrónico utilizando el servidor de protocolo de oficina postal (POP), primero debe configurar un cliente de correo electrónico.

- | El sistema utiliza el servidor POP para almacenar y reenviar correo electrónico. El cliente de correo electrónico trabaja con el servidor POP para recibir y almacenar mensajes de correo electrónico para los usuarios en el lado del cliente. Hay varios clientes de correo electrónico disponibles con soporte de POP, entre ellos están Eudora, Outlook Express y Lotus Notes. Los pasos que debe llevar a cabo para

configurar el cliente son específicos de la interfaz del cliente. Sin embargo, siempre debe proporcionar la misma información. Este es un ejemplo de los pasos que debe seguir si utiliza Outlook Express:

1. Reúna la información del programa cliente de correo electrónico POP.
 - ID de usuario y nombre de dominio completo (el nombre de host más el nombre de dominio). Es la dirección de correo electrónico del usuario para recibir correo y, por lo general, tiene el formato: IDusuario@nombreHost.nombreDominio.

Nota: En algunos clientes, es posible que deba entrar la dirección de host varias veces: al especificar el host del servidor POP para recibir correo, al especificar el host de SMTP para enviar correo, y al identificar el remitente del correo electrónico ante los destinatarios.

 - Nombre de cuenta o usuario de POP. Es el mismo nombre que el del perfil de usuario de i5/OS.
 - La contraseña de usuario. Esta contraseña debe ser igual a la contraseña del perfil de usuario de i5/OS.
2. Identifique el usuario y sus preferencias. En Outlook Express, por ejemplo, pulse **Herramientas** → **Cuentas**, y luego pulse la pestaña **Correo** para identificar la información acerca del usuario y de las preferencias del usuario.
 - Nombre de usuario. Es el nombre del perfil de usuario de i5/OS.
 - Dirección de correo electrónico del usuario. Es el ID de usuario y el nombre de dominio completo.
 - Dirección de respuesta. Puede coincidir con la dirección de correo electrónico del usuario designada por el administrador de la red, pero en el sistema debe existir un perfil de usuario de i5/OS.
3. Identifique el servidor de correo saliente (SMTP). Debe identificar el servidor SMTP en el cliente de correo electrónico, puesto que es el servidor que permite que los usuarios del cliente puedan enviar correo. En Outlook Express, por ejemplo, pulse **Herramientas** → **Cuentas**, seleccione la cuenta de correo electrónico y pulse **Propiedades**. Pulse la pestaña **Servidores** e identifique el servidor SMTP.
 - Nombre de cuenta o usuario de POP. Es el ID de usuario en la dirección de correo electrónico del usuario; y también es el nombre del perfil de usuario de i5/OS.
 - Servidor de correo saliente (SMTP). Es el nombre de host del sistema.
4. Identifique el servidor de correo entrante (POP). En Outlook Express, por ejemplo, pulse **Herramientas** → **Cuentas**, seleccione las cuentas de correo electrónico y pulse **Propiedades**. Pulse la pestaña **Servidores** e identifique el servidor POP.
 - Servidor de correo entrante. Es el nombre de host del sistema.
5. Configure el programa del cliente para que utilice TLS/SSL. En Outlook Express, por ejemplo, siga estos pasos de configuración:
 - a. Pulse **Herramientas** → **Cuentas** y seleccione la cuenta de correo electrónico.
 - b. Pulse **Propiedades** y luego la pestaña **Servidores**.
 - c. Seleccione **Mi servidor requiere autorización** y pulse **Configuración**.
 - d. Seleccione **Usar misma configuración que el servidor de correo entrante** y pulse **Aceptar**.
 - e. Pulse la pestaña **Opciones avanzadas** y seleccione **El servidor requiere una conexión segura (SSL)** para ambos servidores, el de correo entrante (POP) y el de correo saliente (SMTP). Pulse **Aceptar**.
 - f. Pulse **Aplicar** y luego **Aceptar** para cerrar la ventana Propiedades.

JavaMail

JavaMail le permite desarrollar aplicaciones de cliente de correo electrónico.

La API JavaMail proporciona una infraestructura independiente de la plataforma y del protocolo que se puede utilizar para crear aplicaciones de cliente de correo electrónico basadas en tecnología Java. Puede utilizar la API JavaMail para crear un cliente de correo capaz de enviar mensajes de correo multimedia, así como de habilitar la implementación del protocolo de acceso a correo de Internet (IMAP) que permite manejar archivos adjuntos, la autenticación y carpetas.

SMTP, dado que solo soporta datos de tipo carácter, utiliza MIME para representar datos complejos como el texto formateado, archivos adjuntos (de texto y binarios) y contenido multimedia. Si utiliza la API Enviar correo MIME (QtmmSendMail), la aplicación debe convertir los datos en el contenido pertinente. La implementación JavaMail proporciona prestaciones de proceso MIME integradas.

Los componentes de JavaMail se incluyen como parte de IBM Developer Kit para Java.

Conceptos relacionados

JavaMail

Enviar archivos en spool como archivos PDF

Puede enviar archivos en spool con formato de documento portable (PDF) de Adobe y distribuir los documentos por correo electrónico.

Mediante el programa bajo licencia IBM Infoprint Server para iSeries (5722-IP1), puede producir archivos PDF de Adobe a partir de cualquier tipo de datos de salida de i5/OS. Puede enviar los archivos PDF generados como archivos adjuntos de correo electrónico. Puede enviar un solo archivo en spool a una dirección. También puede dividir un archivo en spool en varios archivos PDF y enviar cada uno de ellos a una dirección diferente. Este método le permite enviar facturas de clientes a archivos PDF aparte y enviar la factura pertinente a la dirección de correo electrónico de cada cliente. Se necesita el programa bajo licencia IBM Infoprint Server para iSeries para poder utilizar este método de salida.

Información relacionada



InfoPrint Server User's Guide, PDF



IBM eServer iSeries Printing Redbooks VI -- The Output of e-business

Utilizar el protocolo ligero de acceso a directorio (LDAP) para las direcciones

Puede utilizar el protocolo ligero de acceso a directorio (LDAP) para proporcionar una libreta de direcciones pública basada en el directorio de distribución del sistema.

- | Puede utilizar IBM Tivoli Directory Server para i5/OS (que es la implementación IBM de LDAP) en
- | sustitución de la función que anteriormente servía MAPI. Mediante LDAP, puede proporcionar una sola
- | libreta de direcciones a la que pueden acceder todos los usuarios desde la aplicación cliente.

Para utilizar LDAP, realice estas tareas:

1. Inicie el servidor de directorio.
2. Publique información en el servidor de directorio.
3. Configure el cliente de correo para que utilice LDAP. Los pasos que debe llevar a cabo para completar esta tarea varían en función del cliente de correo (Netscape o Eudora, por ejemplo). Edite las propiedades del cliente de correo para que especifique el servidor LDAP como servidor de directorio para el sistema de direcciones de correo.

Tareas relacionadas

Guía de inicio del Servidor de Directorio

Publicar información en el servidor de directorio

Referencia relacionada

IBM Tivoli Directory Server para i5/OS (LDAP)

Enviar correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)

Puede enviar correo electrónico desde su sistema usando el programa de cliente de servicios de distribución de arquitectura de sistemas en red (SNADS). El remitente del correo electrónico debe ser un usuario local de SNADS.

Requisitos previos

Un usuario local de SNADS debe tener un perfil de usuario para inscribirse en la entrada del directorio de distribución del sistema local. Para inscribir a los usuarios de correo electrónico locales de SNADS, consulte: Inscribir usuarios de correo electrónico.

Para enviar correo electrónico, siga estos pasos:

1. En la interfaz basada en caracteres de i5/OS teclee SNDDST (mandato Enviar distribución) y pulse Intro.
2. Pulse la tecla F10 para ver todos los parámetros.
3. En la primera solicitud, *Información a enviar*, teclee *LMSG y pulse Intro.
4. Entre el ID de usuario del destinatario y la dirección del servidor o una dirección Internet.
5. En la solicitud *Descripción*, entre una descripción de mensaje.
6. Pulse la tecla AvPág y escriba el correo electrónico en la solicitud *Mensaje largo*.
7. Pulse Intro para enviar el correo electrónico.

Nota: También puede utilizar el sistema de direcciones de Internet cuando envíe correo con el mandato Enviar distribución (SNDDST).

Tareas relacionadas

“Inscribir usuarios de correo electrónico” en la página 20

Debe crear perfiles de usuario para inscribir usuarios de correo electrónico.

“Recibir correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)” en la página 37

Puede recibir correo electrónico en su sistema utilizando un programa cliente de servicios de distribución de arquitectura de sistemas en red (SNADS). El destinatario del correo electrónico debe ser un usuario local de SNADS.

Configurar cabeceras para diferenciar entre destinatarios

El mandato Cambiar atributos de distribución (CHGDSTA) cambia el contenido de los atributos de servicios de mensajes (soporte X.400) para las distribuciones de correo.

El parámetro Mantener destinatario (KEEPRCP) especifica qué información de destinatario se almacena y se envía en cada distribución de correo. El establecimiento de este parámetro afecta a cómo se crean las cabeceras MIME para una nota de SNDDST.

Para que se muestren los códigos CC y BCC en las cabeceras MIME (y en las pantallas de los clientes), debe establecer el parámetro KEEPRCP en *ALL. Aunque se establezca este parámetro, los destinatarios de BCC no se muestran, puesto que su propósito es que no se muestren. Los destinatarios de PARA y CC se muestran en el texto de la nota de SNDDST.

Tipos de contenido MIME (Multipurpose Internet Mail Extensions)

Las notas de texto Internet estándar constan de una cabecera general y un cuerpo de texto. Sin embargo, las notas MIME (Multipurpose Internet Mail Extensions) pueden contener múltiples partes, que permiten incluir archivos multimedia adjuntos con el texto.

Información relacionada

 Redbook AS/400 Electronic-Mail Capabilities

Adjuntar archivos

Al enviar correo electrónico utilizando el mandato SNDDST, es posible que le interese enviar un fichero o un documento con el correo electrónico.

Puede enviar correo electrónico con un archivo o un documento adjunto si utiliza el mandato Enviar distribución (SNDDST). SNDDST solo puede enviar un único documento o archivo al mismo tiempo. Si desea enviar varios documentos o archivos adjuntos, envíe correo MIME con la API Enviar correo MIME (QtmmSendMail).

Para adjuntar y enviar un *documento* con el correo electrónico, en la interfaz basada en caracteres, escriba:
SNDDST TYPE(*DOC) DSTD(*descripción*) TOUSRID(*usuario*) DOC(*documento*) FLR(*carpeta*)

Para adjuntar y enviar un *archivo* con el correo electrónico, en la interfaz basada en caracteres, escriba:
SNDDST TYPE(*FILE) DSTD(*descripción*) TOUSRID(*usuario*)
MSG(*mensaje opcional*) DOCTYPE(*bibl/archivo*) DOCMBR(*miembro*)

Si recibe mensajes de error, es posible que esté intentando enviar un archivo o un documento con un formato incompatible con el mandato Enviar distribución (SNDDST). Puede utilizar los mandatos CL COPY de i5/OS para convertir el archivo en un archivo o documento que sea compatible con el mandato SNDDST.

Convertir tipos de archivo para enviarlos con SNDDST

Dando por supuesto que el archivo en spool se ha creado previamente y que el archivo físico y la carpeta ya existen, debe convertir el archivo a un formato que se pueda enviar.

1. Mueva el archivo en spool a un archivo físico de base de datos:
CPYSPLF FILE(*archivospool*) TOFILE(*archivoBD*) JOB(*trabajo3/trabajo2/trabajo1*) SPLNBR(*númerosp1*) TOMBR(*miembro*)
2. Mueva el archivo físico de base de datos a una carpeta:
CPYTOPCD FROMFILE(*bibl/archivoBD*) TOFLR(*carpeta*) FROMMBR(*miembro*) REPLACE(*YES)
3. Envíe el documento:
SNDDST TYPE(*DOC) TOUSRID(*direcciónUsuario*) DSTD(MAIL) DOC(*miembro*) FLR(*carpeta*)

Referencia relacionada

API Enviar correo MIME (QtmmSendMail)

Recibir correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)

Puede recibir correo electrónico en su sistema utilizando un programa cliente de servicios de distribución de arquitectura de sistemas en red (SNADS). El destinatario del correo electrónico debe ser un usuario local de SNADS.

Para recibir correo electrónico, siga este procedimiento.

1. En la interfaz basada en caracteres, escriba QRYDST (mandato Consultar distribución) y pulse la tecla F4. Se muestra la lista de distribuciones.
2. Pulse la tecla F10 para ver parámetros adicionales.
3. En el campo **Archivo en el que recibir la salida**, escriba nombres de archivo y biblioteca que sean fáciles de recordar y pulse Intro. El sistema crea estos archivos físicos.
4. Escriba WRKF (mandato Trabajar con archivos) y pulse Intro. Se muestra la pantalla Trabajar con archivos.

5. Escriba el nombre de archivo y la biblioteca que especificó en el paso 3 y pulse la tecla F4.
6. En la pantalla aparece una lista de todas las distribuciones (correo electrónico). Teclee 5 junto a la distribución que desea visualizar y pulse Intro.
7. En la pantalla Visualizar miembro de archivo físico (DSPPFM), pulse Intro.
8. En la pantalla siguiente, se muestra una larga serie de números para cada fragmento de correo. Copie del séptimo al vigésimo sexto carácter.
9. Pulse dos veces la tecla F3 para salir.
10. Escriba RCV DST (mandato Recibir distribución) y pulse Intro.
11. En el campo **Identificador de distribución**, pegue del séptimo al vigésimo sexto carácter que ha copiado.
12. En el campo **Archivo en el que recibir la salida**, escriba un nuevo nombre de archivo y el mismo nombre de biblioteca que utilizó anteriormente y pulse Intro.
13. Escriba DSPPFM (Visualizar miembro de archivo físico) para ver el archivo que acaba de crear.
14. Pulse F20 (Mayús + F8) para desplazarse a la izquierda y leer los mensajes.

Tareas relacionadas

“Enviar correo electrónico utilizando los servicios de distribución de arquitectura de sistemas en red (SNADS)” en la página 35

Puede enviar correo electrónico desde su sistema usando el programa de cliente de servicios de distribución de arquitectura de sistemas en red (SNADS). El remitente del correo electrónico debe ser un usuario local de SNADS.

Gestionar el correo electrónico

Como usuario o administrador con experiencia, puede gestionar servidores, usuarios y mensajes de correo electrónico para asegurar la distribución de correo electrónico en la red.

Comprobar servidores de correo electrónico

Uno de los problemas más comunes en relación al correo electrónico es que no se inician los correspondientes servidores. Antes de utilizar los servidores de correo electrónico, debe verificar su estado y asegurarse de que todos ellos se están ejecutando.

Para verificar el estado de los servidores, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Gestión del trabajo** → **Trabajos servidores**.
2. Verifique que el servidor SMTP está activo. Busque los trabajos **Qtsmtp** en la columna Nombre de trabajo de la lista Trabajos de servidor activos.
3. Si en la lista no figura ningún trabajo **Qtsmtp**, inicie los servidores SMTP.
4. Verifique que el servidor de la infraestructura de servidor de correo (MSF) está activo. Busque los trabajos **Qmsf** en la columna Nombre de trabajo de la lista Trabajos de servidor activos.
5. Si no hay ningún trabajo **Qmsf** en la lista, teclee STRMSF (mandato Iniciar la infraestructura de servidor de correo) en la interfaz basada en caracteres.
6. Verifique que el servidor POP está activo. Busque los trabajos **Qtpop** en la columna Nombre de trabajo de la lista Trabajos de servidor activos.
7. Si no hay trabajos **Qtpop** en la lista, inicie los servidores POP.
8. Verifique que el servidor SNADS está activo. Busque los trabajos **Qsnads** en la columna Nombre de trabajo de la lista Trabajos de servidor activos.
9. Si no hay trabajos **QSNADS** en la lista, inicie SNADS. En la interfaz basada en caracteres, escriba STRSBS QSNADS.

Para que el correo electrónico funcione, hay que iniciar todos los servidores de correo electrónico.

Conceptos relacionados

“Iniciar y detener los servidores de correo electrónico” en la página 21

Inicie los servidores necesarios para asegurarse de que todo funciona como es debido y de que todos los cambios de configuración que realizó entran en vigor. A veces, podría ser necesario reiniciar los servidores. Puede hacerlo deteniendo los servidores y luego siguiendo los pasos para volver a iniciarlos.

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Eliminar usuarios de correo electrónico de protocolo de oficina postal (POP)

Puede eliminar usuarios de correo electrónico de protocolo de oficina postal (POP) utilizando System i Navigator.

Para eliminar un usuario de correo electrónico del sistema operativo, debe suprimir esta entrada del directorio de distribución del sistema, como se indica a continuación:

1. En la interfaz basada en caracteres, escriba WRKDIRE (mandato Trabajar con entradas de directorio).
2. Desplácese hacia abajo hasta situarse en el campo *Opc*, junto al usuario que desea eliminar.
3. Teclee un 4 (Eliminar) y pulse Intro. Vuelva a pulsar Intro para confirmar. De este modo, se impide la entrega de más correo electrónico al buzón POP del usuario.
4. Inicie sesión en un programa cliente de correo POP como dicho usuario. Reciba y suprima todo el correo electrónico.

Impedir que se dividan os mensajes de correo electrónico largos

Es posible que tenga que impedir que los mensajes largos de correo electrónico se dividan y se entreguen en fragmentos más pequeños, que puedan llevar a confusión.

El protocolo simple de transferencia de correo (SMTP) se puede configurar para que divida los mensajes largos en fragmentos más pequeños. Sin embargo, muchos clientes de correo no pueden volver a reunir los fragmentos, y los mensajes resultan ilegibles. Si los destinatarios no pueden leer mensajes largos debido a que están divididos en varios fragmentos, le interesará inhabilitar la función de división de SMTP.

Para inhabilitar la división de correo electrónico de SMTP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **POP**. Se muestra el diálogo Propiedades de POP.
3. Pulse la pestaña **Configuración**.
4. Para el campo **Tamaño de división de mensaje**, seleccione **Sin máximo**.

Nota: El hecho de desactivar esta función podría causar problemas al enviar mensajes de correo electrónico largos a redes que no pueden manejar mensajes largos.

Conceptos relacionados

“Resolver problemas relacionados con el correo electrónico” en la página 51

Esta información está pensada para ayudarle a resolver problemas que puedan surgir en relación con el correo electrónico.

Recibir estado de entrega de correo electrónico

Si los usuarios desean recibir mensajes sobre el estado de entrega de su correo electrónico saliente, debe habilitar la función de notificación del estado de entrega.

La notificación del estado de entrega permite que los clientes de correo electrónico reciban mensajes de estado cuando el correo electrónico se entrega, retransmite o falla. Si desea permitir que los clientes de correo electrónico hagan esta solicitud, debe habilitar la función de notificación del estado de entrega.

Solo va a habilitar la función de notificación del estado de entrega para sus usuarios. Si los usuarios quieren utilizar la función de notificación del estado de entrega, deben establecer los parámetros pertinentes en sus clientes de correo. Los parámetros varían de un cliente de correo a otro.

Para habilitar la notificación del estado de entrega, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la página Parámetros adicionales.
4. Marque el recuadro de selección **Soporte de notificación de estado de entrega (DSN)** y especifique Dirección de la persona responsable de la notificación DSN.
5. Pulse **Aceptar**.

Al utilizar la función de notificación del estado de entrega, se consumen recursos que pueden afectar al número máximo de destinatarios de un elemento de correo electrónico.

Hospedar un servidor Domino y un servidor SMTP en el mismo sistema

Si ejecuta Domino y el protocolo simple de transferencia de correo (SMTP) en el mismo sistema, le sugerimos que configure cada uno para que se enlace a una dirección IP específica.

Cuando hospeda un servidor Domino y un servidor SMTP en el mismo sistema, debe enlazar cada servidor a una dirección IP. De este modo el correo electrónico se envía a los usuarios de Domino o a los usuarios de SMTP utilizando la dirección IP pertinente, y aunque compartan puerto, el correo electrónico solo lo maneja el sistema al que va destinado.

Para forzar que el servidor SMTP utilice una dirección Internet específica, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la pestaña **Enlaces**.
4. Para enlazar todas las interfaces al puerto 25, marque el botón de selección **Utilizar todas las interfaces**.
5. Marque el botón de selección **Seleccionar una interfaz** para especificar las interfaces de enlace de cliente y servidor con las que desea enlazarse.

Nota: Si se quiere utilizar la conversión de direcciones de red (NAT) en el servidor o en el cortafuegos, debe forzar que el cliente SMTP de i5/OS utilice una dirección de Internet específica.

6. Pulse **Aceptar**.

Ahora el SMTP solo recibe el correo dirigido a esta dirección de Internet. Mire en el servidor del sistema de nombres de dominio (DNS), en la tabla de hosts locales y en el directorio de distribución del sistema para asegurarse de la presencia de la dirección Internet que ha forzado.

En la biblioteca de consulta de Lotus  hallará instrucciones para enlazar SMTP de Domino a una dirección TCP/IP específica.

Conceptos relacionados

“Planificar el correo electrónico” en la página 10

Antes de configurar el correo electrónico, debe elaborar un plan básico sobre cómo utilizar el correo electrónico en su sistema.

Filtrado IP y conversión de direcciones de red (NAT)

Hospedar LDAP Domino y el servidor de directorio en el mismo sistema

Si ejecuta LDAP Domino e IBM Tivoli Directory Server para i5/OS (el servidor de directorio) en el mismo sistema, le sugerimos que configure cada uno de ellos de manera que se enlacen a una dirección IP específica.

Cuando hospeda LDAP Domino y el servidor de directorio en el mismo sistema, puede establecer un número de puerto distinto para cada servidor o bien enlazar cada servidor a una dirección IP. Pero el hecho de cambiar el número de puerto puede ser molesto para los clientes, por lo que la mejor solución podría ser especificar una dirección IP específica para cada servidor. Domino y el protocolo simple de transferencia de correo (SMTP) utilizan cada uno el servidor LDAP pertinente para el sistema de direcciones de correo electrónico.

Para forzar que el servidor de directorio utilice una dirección Internet específica, siga estos pasos:

1. En System i Navigator, seleccione *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **Directorio** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la pestaña **Red**.
4. Pulse **Direcciones IP**.
5. Seleccione **Utilizar las direcciones IP seleccionadas** y especifique qué interfaces de la lista desea enlazar.
6. Pulse **Aceptar** para cerrar la página Directorio - Direcciones IP.
7. Pulse **Aceptar** para cerrar la página Propiedades del directorio.
8. Opcional: Si utiliza LDAP Domino, vea la biblioteca de consulta de Lotus Domino, donde hallará instrucciones para enlazar LDAP Domino a una dirección TCP/IP concreta.
9. Inicie los servidores de correo electrónico.

Información relacionada



Biblioteca de consulta de Domino Lotus

Gestionar el rendimiento del servidor de protocolo simple de transferencia de correo (SMTP)

A continuación se ofrecen sugerencias sobre cómo gestionar un servidor de protocolo simple de transferencia de correo (SMTP) ocupado que utiliza multiproceso.

El servidor SMTP podría estar ocupado porque utiliza toda su capacidad para añadir y finalizar trabajos de prearranque por cada solicitud de correo electrónico.

Si considera que el número de trabajos de prearranque afecta al rendimiento del sistema, puede establecer un valor más bajo para el umbral. Si desea más trabajos, puede establecer un número superior de trabajos de prearranque.

Con los trabajos de prearranque, cada solicitud de correo electrónico se ejecuta como un trabajo propio. Este método permite que cada trabajo se centre únicamente en las solicitudes y necesidades del programa cliente o servidor. Cada trabajo puede realizar llamadas más largas que el tiempo de espera para permitir que se envíen nombres de host con la finalidad de no recibir mensajes de correo electrónico masivo no solicitado.

Para gestionar un servidor SMTP ocupado, puede cambiar los valores siguientes:

- El número de trabajos que se deben iniciar durante la inicialización
- Un número de umbral para los trabajos
- El número de trabajos que hay que añadir cuando el sistema alcanza el umbral
- El número máximo de trabajos en ejecución permitidos
- Seleccionar un subsistema para los trabajos

Para gestionar un servidor ocupado, debe cambiar los valores del servidor SMTP y del cliente SMTP.

El servidor SMTP funciona con el daemon y los trabajos de prearranque: QTSMTPSRVD y QTMSMTPSRVP. El cliente SMTP funciona con el daemon y los trabajos de prearranque: QTSMTPLTD y QTSMTPLTP.

Para cambiar los valores del servidor SMTP, siga estos pasos:

1. En la interfaz basada en caracteres, escriba CHGPJE (mandato Cambiar entradas de trabajo).
2. Entre los valores siguientes para cada solicitud y pulse Intro.

Solicitud	Valor
Subsistema	QSYSWRK
Biblioteca	QSYS
Programa	QTMSRCP
Biblioteca	QTCP
Iniciar trabajos	*SAME
Número inicial de trabajos	4
Umbral	2
Número de trabajos adicionales	2
Número máximo de trabajos	20

Estos valores garantizan que el sistema inicie cuatro trabajos de prearranque, inicie dos trabajos adicionales cuando el número de trabajos disponibles sea inferior a dos, y permita un máximo de veinte trabajos de prearranque.

Cambiar valores del servidor de protocolo simple de transferencia de correo (SMTP)

Utilice el siguiente procedimiento para cambiar los valores del servidor de protocolo simple de transferencia de correo (SMTP).

1. En la interfaz basada en caracteres, teclee CHGPJE (mandato Cambiar entradas de trabajo).
2. Entre los valores siguientes para cada solicitud y pulse Intro.

Solicitud	Valor
Subsistema	QSYSWRK
Biblioteca	QSYS
Programa	QTMSRCP
Biblioteca	QTCP
Iniciar trabajos	*SAME
Número inicial de trabajos	4
Umbral	2

Solicitud	Valor
Número de trabajos adicionales	2
Número máximo de trabajos	20

Estos valores garantizan que el sistema inicie cuatro trabajos de prearranque, inicie dos trabajos adicionales cuando el número de trabajos disponibles sea inferior a dos, y permita un máximo de veinte trabajos de prearranque.

Cambiar valores para el cliente de protocolo simple de transferencia de correo (SMTP)

Siga este procedimiento para cambiar los valores del cliente de protocolo simple de transferencia de correo (SMTP).

1. En la interfaz basada en caracteres, escriba CHGPIE (mandato Cambiar entradas de trabajo).
2. En la solicitud, entre los valores siguientes y pulse Intro.

Solicitud	Valor
Subsistema	QSYSWRK
Biblioteca	QSYS
Programa	QTMSCLCP
Biblioteca	QTCP
Iniciar trabajos	*SAME
Número inicial de trabajos	4
Umbral	2
Número de trabajos adicionales	2
Número máximo de trabajos	20

Estos valores garantizan que el cliente SMTP inicie cuatro trabajos de prearranque, inicie dos trabajos adicionales cuando el número de trabajos disponibles sea inferior a dos, y permita veinte trabajos de prearranque, como máximo.

Seleccionar un subsistema nuevo para los trabajos del servidor de protocolo simple de transferencia de correo (SMTP)

Utilice este procedimiento para seleccionar un nuevo subsistema para los trabajos del servidor de protocolo simple de transferencia de correo (SMTP).

1. Puede especificar un subsistema aparte para el servidor SMTP. Ello debería mejorar el rendimiento, porque se evita la necesidad de compartir recursos.
2. Para especificar un subsistema aparte, siga estos pasos:
 - a. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. Pulse **SMTP** con el botón derecho del ratón y seleccione **Propiedades**.
 - c. Pulse la pestaña **Parámetros adicionales**.
 - d. Marque el botón de selección **Descripción de subsistema**.
 - e. Entre el nombre del nuevo subsistema y la biblioteca en la que se van a crear la descripción del subsistema y la cola de trabajos.

El programa comprueba si existe el subsistema especificado. Si no existe, el programa lo crea junto con entradas de tabla de rutas, entradas de trabajos de inicio automático, entradas de trabajos de prearranque y descripciones de trabajos. Incluso si el subsistema aún no existe, la biblioteca de la descripción del subsistema y la cola de trabajos ya debe existir. Cuando se procesa el trabajo de arranque para el

servidor, este especifica los parámetros para el subsistema que se acaba de crear y, a continuación, somete los trabajos del servidor para el arranque por lotes en el subsistema.

Información de consulta relacionada con el correo electrónico

Puede encontrar información de consulta sobre las entradas de diario del servidor de correo, los mandatos del protocolo simple de transferencia de correo (SMTP) y los verbos y parámetros del protocolo de oficina postal (POP).

Entradas de diario del servidor de correo

Utilice la siguiente información para comprender los códigos y los mensajes que se utilizan en las entradas de diario.

Las tablas siguientes proporcionan información mas detallada sobre cómo leer las entradas de diario.

- “Abreviaturas de entrada de diario”
- “Entradas de anotaciones para el cliente SMTP” en la página 45
- “Entradas de anotaciones para el servidor SMTP” en la página 46
- “Entradas de anotaciones para el servidor de puente” en la página 47
- “Funciones de salidas y creaciones del recurso de conmutación de mensajes (MSF)” en la página 47

Abreviaturas de entrada de diario

Abreviatura	Definición
LIN	Entrada local, se ha recibido una nota para entrega local. La dirección IP que se indica a continuación es el host que ha enviado la nota.
RIN	Entrada de retransmisión, se ha recibido una nota para retransmitir a otro daemon SMTP. La dirección IP que hay a continuación es la que ha enviado la nota.
R	Destinatario
O	Originador
U	Destinatario de no entregado
QTMSINQ	Cola de entrada de SMTP
QTMSOUTQ	Cola de salida de SMTP
QTMSBSSQ	Cola de retención en la que se colocan los mensajes cuando se excede el umbral de almacenamiento del sistema.
QTMSRTQ1	Cola de reintento de primer nivel
QTMSRTQ2	Cola de reintento de segundo nivel
RRSL	Destinatario resuelto

A cada entrada de diario le precede un subtipo o código de 2 caracteres. El primer carácter del subtipo o código consta de un identificador de función para la entrada. El segundo carácter del subtipo o código consta de la acción que documenta esta entrada de diario. En la tabla siguiente se enumeran los identificadores de función.

Identificador de función	Descripción
7	Entrada del servidor de puente
8	Cliente SMTP

Identificador de función	Descripción
9	Servidor SMTP
A	No entrega de MSF
B	Entrega local de MSF
C	Reenvío de mensajes de MSF
D	Crear mensaje POP
E	API Enviar correo
F	Domino MTA
G	Complemento de túnel
H	SNADS (Conmutador)
I	Analizador MIME (un complemento de entrega local)
L	FAX (Entrega local)
M	SNADS
O	Filtrado
P	Salida SMTP de MFS para resolución de direcciones

Todas las entradas de diario que se documentan aquí utilizan el tipo de entrada de anotaciones (LG).

Entradas de anotaciones para el cliente SMTP

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Quitar el contenedor de la cola para proceso	8B	Justo después de establecer el código floater, anotar que se quita correo de la cola.
LG	Entrega de correo satisfactoria	88 82	Anotar correo enviado satisfactoriamente. Anotar cada destinatario.
LG	Correo que no se puede entregar	83	Anotar correo no entregado.
LG	Tiempo de espera de primer nivel	8C	Anotar al añadir a la cola de reintentos de primer nivel.
LG	Tiempo de espera de segundo nivel	8D	Anotar al añadir a la cola de reintentos de segundo nivel.
LG	Correo preparado para el reintento	8E 8F	Anotar cuando el correo reintentado se vuelve a poner en QTMSOUTQ.
LG	COD devuelto al originador	87	Anotar cuando confirmación de entrega (COD) se pone en la cola de BRSR.
LG	No se puede procesar, recurso ocupado	86	Anotar cuando el correo se vuelve a poner en QTMSOUTQ porque la malla de conexiones está llena.

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Examinar registros de destinatarios	86	Anotar cuando el correo se vuelve a poner en QTMSOUTQ porque el estado del destinatario ha cambiado; es decir, el registro MS se resolvió en estado de preparado para entregar el mensaje.
LG	No se puede entregar	87	Anotar la transferencia de correo a QTMSINQ para aviso de no entregado en dos lugares.
LG	Consulta de MX	8K	Anotar una anomalía de res_send y un número de error sobre el motivo de la anomalía junto con el almacenamiento intermedio de consulta.

Entradas de anotaciones para el servidor SMTP

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Recibir correo	94 91 92 9T 99	Anotar la recepción de correo justo después de recibir la secuencia de finalización CRLF <> CRLF(local). Se anotan el originador y el destinatario. Tamaño del mensaje <i>nnnnn</i> , siendo <i>nnnnn</i> el número de bytes. MSGID
LG	Recibir correo retransmitido	95 91 92	Anotar el correo justo después de recibir la secuencia de finalización CRLF <> CRLF (retransmitido). Se anotan el originador y el destinatario.
LG	Pasar correo al servidor de puente	97	Anotar la entrada de CORREO en QTMSINQ (correo entrante).
LG	Pasar correo al cliente para la entrega remota	96	Anotar la entrada de CORREO en QTMSOUTQ (correo retransmitido).
LG	CONEXIÓN RECHAZADA 1.2.3.4....	9S	Anotar las conexiones rechazadas en función de los valores de conexión restringidos. 1.2.3.4 es la dirección IP rechazada.
LG	RETRANSMISIÓN RECHAZADA 1.2.3.4....	9V	Anotar las retransmisiones rechazadas en función de los valores de retransmisión restringidos. 1.2.3.4 es la dirección IP rechazada.

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Rechazado por el servidor SMTP	9W	El mensaje ha sido rechazado por el servidor SMTP.

Entradas de anotaciones para el servidor de puente

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Obtener correo de la cola de entrada (IN)	7A	Anotar correo que deja de estar en la cola QTMSINQ.
LG	Pasar correo a SNADS	7O	Anotar la transferencia satisfactoria a QSNADS.
LG	Poner el contenedor en la cola BUSY debido al uso de espacio	7L	Anotar cuando se pone correo en la cola QTMSBSSQ debido a un desbordamiento de umbral.
LG	Obtener correo de la cola BUSY	7M	Anotar cuando el correo deja de estar en la cola QTMSBSSQ. El espacio se ha reclamado y ahora el correo se puede procesar.
LG	Pasar el mensaje a MSF	7H 71 72	Anotar cuando se inserta el mensaje en la infraestructura.
LG	Creación del mensaje COD	7R 7G	Anotar cuando el mensaje COD se inserta en la infraestructura. Anotar el MSGID de MSF porque se está creando el nuevo mensaje COD.
LG	No se puede entregar este elemento de correo a un destinatario	7P 7G	Anotar el hecho de que ha creado un aviso que no se puede entregar. Anotar el MSGID del nuevo aviso de mensaje no entregable.

Funciones de salidas y creaciones del recurso de conmutación de mensajes (MSF)

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Creación del mensaje de no entrega	AP A1 A2	Anotar el mensaje de no entrega que se inserta en MSF.
LG	El correo se entrega a un buzón POP	B8 B2	Anotar la entrega del mensaje al buzón PPP local. La dirección IP es el directorio de buzones POP. El destinatario también se incluye en la lista.
LG	Enviar mensaje COD a MSF	BR B1 B2	Anotar la inserción de mensaje COD en MSF.

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Comprobar la disponibilidad	CN	Salida MSF de reenvío de mensaje SMTP. Anotar el MSGID que se ha vuelto a poner en la cola QMSF debido a que no se había iniciado SMTP.
LG	Poner el correo en la cola	C6 C1 C2	Anotar el correo que se pone en la cola QTMSOUTQ.
LG	Uso de la API Sendmail	EH E1 E2 ET	Anotar la creación del mensaje por la API SendMail. Tamaño de mensaje <i>nnnnn</i> , siendo <i>nnnnn</i> el tamaño del mensaje (todos los adjuntos).
LG	El correo se destina a un sistema remoto puenteado SNADS	G8 G2	Anotar cuando el mensaje se envía por túnel. Incluir el sistema enviado al destinatario.
LG	Se recibe correo por túnel a través de un puente SNADS.	GQ G2	Anotar que se recibe el mensaje por túnel para destinatario de entrega local.
LG	SNADS de resolución de direcciones conmuta en uno o en otro sentido	H1	SNADS ha conmutado un mensaje en MSF.
LG	Reinserción de nota MIME analizada en la infraestructura	IH I1 I2 IG	Anotar cuando el mensaje MIME analizado se reinserta en MSF.
LG	Rechazado por el filtrado	OW	El mensaje se ha rechazado. Se anota tanto si se descarta como si se conserva. Se anota también si se ha reescrito y entregado.

Tipo	Acción	Subtipos o códigos	Comentarios
LG	Tecleado por el programa de salida de MSF de resolución de direcciones SMTP	P2	<p>El mensaje se ha marcado de la siguiente manera:</p> <ul style="list-style-type: none"> • POP LclDel: marcado para que el programa de salida de entrega local POP lo entregue. • SMTP MsgFwd: marcado para reenviar a SMTP para que lo envíe. • SMTP NonDel: marcado para notificación de no entrega. • Parse: enviado al código del analizador. • PutBk: vuelto a poner en la infraestructura para que lo maneje algún otro programa de salida (por ejemplo, Domino o SNADS). • chg to SNADS: el tipo de dirección ha pasado a ser SNADS.

Tareas relacionadas

“Comprobar los diarios de componentes” en la página 53

Puede comprobar los diarios que registran errores para determinar cómo resolver un determinado problema relacionado con el correo electrónico.

Protocolo simple de transferencia de correo (SMTP)

El protocolo simple de transferencia de correo (SMTP) es un protocolo TCP/IP que se utiliza para enviar y recibir correo electrónico. Normalmente se utiliza con POP3 o con el protocolo de acceso a mensajes de Internet (IMAP) para guardar mensajes en un buzón del servidor y descargarlos periódicamente del servidor para el usuario.

Mandatos de SMTP

La tabla siguiente describe los mandatos de SMTP y sus funciones, e indica si el servidor SMTP de i5/OS soporta los mandatos.

Mandato SMTP	Qué hace	Soportado por System i
AUTH (Authentication)	Indica un mecanismo de autenticación al servidor SMTP. Se soportan tanto PLAIN como LOGIN.	Sí
DATA (Data)	Considera las líneas situadas después del mandato como correo electrónico del remitente.	Sí
EHLO (Extension Hello)	Habilita las extensiones SMTP.	Sí
EXPN (Expand)	Solicita al receptor que confirme que se ha identificado una lista de correo.	No
HELO (Hello)	Identifica al remitente de SMTP ante el receptor de SMTP.	Sí

Mandato SMTP	Qué hace	Soportado por System i
HELP (Help)	Solicita al receptor que envíe información de ayuda al remitente.	Sí
MAIL (Mail)	Inicia una transacción de correo electrónico para entregar el correo electrónico a uno o más destinatarios.	Sí
NOOP (Noop)	Solicita al receptor que envíe una respuesta válida (pero sin especificar otras acciones).	Sí
QUIT (Quit)	Solicita al receptor que envíe una respuesta válida y luego cierre el canal de transmisión.	Sí
RCPT (Recipient)	Identifica un destinatario individual de correo electrónico.	Sí
RSET (Reset)	Finaliza la transacción de correo electrónico actual.	Sí
SAML (Send and mail)	Entrega correo electrónico a una o más estaciones de trabajo y destinatarios si el usuario no está activo.	No
SEND (Send)	Entrega correo electrónico a una o más estaciones de trabajo.	No
SOML (Send or mail)	Entrega correo electrónico a una o más estaciones de trabajo o destinatarios si el usuario no está activo.	No
STARTTLS (Start Transport Layer Security)	Solicita al servidor SMTP que inicie una negociación de capa de sockets seguros (SSL) o TLS con el cliente SMTP para establecer una sesión SSL o TLS.	Sí
TURN (Turn)	Solicita al receptor que envíe una respuesta válida y que, a continuación, se convierta en el remitente de SMTP, o bien solicita al receptor que envíe una respuesta de rechazo y siga siendo el receptor de SMTP.	No
VERFY (Verify)	Solicita al receptor que confirme que se ha identificado un usuario.	Sí

Conceptos relacionados

“Escenario: enviar y recibir correo electrónico localmente” en la página 5

En este escenario se hace una demostración de cómo se procesa el correo electrónico entre usuarios locales.

Protocolo de oficina postal (POP)

La interfaz de correo Protocolo de oficina postal (POP) Versión 3 está definida en la solicitud de comentarios (RFC) 1939 (POP3), en la RFC 2449 (Mecanismo de extensión POP3) y en la RFC 2595 (Utilizar TLS con IMAP, POP3 y ACAP). Las solicitudes de comentarios (RFC) son el mecanismo que se utiliza para definir los estándares de Internet en evolución.

El software de cliente utiliza mandatos denominados *verbos* para comunicarse con el servidor POP. El servidor POP de i5/OS soporta los verbos siguientes.

Verbo y parámetros	Descripción
USER <id>	Pasar ID de usuario
PASS <password>	Contraseña
STAT	Consultar buzón
LIST <opt msg #>	Consultar estadísticas de mensajes
RETR <msg #>	Recuperar mensaje
DELE <msg #>	Suprimir mensaje
RSET	Restablecer el estado de supresión de mensaje
TOP <msg #> <lines>	Recuperar datos y cabecera de mensaje
UIDL <opt msg #>	Obtener listado de ID exclusivos de mensaje
NOOP	Sin operación
QUIT	Abandonar la sesión de cliente
CAPA	Listar las prestaciones
STLS	Iniciar la seguridad de capa de transporte (TLS)

Conceptos relacionados

“Escenario: enviar y recibir correo electrónico localmente” en la página 5

En este escenario se hace una demostración de cómo se procesa el correo electrónico entre usuarios locales.

“Protocolo de oficina postal (POP) en i5/OS” en la página 4

El servidor de protocolo de oficina postal (POP) es la implementación i5/OS de la interfaz de correo del Protocolo de Oficina Postal Versión 3.

Resolver problemas relacionados con el correo electrónico

Esta información está pensada para ayudarle a resolver problemas que puedan surgir en relación con el correo electrónico.

Tareas relacionadas

“Impedir que se dividan os mensajes de correo electrónico largos” en la página 39

Es posible que tenga que impedir que los mensajes largos de correo electrónico se dividan y se entreguen en fragmentos más pequeños, que puedan llevar a confusión.

Determinar problemas relacionados con el correo electrónico

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Para identificar el origen probable de los problemas del protocolo simple de transferencia de correo (SMTP), siga estos pasos:

1. Verifique que se ha configurado TCP/IP para el correo electrónico.
 - a. Asegúrese de que se han instalado los PTF que sean necesarios.
 - b. Compruebe los servidores de correo electrónico para asegurarse de que los servidores necesarios se han iniciado y están en ejecución.
2. Verifique el nombre de dominio local.
 - a. En System i Navigator, expanda *su sistema* → **Red**.
 - b. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**.

- c. Pulse la pestaña **Información de dominio de host** y verifique el nombre del dominio local.
3. Establezca valores inferiores para los reintentos de SMTP.
 - a. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. Pulse dos veces en **SMTP**.
 - c. Pulse la pestaña **Reintentos de correo de salida**.
4. Verifique que la dirección y el ID de usuario del receptor se encuentran en el directorio de distribución del sistema.
 - a. En System i Navigator, expanda *su sistema* → **Usuarios y grupos** → **Todos los usuarios**.
 - b. Pulse el **Perfil** del ID de usuario con el botón derecho del ratón y seleccione **Propiedades**.
 - c. Pulse **Personal** y vaya a la pestaña **Correo** para verificar la dirección.
5. Verifique si se necesita una entrada de la tabla de hosts para que el correo electrónico llegue a la dirección del destino.
 - a. En la interfaz basada en caracteres, escriba CHGTCPHTE (mandato Cambiar entrada de tabla de hosts TCP/IP) y teclee la dirección Internet del servidor de correo electrónico.
 - b. Si no se muestra ninguna entrada de la tabla de hosts, entre el nombre de host para esa dirección Internet.
6. Asegúrese de que no ha superado el umbral de almacenamiento.
 - a. En System i Navigator, expanda *su sistema* → **Configuración y servicio** → **Hardware** → **Unidades de disco** → **Agrupaciones de discos**.
 - b. Pulse con el botón derecho del ratón la agrupación de discos origen que desea ver y seleccione **Propiedades**.
 - c. Seleccione la pestaña **Capacidad**.
Si la utilización del sistema es mayor que el umbral, el correo podría dejar de funcionar.
7. Verifique que la función de división de correo electrónico está inhabilitada.
 - a. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. Pulse dos veces en **POP**. Aparece el diálogo Propiedades de POP.
 - c. Pulse la pestaña **Configuración**.
 - d. Para el campo **Tamaño de división de mensaje**, verifique que está seleccionado **Sin máximo**.
8. Ejecute el mandato Rastrear aplicaciones TCP/IP. En la interfaz basada en caracteres, escriba TRCTCPAPP.
9. Consulte los diarios de los componentes para localizar el problema.

Conceptos relacionados

“Controlar el acceso al correo electrónico” en la página 11

Debe controlar quién accede a su sistema mediante correo electrónico para proteger sus datos de los ataques maliciosos.

Ejemplos de agrupaciones de discos independientes

“Controlar el acceso del protocolo de oficina postal (POP)” en la página 12

Para garantizar la seguridad del sistema, debe controlar el acceso del protocolo de oficina postal (POP).

“Resolver problemas relacionados con la API QtmmSendMail” en la página 54

Puede utilizar este proceso de detección de errores para resolver los problemas relacionados con la API Enviar correo MIME (QtmmSendMail).

Tareas relacionadas

“Comprobar servidores de correo electrónico” en la página 38

Uno de los problemas más comunes en relación al correo electrónico es que no se inicien los correspondientes servidores. Antes de utilizar los servidores de correo electrónico, debe verificar su estado y asegurarse de que todos ellos se están ejecutando.

“Configurar TCP/IP para correo electrónico” en la página 15

Debe configurar el TCP/IP antes de configurar el correo electrónico en su sistema.

“Comprobar los trabajos de la infraestructura de servidor de correo (MSF)” en la página 55

Debe comprobar los trabajos de la infraestructura de servidor de correo en el sistema QSYSWRK para determinar una posible causa del error en la API QtmmSendMail.

“Comprobar los diarios de componentes”

Puede comprobar los diarios que registran errores para determinar cómo resolver un determinado problema relacionado con el correo electrónico.

“Hacer un seguimiento del correo electrónico no entregado” en la página 54

Puede utilizar un ID de usuario genérico para hacer un seguimiento de los problemas que se producen con el correo electrónico que no se puede entregar. Este método puede resultar útil para los problemas de configuración y de entrega de correo electrónico.

Información relacionada



Soporte para IBM System i

Comprobar los diarios de componentes

Puede comprobar los diarios que registran errores para determinar cómo resolver un determinado problema relacionado con el correo electrónico.

El sistema operativo utiliza distintas colas, programas y documentos de registro por diario que le pueden indicar por qué el servidor de correo electrónico no entrega el correo. La función de registro por diario puede resultar útil para facilitar información sobre los posibles problemas del sistema de correo electrónico. El registro por diario utiliza ciclos de unidad de proceso, por lo que la máquina ofrece un mejor rendimiento cuando esta función está desactivada.

La función de registro por diario documenta los elementos siguientes:

- Transiciones -- de programas a colas, de colas a programa.
- Sucesos -- llegada de correo a través del servidor, entrega de correo a través del cliente, almacenamiento de correo en colas de reintento o en colas ocupadas de recursos.
- Seguimiento y algunos datos de medición -- ID de mensaje 822, ID de mensaje MSF, tamaño de mensaje, originador, destinatarios.

Los registros de diario se almacenan en receptores de diario. El usuario es el que gestiona estos receptores. Cuando el diario esté lleno, emita el mandato Cambiar diario (CHGJRN) para pasar a un nuevo receptor de diario. La nueva función de registro por diario de SMTP utiliza el diario QZMF.

Para activar el registro por diario y ver el contenido del diario, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse dos veces en **SMTP**.
3. Pulse la pestaña **General**.
4. Marque el recuadro de selección **Habilitar entradas de diario**.
5. Abra una sesión de emulación.
6. Para convertir las entradas de diario de SMTP a un formato visualizable, vaya a la interfaz basada en caracteres y teclee: DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(*bibDiarios/zmfstuff*) OUTMBR(MAR2) ENTDTALEN(512), donde *bibDiarios* es el nombre de la biblioteca y *zmfstuff* es el nombre del archivo físico.
7. Para ver las entradas de diario de SMTP, escriba DSPPFM FILE(*bibDiarios/zmfstuff*) MBR(MAR2) en la línea de mandatos.
8. Pulse F20 (Mayús + F8) para ver información específica del diario.

Conceptos relacionados

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Referencia relacionada

“Entradas de diario del servidor de correo” en la página 44

Utilice la siguiente información para comprender los códigos y los mensajes que se utilizan en las entradas de diario.

Hacer un seguimiento del correo electrónico no entregado

Puede utilizar un ID de usuario genérico para hacer un seguimiento de los problemas que se producen con el correo electrónico que no se puede entregar. Este método puede resultar útil para los problemas de configuración y de entrega de correo electrónico.

1. Seleccione o cree un ID de usuario para recibir la notificación. En la interfaz basada en caracteres, escriba CRTUSRPRF (mandato Crear perfil de usuario) y pulse Intro.
2. Escriba WRKDIRE (mandato Trabajar con entradas de directorio) y pulse Intro.
3. Escriba 1 para añadir el usuario al directorio de distribución del sistema.
4. Asegúrese de que el valor del almacén de correo es 2 y que el valor de dirección preferida es 3.
5. Pulse F19 (Añadir nombre para SMTP).
6. Escriba NONDELIVERY@localhost.domain como dirección SMTP para cualquier usuario de POP.

Este usuario recibe una copia del correo electrónico que no se puede entregar.

Nota: El ID de usuario que teclee debe ser un ID real para poder supervisar eficazmente los avisos de no entrega. El remitente recibe una copia del aviso de no entrega con una lista de los destinatarios que no han recibido el correo electrónico.

Conceptos relacionados

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Resolver problemas relacionados con la API QtmmSendMail

Puede utilizar este proceso de detección de errores para resolver los problemas relacionados con la API Enviar correo MIME (QtmmSendMail).

- | Es posible que encuentre errores que se devuelvan con la API QtmmSendMail. Para obtener descripciones de los mensajes de error devueltos por la API, consulte la API QtmmSendMail.

Conceptos relacionados

“Determinar problemas relacionados con el correo electrónico” en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Referencia relacionada

API Enviar correo MIME (QtmmSendMail)

Comprobar la llamada de API

Para recuperar el sistema ante un error relacionado con la interfaz de programación de aplicaciones (API) QtmmSendMail, debe asegurarse de que recibe mensajes de error de la API en la pantalla de la estación de trabajo.

Si codifica que se devuelva el error, el programa lo devuelve al programa. Sin embargo, si establece que este valor sea 0 (como se ve en los ejemplos siguientes), el error aparece en la pantalla de la estación de trabajo.

Ejemplo de C

```
Qus_EC_t      Snd_Error_Code;  
Snd_Error_Code.Bytes_Provided=0;
```

Ejemplo de RPG

```
DAPIError      DS  
D APIBytes      1      4B 0  
D CPFId         9      15  
C              Eval  APIBytes  = 0
```

Comprobar el archivo MIME (Multipurpose Internet Mail Extension)

Es posible que tenga problemas con el archivo MIME (Multipurpose Internet Mail Extension) que hace que la API QtmmsendMail devuelva un error. Debe comprobar el archivo MIME para asegurarse de que estos problemas se han arreglado.

1. Compruebe la ubicación del archivo MIME. El archivo MIME debe estar situado en el sistema ROOT y empezar por un signo "/", por ejemplo, /miarchivo.txt, y el nombre de archivo debe incluir la vía de acceso /midirectorio/miarchivo.mime.
2. Compruebe los niveles de autorización. Los perfiles QMSF y QTCP deben tener autorización para leer y suprimir el archivo MIME.
 - a. En la interfaz basada en caracteres, escriba WRKLNK (mandato Trabajar con enlaces de objeto).
 - b. Teclee 9 (Visualizar) para trabajar con las autorizaciones QMST y QTCP. Se muestra la pantalla Trabajar con autorización.
3. Compruebe que el archivo MIME tiene una sentencia de fin de cabecera (CRLF) entre el cuerpo y la cabecera.
4. Compruebe que el archivo MIME está en conformidad con las solicitudes de comentarios (RFC) de MIME.

Nota: Para obtener más información sobre la sentencia de fin de cabecera, vea la sección 2.1 de la RFC2822 (<http://rfc.net/rfc2822.html>).

Comprobar los trabajos de la infraestructura de servidor de correo (MSF)

Debe comprobar los trabajos de la infraestructura de servidor de correo en el sistema QSYSWRK para determinar una posible causa del error en la API QtmmsendMail.

1. Si la MSF ha dejado de procesar el mensaje, vea si hay mensajes de error en los trabajos de MSF.
2. Si el trabajo de infraestructura ha finalizado, el archivo MIME se tiene que haber suprimido. Esto significa que la infraestructura ha procesado el archivo MIME. El problema no se encuentra en la API, sino en la configuración de SMTP.

Conceptos relacionados

"Determinar problemas relacionados con el correo electrónico" en la página 51

Los pasos para determinar la causa de un problema relacionado con el correo electrónico suelen ser sencillos.

Información relacionada con el temario Correo electrónico

Manuales del producto, publicaciones IBM Redbooks, sitios Web y otros temarios de Information Center que contienen información relacionada con el temario Correo electrónico. Puede ver o imprimir cualquiera de los archivos PDF.

Manuales

AnyMail/400 Mail Server Framework Support  (alrededor de 622 KB)

Aquí hallará información sobre la infraestructura que rige el servidor de correo de i5/OS.

IBM Redbooks

- AS/400 Electronic-Mail Capabilities  (alrededor de 3593 KB)
En la documentación de estos libros rojos IBM Redbooks encontrará información detallada sobre el correo electrónico y SMTP.
- AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet  (alrededor de 2160 KB)
Esta documentación de Redbooks facilita información de seguridad, incluidos los pasos para hacer limpieza del sistema operativo i5/OS si su sistema sufre un ataque masivo.

Sitios Web

- Soporte para IBM System i 
Descargue los archivos PDF actuales para el sistema operativo i5/OS utilizando la estación de trabajo como pasarela que lleva a la página de PDF en Internet, o consulte las soluciones de i5/OS en la categoría Información Técnica y Bases de Datos.
- Índice de RFC 
Los protocolos de correo electrónico están definidos en las RFC (solicitudes de comentarios). Las RFC son vehículos que se utilizan para definir los estándares de Internet en evolución. Para obtener más información acerca de SMTP, consulte la RFC 1939 (POP3), la RFC 2449 (Mecanismo de extensión POP3) y la RFC 2595 (Utilizar TLS con IMAP, POP3 y ACAP).
- Lotus Domino para i5/OS 
La página Web presenta Lotus Domino para i5/OS y las soluciones que proporciona el programa bajo licencia.
- Lotus Domino Reference Library 
Aquí encontrará información sobre Domino, leyendo libros blancos, manuales, presentaciones, entre otras cosas.
- Documentación de Lotus 
Las páginas de documentación de Lotus proporcionan enlaces que llevan a recursos como la documentación del producto, libros blancos y publicaciones Redbooks, entre otras cosas.

Más información

System i y la seguridad en Internet

Consulte este temario de Information Center para proteger la red de System i.

Referencia relacionada

“Archivo PDF del tema Correo electrónico” en la página 2
Puede ver e imprimir un archivo PDF de esta información.

Apéndice. Avisos

Esta información se ha escrito para productos y servicios ofrecidos en Estados Unidos de América.

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. El representante local de IBM le puede informar acerca de los productos y servicios que actualmente están disponibles en su localidad. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios de IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre las licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japón

El párrafo siguiente no es de aplicación en el Reino Unido ni en ningún otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN Y DE COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de garantías, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información incluida en este documento está sujeta a cambios periódicos, que se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de esos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto, y el usuario será responsable del uso que se haga de estos sitios Web.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciatarios de este programa que deseen obtener información acerca de él para: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, sujeta a los términos y condiciones pertinentes, e incluir en algunos casos el pago de una cantidad.

El programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, lo proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM, el Acuerdo de Licencia para Código de Máquina de IBM o cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento contenidos en esta documentación se han determinado en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Pueden haberse realizado mediciones en sistemas que estén en fase de desarrollo y no existe ninguna garantía de que esas mediciones vayan a ser iguales en los sistemas disponibles en el mercado. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los suministradores de esos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha comprobado dichos productos y no puede afirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las consultas acerca de las posibilidades de productos no IBM deben dirigirse a los suministradores de los mismos.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que muestran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir los programas de ejemplo de cualquier forma, sin tener que pagar a IBM, con intención de desarrollar, utilizar, comercializar o distribuir programas de aplicación que estén en conformidad con la interfaz de programación de aplicaciones (API) de la plataforma operativa para la que están escritos los programas de ejemplo. Los ejemplos no se han probado minuciosamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni dar por sentada la fiabilidad, la facilidad de mantenimiento ni el funcionamiento de los programas.

Cada copia o parte de estos programas de ejemplo, así como toda obra que se derive de ellos, debe incluir un aviso de copyright como el siguiente:

© (nombre de su empresa) (año). Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información de la interfaz de programación

Esta publicación, Correo Electrónico, documenta las interfaces de programación pertinentes que permiten al cliente escribir programas para obtener los servicios de IBM i5/OS.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

AIX
AS/400
Domino
eServer
i5/OS
IBM
IBM (logotipo)
Infoprint
iSeries
Lotus
Lotus Notes
Redbooks
System i
The Output of e-business
Tivoli

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Java y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc., en Estados Unidos y/o en otros países.

Los demás nombres de compañías, productos o servicios pueden ser marcas registradas o de servicio de terceros.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.



Impreso en España