Host Access for the Cloud

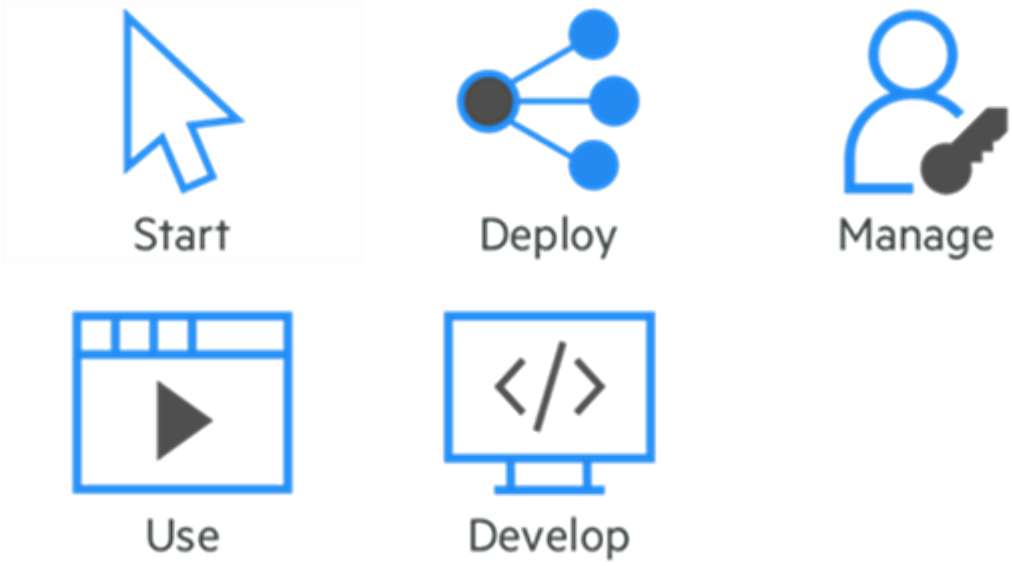
2.7.6

Table of contents

1. Bienvenido a Host Access for the Cloud

El cliente Web Host Access for the Cloud proporciona acceso HTML5 basado en navegador a las aplicaciones de host 3270, 5250, VT, UTS, ALC y T27. El producto Host Access for the Cloud elimina la necesidad de utilizar el escritorio; no hay software que distribuir, parches que aplicar ni configuraciones que establecer. Con él puede proveer acceso a usuarios a todas sus aplicaciones de host, independientemente de cuál sea la plataforma utilizada.

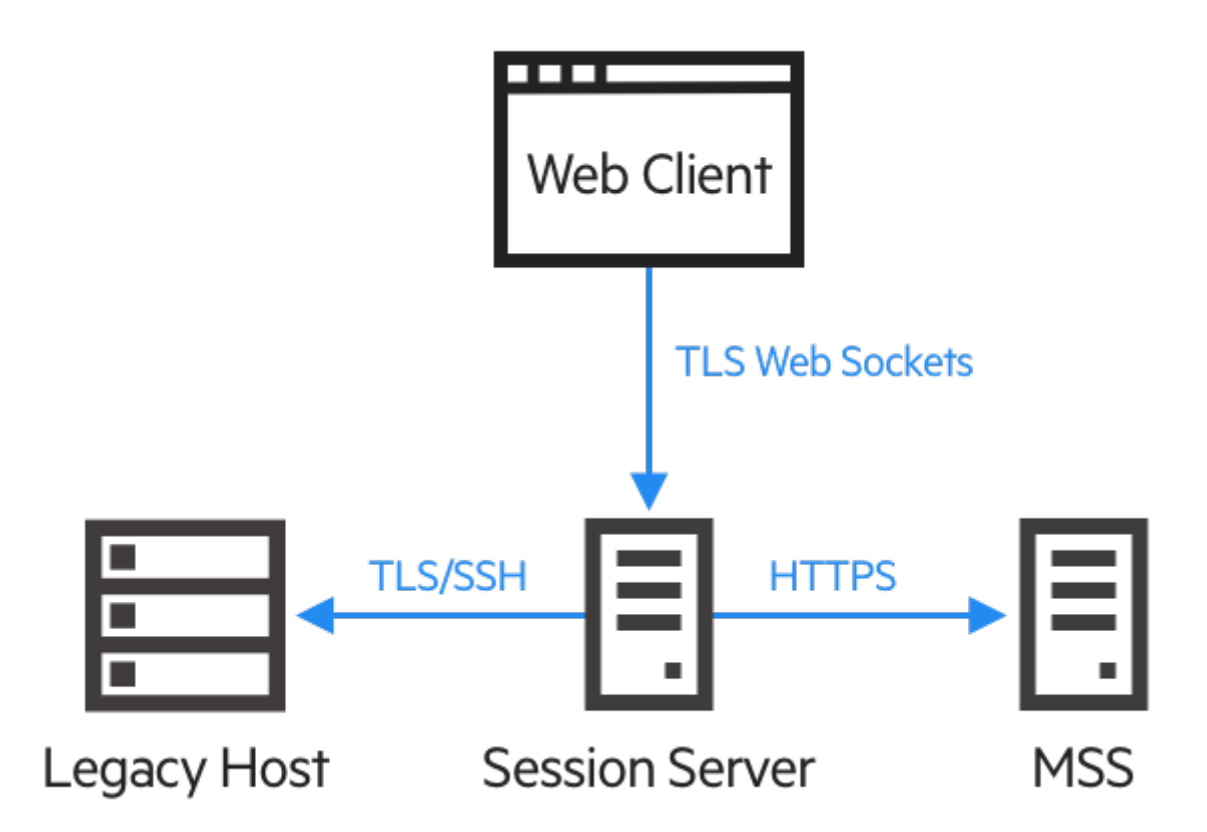
El cliente Web funciona con una completa protección de sesión mediante TLS para proteger la comunicación con sus sistemas de mainframe.



2. Conceptos básicos

Host Access for the Cloud ofrece emulación de terminal de huella cero que proporciona acceso HTML5 basado en navegador a aplicaciones de host 3270, 5250, VT, UTS, ALC y T27 sin necesidad de utilizar el escritorio ni de instalar ni gestionar entornos de tiempo de ejecución de Java. Una ubicación administrativa centralizada reduce los costes de TI y el tiempo de administración de escritorios, al tiempo que provee y suministra de forma eficiente acceso a host a los usuarios finales. La comunicación se protege mediante seguridad HTTPS, TLS y SSH.

2.1 Cómo funciona



2.1.1 Componentes

Familiarícese con los tres componentes:

- Host Access Management and Security Server (Servidor de administración y seguridad de acceso a host)

  El Host Access Management and Security Server (MSS) provee una Consola Administrativa, una ubicación centralizada basada en la web en la que puede agregar, editar y eliminar sesiones de terminal. El MSS forma parte de la extensa historia de Micro Focus y es compatible con otros productos de Micro Focus.

  , que aparecerá en la documentación, indicará dónde se requiere una configuración adicional en la Consola Administrativa de MSS.

- Servidor de Sesión

  El servidor de sesión es el motor que permite a los usuarios finales acceder de forma segura al host desde el cliente web y otros conectores compatibles. Atiende al cliente web y los conectores relacionados en el front-end y, a continuación, administra las conexiones al host en el back-end, lo que garantiza la autenticación y la autorización adecuadas a través de MSS y la comunicación segura a través de TLS. Varios servidores de sesión pueden servir hasta decenas de miles de sesiones y proporcionar un acceso rápido y eficiente a los datos de host.

- Cliente Web

  El cliente web es el emulador de terminal basado en la web donde sus usuarios pueden acceder fácilmente a las sesiones autorizadas desde cualquier plataforma y ubicación.

  El Cliente web provee macros, asignación de teclado y de color, teclado en pantalla, funcionalidad de copiar/pegar, actualizaciones de pantalla iniciadas por el host y capacidades de transferencia de archivos

2.1.2 Funciones de administrador y usuario final

Las funciones de administrador y usuario final se describen en la documentación y el flujo de trabajo. El administrador crea sesiones, asigna usuarios a esas sesiones y establece las preferencias de los usuarios. El usuario final accede a las sesiones asignadas, interactúa con el cliente web para conectarse al host y realiza las tareas.

2.1.3 Compatibilidad con el navegador y el sistema operativo

Host Access for the Cloud es un producto de 64 bits, compatible con los navegadores Google Chrome, Mozilla Firefox, y Microsoft Internet Explorer y Edge. El uso de contenedores de Docker permite la ampliación vertical y horizontal, y admite tecnologías basadas en la nube. Puede encontrar la lista completa de plataformas compatibles y otros requisitos de instalación en los requisitos del sistema de evaluación.

2.1.4 Consideraciones relativas a la seguridad

Cuando abre los hosts heredados para los usuarios que se encuentran fuera del firewall corporativo (socios de negocios, usuarios remotos, personal de ventas móvil y otros), tendrá que blindar la información frente a amenazas de seguridad conocidas. Con Host Access for the Cloud, puede proporcionar acceso Web-a-host seguro para todos los usuarios, tanto si están a la vuelta de la esquina o alrededor del mundo. Host Access for the Cloud, junto con MSS, proporciona conexiones HTTPS y una gran variedad de opciones de autorización y autenticación.

Host Access for the Cloud es compatible con los protocolos TLS y SSH para proteger los datos de misión crítica. Para proteger sus contraseñas y otros datos sensibles, utilice el protocolo HTTPS, que proporciona cifrado TLS.

Host Access for the Cloud se puede conectar de forma segura al navegador, el host y el servidor de administración. Consulte "Proteger conexiones" para obtener información sobre cómo proteger esas conexiones.

2.2 Cómo obtener Host Access for the Cloud

2.2.1 Requisitos del sistema de evaluación

Para instalar y evaluar correctamente Host Access for the Cloud, el sistema necesita lo siguiente:

- 8 GB de memoria.
- Un navegador y un sistema operativo compatibles.

Consulte Requisitos mínimos del sistema para obtener una lista completa de los entornos compatibles.

Descarga del software de evaluación

Si aún no dispone del software, visite nuestro sitio y complete un formulario de petición de evaluación. Recibirá un mensaje de correo electrónico con instrucciones para descargar e instalar una copia de evaluación de Host Access for the Cloud válida durante 60 días. Esta copia de evaluación le permite abrir y cerrar sesiones de host y mantener 25 conexiones de host activas simultáneamente. La página de prueba tiene toda la información que necesita para dar el paso siguiente.

La página de descargas de Micro Focus contiene los archivos comprimidos necesarios para realizar la instalación en todas las plataformas admitidas, incluido el conector de Windows. Diferentes archivos de activación permitirán usar distintas ediciones o plataformas de Host Access for the Cloud.

2.2.2 Instalación básica

Las siguientes instrucciones le proporcionan la instalación básica predeterminada. Esto significa que todos los componentes se instalan localmente y utilizan puertos predeterminados.. Una vez

realizada esta instalación, puede realizar el recorrido para familiarizarse con Host Access for the Cloud y MSS.

1. Desde la página de descargas de Micro Focus, descargue su paquete de instalación del producto. El paquete incluye soporte para todas las plataformas compatibles.
2. Mediante las indicaciones del programa de instalación, instale Host Access for the Cloud y el Servidor de Administración y Seguridad (MSS).

MSS utiliza archivos de activación (activation.jaw) para habilitar las funciones del producto. El programa de instalación contiene el archivo de activación necesario y este se activa como parte del proceso de instalación.

> **Nota**
>
> Durante una instalación básica, se utiliza un certificado autofirmado para garantizar conexiones seguras. Al pasar a un entorno operativo, puede proporcionar sus propios certificados.

Ahora puede realizar el paso siguiente, el recorrido por Host Access for the Cloud.

2.3 Recorrido

Las siguientes instrucciones se basan en una instalación básica por defecto. Esto significa que todos los componentes se instalan localmente y utilizan puertos por defecto. Una vez realizada esta instalación, puede seguir los pasos para familiarizarse con Host Access for the Cloud y MSS.

Consulte la sección de distribución para obtener información sobre la instalación en entornos operativos y diferentes situaciones de producción.

2.3.1 Pasos que seguirá

1. Abra la Consola Administrativa MSS.
2. Crear una nueva sesión. Esto abre una nueva ventana de navegador y se visualiza el panel Conexión del cliente web.
3. Configurar parámetros y conectar, incluidas las opciones de conexión y preferencias de usuario.
4. Asignar usuarios a sesiones y configurar la autenticación.
5. Proporcionar acceso a las sesiones a los usuarios finales.

Abra la Consola Administrativa MSS

1. En el menú Inicio de un entorno de Windows, en Micro Focus Host Access for the Cloud, haga clic en la Consola Administrativa o abra la URL de la página de entrada a la sesión del administrador en el navegador web. La URL utiliza este formato: `https://myserver.mycompany.com:443/adminconsole`.

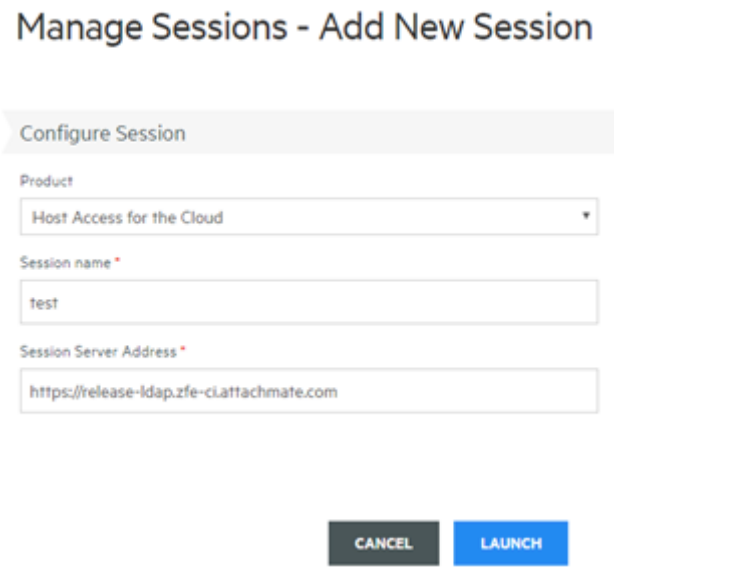
2. Si se conecta utilizando HTTPS y su servidor tiene un certificado autofirmado, su navegador le avisará del certificado que usted ha creado. Este comportamiento es normal; usted puede aceptar el certificado autofirmado o elegir proceder y se abrirá la página de inicio de sesión del administrador. Estos avisos cesarán después de que haya adquirido un certificado firmado por una CA o de que haya importado el certificado autofirmado a su almacén de certificados.
3. La cuenta administrativa incluye una contraseña integrada, **admin**. Entre como administrador mediante esta contraseña o la contraseña que especificó al instalar MSS.

Crear una nueva sesión

Consulte Add a Session (Añadir una sesión) en la Guía del administrador de MSS para obtener instrucciones completas.

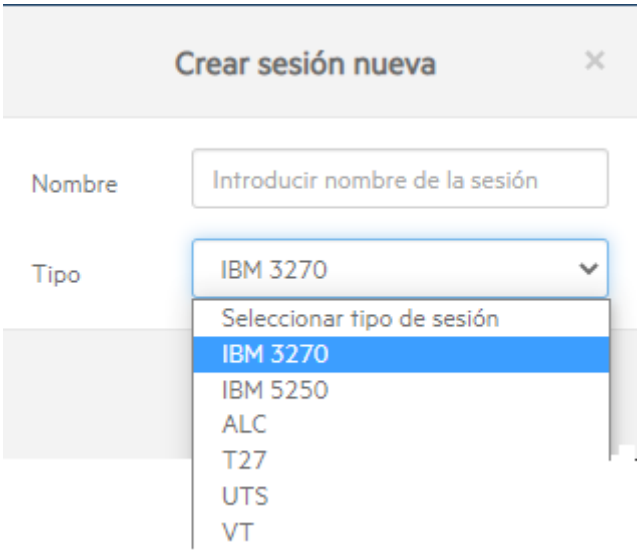
Puede añadir y actualizar la configuración de sesión desde el panel Administrar sesiones de la Consola Administrativa. Cuando usted agrega una sesión, ésta está disponible en la lista de sesión de este panel.

1. En el panel Administrar sesiones, haga clic en AÑADIR para crear una nueva sesión.



2. Si aún no está seleccionado, seleccione Host Access for the Cloud, introduzca un nombre de sesión y haga clic en Iniciar para abrir una nueva ventana del navegador y empezar a configurar la sesión para el servidor mostrado en la dirección del servidor de sesión.

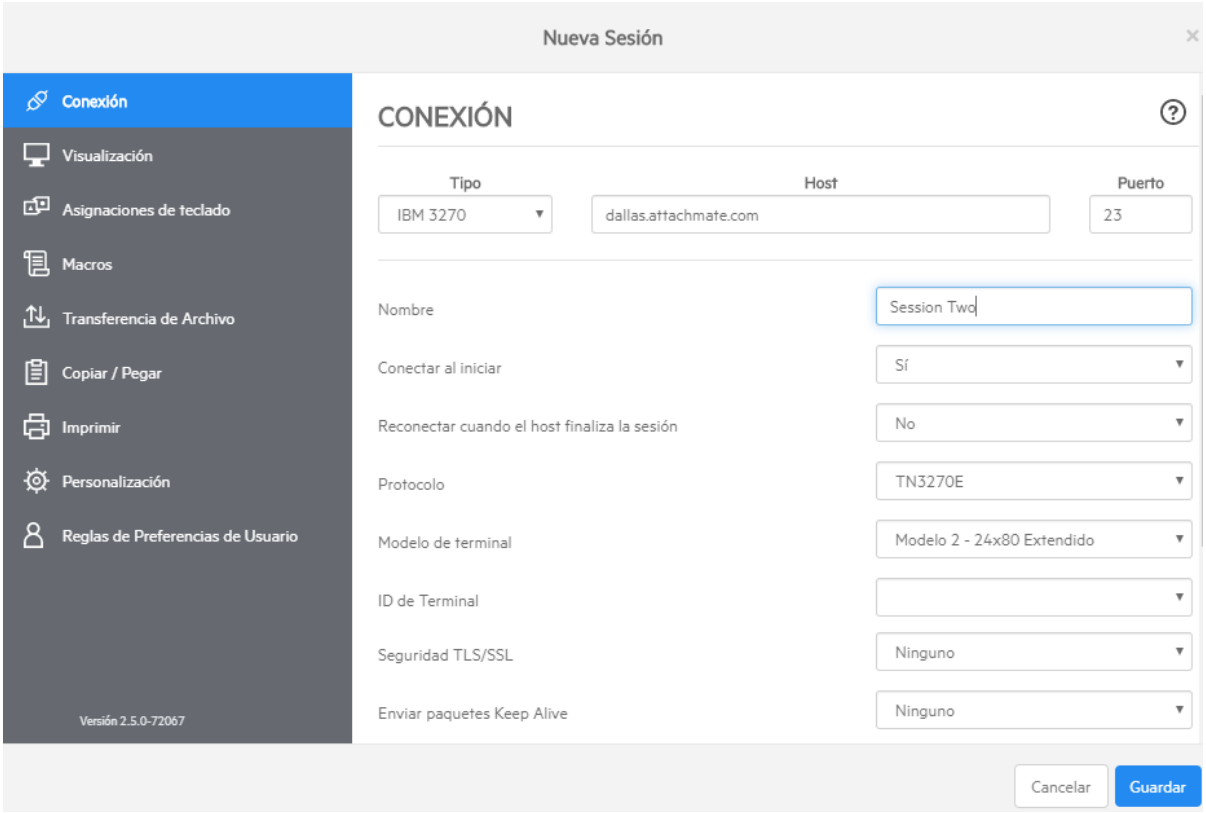
3. En el cuadro de diálogo Crear sesión nueva, seleccione el tipo de host en la lista desplegable y haga clic en Siguiente.



Configurar parámetros y conectar

En la ventana de navegador del cliente web puede configurar distintos parámetros y opciones para la sesión, así como conectarse con el host.

1. En el panel Conexión, introduzca la información de conexión necesaria para la sesión que va a crear.



2. Los parámetros de conexión varían en función del tipo de conexión con el host. Para descripciones detalladas de las opciones de configuración para cada tipo de host, véase la ayuda del cliente web. Las opciones de configuración incluyen la asignación de pulsaciones de

teclas a teclas seleccionadas, asignación de colores de host que coincidan con sus preferencias y la grabación de macros de sesión.

- Asignación de teclas

  a. Para asignar teclas a teclas seleccionadas, abra Asignaciones de Teclado.

  b. Pulse la tecla o combinación de teclas que desee utilizar para activar la acción seleccionada.

  c. En la lista desplegable Acción, seleccione la acción que desee asignar a la pulsación de tecla. Haga clic en  para completar la asignación de teclas. Puede continuar añadiendo y asignando teclas.

  d. Haga clic en Guardar para terminar la asignación de teclas.

- Cambiar los colores de host y otras opciones

  En el panel de navegación izquierdo, puede abrir el panel Visualización para asignar colores de host, ajustar opciones de fuente y de teclado y habilitar zonas activas. Las elecciones de color son específicas para cada sesión.

- Ajuste de las preferencias de usuario

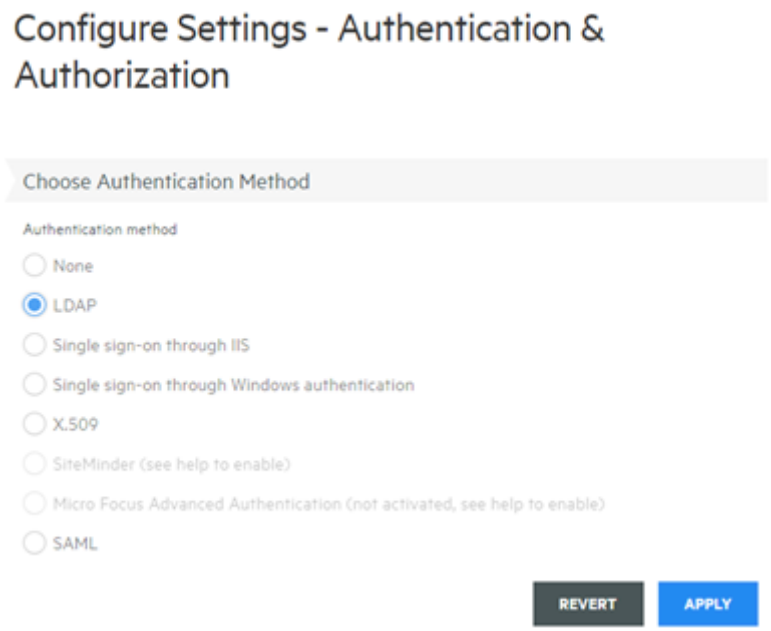
  Abra Reglas de Preferencias del Usuario para extender las opciones de configuración a los usuarios finales.

3. Haga clic en Salir para volver a la ventana del navegador de la Consola Administrativa a fin de autenticar y asignar usuarios a sesiones.

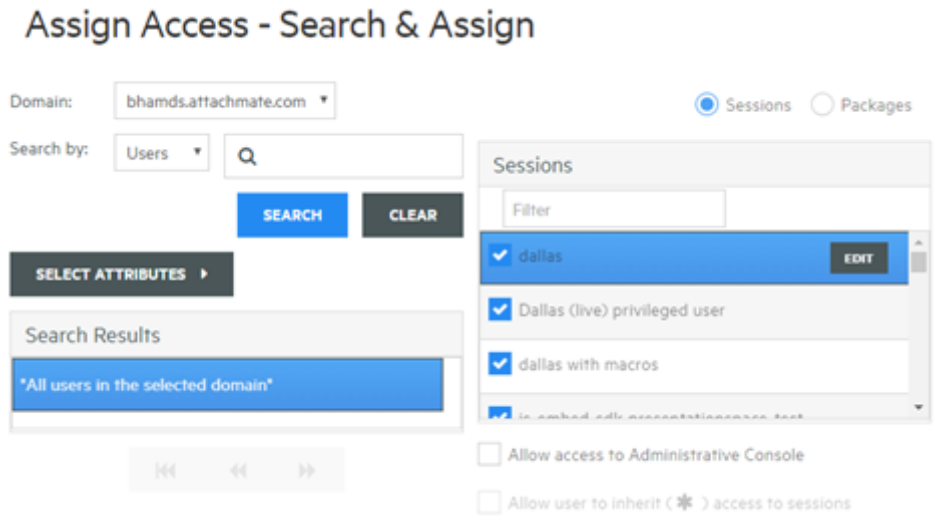
Asignar usuarios a sesiones y configurar la autenticación

Una vez creadas las sesiones, debe conceder a los usuarios acceso a esas sesiones. Los usuarios se autentican y se asignan a sesiones en la Consola Administrativa de MSS. Se puede asignar un usuario a varias sesiones.

1. La autenticación y la autorización validan la identidad de un usuario y el método que desea utilizar para asignar sesiones a usuarios individuales o grupos de usuarios. En el panel de navegación izquierdo, seleccione Configure Authentication (Configurar Autenticación).
2. Elija un método de autenticación. Las opciones cambian en función de su selección.



3. En la documentación del MSS, hay descripciones de las distintas opciones. Haga clic en ?.
4. Haga clic en Aplicar para terminar el proceso.
5. Abra Assign Access (Configuración de Control de Acceso) para asignar sesiones a usuarios individuales o a grupos de usuarios.



6. Asigne las sesiones a los usuarios que desea que accedan ellas y haga clic en Aplicar. También puede elegir permitir a los usuarios heredar acceso a las sesiones y a la Consola Administrativa.

MSS Consulte Select a method to authenticate users (Seleccionar un método de autenticación de usuarios) en la Guía administrativa de MSS.

Proporcionar acceso a las sesiones a los usuarios finales

El último paso consiste en compartir una dirección URL en el servidor de sesión con los usuarios. Por lo general, la dirección URL presenta un aspecto similar al siguiente: `https://myserver.mycompany.com:port`

Al acceder al servidor de sesión, se solicitará a los usuarios que entren a la sesión según sea necesario y se les concederá acceso a las sesiones asignadas.

En implementaciones más complejas, la dirección URL que proporcione será para un equilibrador de carga y no para el propio servidor de sesión. Estos enlaces se incrustan a menudo en portales corporativos u otros sitios Web comerciales.

3. Distribución

3.1 Distribución de Host Access for the Cloud

En esta sección, se va más allá de la configuración básica de evaluación y se presupone que va a pasar a la fase de producción. Consulte Cómo obtener Host Access for the Cloud para obtener información sobre una instalación sencilla.

- Requisitos mínimos del sistema
- Acerca de MSS
- Planificación de la distribución
- Modelo de alta disponibilidad
- Instalación y configuración
- Puertos

3.2 Requisitos mínimos del sistema

Estas plataformas y *versiones posteriores* son compatibles con Host Access for the Cloud. Los requisitos no tienen en cuenta otras aplicaciones y recursos que pueden instalarse en el sistema.

3.2.1 Navegadores web compatibles

- Google Chrome v102 (recomendado)
- Mozilla Firefox v91 (recomendado)
- Microsoft Edge 84
- Apple iOS Safari 14

3.2.2 Servidor de sesión

- **Hardware**
  - CPU: 2 núcleos (se recomiendan 4 núcleos)
  - Cantidad de memoria libre: 4 GB (se recomiendan 6 GB)
- **Sistema operativo (64 bits)**
  - Windows Server 2012
  - SUSE Linux Enterprise Server (SLES) v11 SP4
  - Red Hat Enterprise Linux 7.6
  - Linux en sistemas z
    - SUSE Linux Enterprise Server (SLES) v12 SP4
    - Red Hat Enterprise Linux 7.6

3.2.3 Requisitos adicionales

- Consulte la Guía de instalación de MSS para obtener información sobre los requisitos del sistema para MSS.
- Los equilibradores de carga de MSS y Host Access for the Cloud deben admitir sesiones persistentes y sockets web.

3.3 Acerca de MSS

El Servidor de Administración y Seguridad (MSS) de Host Access protege, administra y supervisa de forma centralizada el acceso del usuario a las conexiones de host. La creación de sesiones, el ajuste de la medición y la configuración de los ID de terminal se realizan con MSS.

Documentación de MSS:

- 12.8.6 Notas de la versión
- Guía de instalación
- Guía administrativa
- Automated Sign-On for Mainframe - Administrator Guide (Inicio de sesión automatizado para mainframe: guía del administrador)

3.4 Planificación de la distribución

¿Cuántos servidores de sesión se deben distribuir? ¿Cuántos servidores MSS? ¿Hay otras consideraciones que se deben tener en cuenta? En esta sección, aprenderá a optimizar la distribución del servidor de sesión y MSS.

3.4.1 Ampliación y alta disponibilidad

Determinar cuántos servidores de sesión y MSS necesita para satisfacer sus necesidades es el primer paso de la plantificación de la distribución. Independientemente de sus necesidades, Host Access for the Cloud puede distribuirse para proporcionar capacidad y alta disponibilidad.

Su solución dependerá de sus necesidades. Sin embargo, consulte "Modelo de distribución de alta disponibilidad" para obtener un ejemplo de distribución ampliable y de alta disponibilidad.

Las principales preguntas a las que debe responder son:

- ¿Cuál es el número máximo de sesiones de host que se utilizarán simultáneamente?
- ¿Cuántos usuarios utilizarán el sistema?
- ¿Qué grado de disponibilidad debe ofrecer el sistema en caso de un fallo en varias áreas del sistema?

3.4.2 Ampliación

La ampliación es la capacidad de un sistema de gestionar distintos volúmenes de carga. Para aumentar la capacidad, un sistema puede ampliarse (verticalmente) mediante la ejecución de un servidor más potente o incrementarse de forma progresiva (horizontalmente) mediante la adición de más servidores o nodos.

En cada caso, existen desventajas que se deben tener en cuenta:

- **La ampliación vertical** ofrece la simplicidad de contar con menos servidores. Sin embargo, aumenta el riesgo de un fallo significativo si el servidor deja de funcionar.
- **La ampliación horizontal** incluye más servidores, pero extiende el riesgo a muchos servidores, por lo que, si uno deja de funcionar, esto afectará a una menor cantidad de usuarios.

Gracias a su mayor capacidad de recuperación, se recomienda una ampliación horizontal mediante la adición de más servidores o nodos cuando aumente la capacidad.

3.4.3 Alta disponibilidad

La alta disponibilidad es la capacidad de un sistema para seguir proporcionando servicios cuando se produce un fallo en alguna parte del sistema. Esta se consigue mediante la adición de redundancia en componentes clave del sistema.

> **Nota**
>
> En esta guía, se aborda la provisión de la alta disponibilidad de los servicios centrales de Host Access for the Cloud. Sin embargo, la alta disponibilidad real se basa en la redundancia en muchas capas de todas las áreas de los sistemas, lo que sobrepasa el ámbito de este documento.

La alta disponibilidad en Host Access for the Cloud se consigue mediante:

- La distribución de suficientes servidores de sesión y MSS para proporcionar la capacidad necesaria con función de capacidad de aumento (libre) para fallos.
- El establecimiento de una capacidad de aumento adecuada para que, cuando falle un servidor y la carga se conmute por error a los servidores restantes, estos no vean comprometida su seguridad por la carga adicional.
- El uso de equilibradores de carga para distribuir la carga y enviar a los usuarios a otros servidores en caso de fallo.
- La réplica de datos entre servidores de MSS, que gestiona la agrupación en clúster de MSS.

Consulte Modelo de distribución de alta disponibilidad para obtener un ejemplo de cómo alcanzar estos requisitos.

3.4.4 Ajuste de tamaño de los servidores de sesión

El número de servidores de sesión necesarios se determina en función del número de sesiones de host simultáneas que se están ejecutando. Las sesiones de host generan más carga en el servidor de sesión que los usuarios, por lo que es necesario centrarse en la cantidad de sesiones de host necesarias en lugar de en la cantidad de usuarios.

Número de sesiones de host simultáneas	**Número de servidores de sesión necesarios**
Hasta 3.000	2 servidores de sesión
Más de 3.000	(Número de sesiones de host necesarias) / 2.000 +1 (mínimo tres)

- Un único servidor de sesión admite 2000 sesiones de host simultáneas.
- Un servidor de sesión presenta una capacidad de ampliación integrada para 1.000 usuarios adicionales en caso de conmutación por error.
- Se necesita un mínimo de dos servidores de sesión para la alta disponibilidad.

3.4.5 Ajuste de tamaño de los servidores MSS

Número de usuarios simultáneos	Número de servidores MSS necesarios
Hasta 30.000	3 servidores MSS
Más de 30.000	(Número de usuarios necesarios) / 10.000 +1 (debe ser un número impar)

- Un único servidor MSS admite 10.000 usuarios simultáneos.
- Un servidor MSS presenta una capacidad de ampliación integrada para 5.000 usuarios adicionales en caso de conmutación por error.
- Se necesita un mínimo de tres servidores MSS para la alta disponibilidad
- Se necesita un número impar de servidores MSS para la alta disponibilidad debido a la necesidad de un quórum de base de datos.

3.4.6 Uso de equilibradores de carga

Deberá proporcionar equilibradores de carga para los servidores de sesión y MSS. Hay valores de configuración habituales que debe tener en cuenta:

- **Load Balancing Algorithm** (Algoritmo de equilibro de carga): el algoritmo determina el servidor al que se envía el tráfico nuevo. Se recomienda "Least Connections" (Número mínimo de conexiones) o algo similar. Comprobar que esta opción distribuya adecuadamente la carga es fundamental para la estabilidad general del sistema. Si el equilibrador de carga no se ha configurado correctamente o no funciona de forma adecuada, se corre el riesgo de que se sobrecargue un servidor individual.
- **Session Persistence (Affinity/Sticky Sessions)** (Persistencia de sesión, sesiones de afinidad/persistentes): se trata de la capacidad de enviar el mismo usuario al mismo servidor mediante varias peticiones. Tanto el servidor de sesión como el MSS son aplicaciones con estado y requieren que las sesiones persistentes estén habilitadas en sus equilibradores de carga.
- **Health Check Endpoint** (Puesto final de comprobación de estado): se trata de la dirección URL en el servicio de destino que se utiliza para determinar si la instancia presenta un buen estado y debería permanecer en servicio. Cada tipo de servidor proporciona su propia dirección URL de estado.

En la sección Modelo de distribución de alta disponibilidad, se proporcionan valores de configuración recomendados para cada uno de estos ajustes.

Opciones de TLS

Existen tres opciones habituales para la gestión de TLS en un equilibrador de carga. La opción que elija dependerá de sus necesidades.

El certificado debe estar instalado en el equilibrador de carga en las dos primeras opciones. La tercera opción, la transferencia directa de TLS, no requiere un certificado en el equilibrador de carga. El plan de alta disponibilidad utiliza puentes TLS para proporcionar TLS de extremo a extremo, al mismo tiempo que permite la persistencia basada en cookies. Las opciones son:

- **TLS Termination/Offloading** (Finalización/descarga de TLS): esta opción finaliza la conexión HTTPS en el equilibrador de carga y continúa con el servicio mediante HTTP.
- **TLS Bridging (Re-encryption)** (Puentes TLS, recifrado): esta opción finaliza la conexión HTTPS en el equilibrador de carga y establece de nuevo una conexión HTTPS entre el equilibrador de carga y el servicio. Esto proporciona TLS de extremo a extremo y al mismo tiempo permite que el equilibrador de carga inyecte una cookie para la persistencia de la sesión.
- **TLS Passthrough (Required for X.509)** (Transferencia directa de TLS, necesaria para X.509): el equilibrador de carga distribuye mediante proxy la conexión TLS sin descifrarla. La desventaja de esta opción es que, dado que no se puede inyectar una cookie, la persistencia debe basarse en la dirección IP de origen o un elemento similar.

TLS con entrada única X.509

Al utilizar la autenticación X.509, se debe establecer la opción de transferencia directa de TLS en los equilibradores de carga de Host Access for the Cloud y MSS, ya que los certificados de cliente se deben presentar a los servidores en el backend. Como se requiere la transferencia directa de TLS, es necesario un método no basado en cookies para la persistencia de sesión, como la dirección IP de origen para los equilibradores de carga del servidor de sesión y MSS. Esto es necesario porque con la transferencia directa de TLS, no hay posibilidad de que el equilibrador de carga descifre la conexión para establecer o incluso ver una cookie.

3.4.7 Administrador de ID de Terminal

El Administrador de ID de Terminal Server no admite actualmente la alta disponibilidad. Puede configurar un servidor pasivo, pero no se replicará el estado de los ID desde el servidor activo. Si el servidor activo no está disponible, aún podrá acceder al servidor pasivo, pero los ID no conservarán su estado actual.

3.4.8 Opciones de distribución

Puede distribuir servidores de sesión de una de estas dos formas:

1. Mediante el uso del método tradicional, es decir, la instalación de cada servidor de sesión en un servidor específico.
2. Mediante el uso de Docker para ejecutar cada servidor de sesión en un contenedor. Docker ofrece diversas ventajas, incluida una mayor flexibilidad en relación con la cantidad de servidores de sesión que puede ejecutar en un único servidor. Consulte Uso de Docker para obtener más información.

3.4.9 Descripción de las interrupciones del servicio

> **Nota**
>
> Al considerar las opciones de distribución, tenga en cuenta que HACloud se compone de varios servicios: el servidor de sesión, MSS y sus complementos, el Administrador de ID de Terminal y la medición. Por defecto, MSS, el Administrador de ID de Terminal y la medición se ejecutan juntos en un solo proceso, pero se pueden configurar para que se ejecuten en procesos independientes. El servidor de sesión de HACloud siempre se ejecuta en su propio proceso.
>
> Cuando se detiene el servidor de sesión, se cierran todas las sesiones de host en ese servidor. Los usuarios que hayan entrado a ese servidor deberán autenticarse de nuevo cuando se reinicie el servidor o cuando se redirija a un servidor nuevo.

En esta tabla, se describen los efectos sobre las capacidades del usuario final cuando los servicios no están disponibles o se han reiniciado.

Acción	Servidor inactivo	Servidor reiniciado
MSS		
Entrada	No	Sí
Crear nuevas sesiones de host	No	Sí
Utilizar sesiones de host existentes	Sí	Sí
Reconectar sesiones de host existentes	Sí (sin incluir las sesiones SSH)	Sí
Editar sesiones	No	Sí (es necesario volver a entrar)
Grabar/editar macros de usuario	No	Sí
Administrador de ID de Terminal		
Conectar una sesión de host que requiere un ID	No	Sí
Conectar una sesión de host que no requiere un ID	Sí	Sí
Servidor de medición		
Crear nuevas sesiones de host	No*	Sí
Utilizar sesiones de host existentes	Sí	Sí

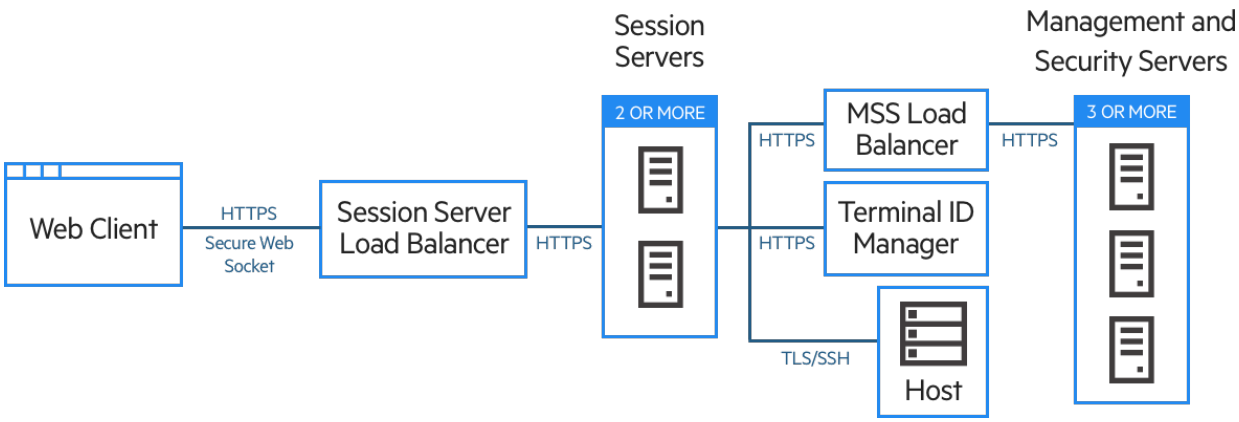
*Si la propiedad `metering.host.required` se ha establecido en "false" (falso), se pueden crear nuevas sesiones.

Si un servidor de sesión pasa a estar inactivo, se perderán todas las sesiones de todos los usuarios conectados a través del equilibrador de carga a ese servidor de sesión. Cada usuario deberá entrar a otro servidor de sesión (a través del equilibrador de carga) e iniciar nuevas sesiones.

3.5 Modelo de distribución de alta disponibilidad

A continuación, se proporciona un ejemplo de cómo distribuir Host Access for the Cloud de forma segura y ampliable, y con alta disponibilidad. Aunque variarán los detalles de cada distribución, por ejemplo, es posible que distribuya tres o más servidores de sesión, el objetivo de este documento es proporcionar un punto de partida eficaz y dar respuesta a las preguntas de distribución más frecuentes.

3.5.1 Arquitectura



Esta distribución consta de:

- Equilibrador de carga del servidor de sesión
- Dos o más servidores de sesión
- Equilibrador de carga del servidor MSS
- Tres o más servidores MSS
- Administrador de ID de Terminal
- Servidor de gestión de identidades o LDAP
- Host/sistema mainframe

3.5.2 Ventajas de la distribución

En este ejemplo, comprobará:

- La capacidad de hasta 3.000 sesiones de host y de ampliación según se necesario.
- La alta disponibilidad de servicios clave, minimizando los únicos puntos de fallo y distribuyendo la carga mediante equilibradores de carga.
- La capacidad de gestionar simultáneamente el fallo de un servidor de sesión y MSS sin una reducción considerable del rendimiento del cliente Web debido a la capacidad de aumento integrada.
- Opciones de autenticación y autorización de MSS
- Comunicación segura a través de HTTPS

3.5.3 Pasos al realizar la distribución

MSS Varios pasos de distribución requieren la configuración de la Consola Administrativa de MSS.

Es recomendable que siga estos pasos al realizar la distribución:

1. Obtenga información sobre los procedimientos básicos de distribución.
2. Proporcione recursos en función de los requisitos del sistema y las directrices de ajuste de tamaño.
3. Instale MSS y cree un clúster.
4. Configure el equilibrador de carga de MSS.
5. Instale los servidores de sesión.
6. Configure el equilibrador de carga del servidor de sesión.
7. Configurar la autenticación y la autorización
8. Compruebe la distribución.

Ha aprendido los conceptos básicos de distribución, los requisitos del sistema y las directrices de ajuste de tamaño en las secciones anteriores.

3.5.4 Instalación de MSS

MSS Consulte la Guía de instalación de MSS para obtener instrucciones completas.

Instale tres servidores MSS y configure cada uno de ellos para la agrupación en clúster. Existe documentación que puede guiarle por este proceso:

1. Abra los puertos en el cortafuegos. Los puertos utilizados por MSS y Host Access for the Cloud se muestran aquí..
2. Instale MSS y, a continuación, los componentes de Host Access for the Cloud para MSS. Para ello, ejecute el programa de instalación de Host Access for the Cloud en cada servidor MSS.
3. Añada cada servidor a un clúster.
4. En cada servidor de MSS, configure los valores de configuración generales, los ajustes de seguridad y otras opciones según sea necesario.

Más información

- Puertos
- Guía de instalación de MSS
- MSS Clustering (Agrupación en clúster de MSS)

3.5.5 Configuración de un equilibrador de carga de MSS

MSS Utilice estos valores cuando configure el equilibrador de carga de MSS:

- **Load balancing algorithm** (Algoritmo de equilibrador de carga): el número mínimo de conexiones (o algo similar).
- **Persistencia de sesión:**

Configure el equilibrador de carga de MSS para que se mantenga en las cookies y los parámetros de URL existentes en el orden especificado a continuación:

```
- Persistencia en **SESSIONID** de cookie
- Persistencia en **sessid** de parámetro de URL (solo es necesario si se ha configurado la entrada única a través de IIS como método de autenticación)
- Persistencia en **JSESSIONID** de cookie
- Persistencia en **jsessionid** de parámetro de URL
```

- **Health check endpoint** (Puesto final de comprobación de estado): `https://<mss-server>/mss/actuator/health`
- **TLS:** configure TLS e instale los certificados según sea necesario.

Más información

- MSS Using a Load Balancer (MSS mediante un equilibrador de carga)

3.5.6 Instalación de servidores de sesión

Instale dos o más servidores de sesión.

En cada servidor de sesión:

1. Abra los puertos en el cortafuegos. Los puertos utilizados por MSS y Host Access for the Cloud se muestran aquí.
2. Instale el servidor de sesión. Durante la instalación, opte por utilizar un servidor MSS remoto e introduzca la dirección y el puerto del equilibrador de carga de MSS.
3. Importe el certificado del servidor de sesión en cada uno de los almacenes de confianza del subsistema de confianza de MSS: `system-trustcerts.bcfks`. Esta acción se realiza automáticamente en el servidor MSS seleccionado por el equilibrador de carga durante la instalación, pero debe realizarse manualmente en los demás servidores. Es recomendable importar o verificar su presencia en cada servidor MSS.

Más información

- Puertos
- Instalación y configuración
- Protección de las conexiones

3.5.7 Configuración del equilibrador de carga del servidor de sesión

Utilice estos valores para configurar el equilibrador de carga:

- **Load balancing algorithm** (Algoritmo de equilibrador de carga): el número mínimo de conexiones (o algo similar).
- **Session persistence** (Persistencia de sesión): habilitada; utilice JSESSIONID o una cookie nueva. A diferencia del equilibrador de carga de MSS, no es necesario que utilice la cookie JSESSIONID existente.
- **Health check endpoint** `https://<session-server:7443>/actuator/health` (Puesto final de comprobación de estado): en el servidor de sesión específico, tenga cuidado al configurar cómo determinar si un nodo ha fallado y qué hacer cuando se produzca este fallo. Si aún hay usuarios conectados a la instancia, esos usuarios pueden perder sus conexiones de host. Para evitar marcar una instancia como fallida demasiado pronto, considere la posibilidad de aumentar los tiempos de espera o el número de reintentos. Algunos equilibradores de carga proporcionan un "modo de purga", que permite a los usuarios existentes seguir conectados, pero que enviará a los nuevos usuarios a otras instancias.
- **TLS:** configure TLS e instale los certificados según sea necesario.

3.5.8 Configuración de la autenticación y la autorización

Consulte Autenticación y autorización para obtener más información sobre cómo elegir y configurar la autenticación y la autorización.

3.5.9 Verificación de la instalación

Tras instalar y configurar todos los componentes, deberá:

- Entrar a la Consola Administrativa de MSS (a través del equilibrador de carga de MSS).
- Desplácese a Gestionar sesiones > Añadir una nueva sesión y cree una sesión de prueba.
- Asigne la sesión de prueba a un usuario de prueba.
- Entre en el servidor de sesión como usuario de prueba a través del equilibrador de carga del servidor de sesión.
- Compruebe que la sesión asignada esté disponible, se abra y se pueda conectar.

3.5.10 Configuración de la entrada única (opcional)

A continuación, se muestran algunas consideraciones adicionales que se deben tener en cuenta al configurar la entrada única en una distribución de alta disponibilidad.

SAML (Lenguaje de marcado de aserción de la seguridad)

MSS La Guía del administrador de MSS incluye instrucciones de autenticación SAML.

1. Importe el equilibrador de carga de MSS en el elemento `servletcontainer.bcfks` de cada servidor MSS como certificado de confianza.
2. Actualice `management.server.url` en el archivo `container.properties` de cada servidor MSS para utilizar la dirección del equilibrador de cada MSS.
3. Defina la propiedad `management.server.callback.address` en cada archivo `container.properties` de MSS en una dirección a la que pueda acceder el servidor de sesión para una instancia de MSS específica.
4. Reinicie los servidores MSS.
5. Entre en la Consola Administrativa del servidor MSS activo para configurar la autenticación SAML. Confirme que el DNS del equilibrador de carga de MSS se utilice en el campo Assertion consumer service prefix URL (URL de prefijo del servicio de consumidor de aserción) y añada el DNS de los equilibradores de carga de MSS y Host Access for the Cloud en la lista blanca de SAML
6. Descargue y edite los metadatos del proveedor de servicios para insertar cada dirección del servidor MSS como AssertionConsumerService e importe los metadatos actualizados en el proveedor de identidades de SAML. Por ejemplo:

```
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-loadbalancer:8443/mss/callback/SAML2Client" index="0"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-server-1:8443/mss/callback/SAML2Client" index="1"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-server-2:8443/mss/callback/SAML2Client" index="2"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mss-server-3:8443/mss/callback/SAML2Client" index="3"/`
```

7. Ajuste el indicador de cookie SameSite en "None". Consulte Definición del atributo SameSite.

X.509

MSS La Guía del administrador de MSS incluye instrucciones de configuración de X.509.

En cada caso, el certificado utilizado debe tener un Nombre alternativo del firmante (SAN) que contenga todos los nombres DNS del servidor MSS, junto con el nombre DNS del equilibrador de carga.

1. Compruebe que el cortafuegos del servidor MSS permita el tráfico HTTP en el puerto de autenticación mutua; 8003 es el valor por defecto.
2. En cada MSS:
   - Sustituya el certificado de la entrada de motor servlet en los archivos `servletcontainer.bcfks`.
   - Sustituya el certificado de la entrada del sistema en los archivos `system-keystore.bcfks`.
3. Importe el certificado en el archivo `trustcerts.bcfks` de cada servidor de sesión como certificado de confianza.
4. Reinicie MSS y los servidores de sesión.
5. Configure los equilibradores de carga de MSS y HACloud para la transferencia directa de TLS.
6. Configure la autenticación X.509 como se documenta aquí: Cómo configurar la autenticación X.509.

3.5.11 Configuración de la lista de sesiones asignadas

Tiene la opción de usar la lista de sesiones asignadas para iniciar nuevas sesiones. Para ello, se necesita una configuración adicional:

- Configure el equilibrador de carga de MSS para mantener primero el SESSIONID y, a continuación, las cookies JSESSIONID. Es importante configurar la persistencia en ese orden específico.
- El acceso a la lista de sesiones asignadas debe realizarse a través del mismo equilibrador de carga de MSS que el servidor de sesión de HACloud utiliza para conectarse a MSS.

Más información:

- Proporcionar acceso a las sesiones de host
- Uso de equilibradores de carga

3.6 Instalación y configuración

MSS La ayuda de la Consola del administrador de MSS tiene información sobre la activación de productos.

Recuerde los siguientes puntos al realizar la instalación:

- **Archivos de activación**

  Los archivos de activación (activation.jaw) se utilizan para habilitar la funcionalidad del producto. Por ejemplo, el paquete de instalación incluye el archivo de activación necesario para habilitar la comunicación entre Host Access for the Cloud y MSS. Por lo general, se activa como parte del proceso de instalación. Los archivos de activación se descargan en la página de descargas de Micro Focus y son específicos para las distintas ediciones y plataformas admitidas por Host Access for the Cloud. Para trabajar en un entorno de producción, se requiere una activación.

  Si la activación no formó parte de la instalación, deberá abrir la Consola Administrativa y completar el proceso de activación (Configurar parámetros > Activación del producto). Consulte la sección Actualización de versiones anteriores para obtener información sobre cómo gestionar los archivos de activación al actualizar.

- **Proxy inverso IIS con Host Access for the Cloud**

  Si tiene previsto utilizar el Proxy inverso IIS, consulte Acceso a Host Access for the Cloud mediante el Proxy inverso IIS para conocer los requisitos previos y las instrucciones de configuración.

- **Seguridad**

  Host Access for the Cloud es compatible con los protocolos TLS y SSH para proteger los datos de misión crítica. Para proteger sus contraseñas y otros datos sensibles, los navegadores deben utilizar el protocolo HTTPS.

  Desde el punto de vista de la seguridad, resulta ventajoso ejecutar servicios como un usuario dedicado con un conjunto mínimo de privilegios. A esto se le conoce como identificador principal de privilegios mínimos.

  - En Linux, debe instalar HACloud y MSS como usuario dedicado (no "root") con privilegios reducidos.
  - En Windows, debe instalar primero el producto y, a continuación, ajustar el sistema para ejecutar el servicio del servidor de sesión como usuario dedicado con privilegios reducidos. Consulte Ejecución del servicio del servidor de sesión como usuario dedicado con privilegios reducidos para obtener instrucciones.
  - Instrucciones para realizar esta tarea en MSS.

3.6.1 Instalación en diferentes plataformas

Host Access for the Cloud y Java

Tanto el servidor de sesión como MSS requieren Java versión 11. Este requisito de Java se cumple durante la instalación, excepto en determinados sistemas, como Linux en Sistema Z, que requiere IBM JDK. La información sobre la opción nojdk está disponible en la sección de instalación de z/Linux.

Host Access for the Cloud y MSS requieren que la instalación de Java admita un nivel de cifrado sin límite. Encontrará más información en el sitio Web de Java.

En caso necesario, puede utilizar las variables de entorno especificadas en la opción nojdk e INSTALL4J_JAVA_HOME_OVERRIDE para especificar una instalación de Java específica.

Windows

Cuando se instalan servidores en una plataforma Windows, el instalador debe lanzarlo un usuario que sea administrador con privilegios administrativos. Una instalación básica de Windows se describe en Cómo obtener Host Access for the Cloud.

UNIX

- Debe instalarlo como “root” o utilizar una cuenta de usuario con privilegios de raíz para completar una instalación correcta. Si la instalación se ha concluido correctamente, la aplicación instalada se puede iniciar y gestionar mediante “root” o por quien se esté ejecutando como “root”.
- Si usted está trabajando con plataformas Linux, siga estos pasos para configurar el servidor de sesión para que se inicie automáticamente cuando su sistema arranque.
- Se necesitan privilegios elevados para abrir cualquier puerto de aplicación inferior al puerto 1024. Host Access for the Cloud no se iniciará mediante un número de puerto inferior a menos que disponga de suficientes privilegios del sistema para abrir puertos con números bajos.
- Puede utilizar el comando chmod para asignar privilegios de aplicación a usuarios distintos al usuario "root".
- Si está instalando en un sistema Linux sin cabeza y no hay fuentes instaladas en el sistema, puede encontrarse con este error de fuente: `java.lang.Error: Probable fatal error: No fonts found`. Asegúrese de que fontconfig o como mínimo una fuente esté instalada en el sistema para proceder con la instalación.

z/Linux (SUSE E11.x y RHEL 6.x)

Para sistemas como Linux en Sistema Z, que requieren IBM JDK, puede utilizar el medio de instalación “nojdk”, que no incluye JDK empaquetado.

- La instalación debe poder localizar un ejecutable de Java para iniciar. Si el instalador no puede encontrar un ejecutable de Java, puede ajustar la variable de entorno INSTALL4J_JAVA_HOME para referirse a un directorio de instalación de Java bin.
- Una vez arrancado, el programa de instalación buscará automáticamente JDKs compatibles con la versión en el sistema. Si se encuentra más de un JDK, se mostrará una lista en la que podrá elegir uno. Si solo se encuentra un JRE en el sistema, podrá continuar con la instalación, pero el servidor de Host Access for the Cloud no se ejecutará correctamente hasta que haya actualizado la propiedad `wrapper.java.command` ubicada en `sessionserver/conf/container.conf` para hacer referencia a una instalación de JDK.

Si es necesario, puede utilizar las variables de entorno indicadas anteriormente y la variable INSTALL4J_JAVA_HOME_OVERRIDE para especificar una instalación de Java específica.

Uso de una instalación sin supervisión

La instalación de Host Access for the Cloud se basa en la tecnología install4j, que admite el modo sin supervisión. La instalación sin supervisión permite instalar el producto de la misma manera en diversos equipos.

Para utilizar la instalación sin supervisión:

1. Instale el servidor de sesión en un equipo mediante el instalador automático. Puede utilizar la interfaz gráfica o el modo de consola (-c) para instalar el producto.

   El proceso de instalación crea un archivo de texto `response.varfile`, que contiene las opciones de instalación seleccionadas. El archivo se encuentra en `[instalación del servidor de sesión]\.install4j\response.varfile`.
2. Copie `response.varfile` en otro equipo en el que desee instalar el servidor de sesión.
3. Busque el archivo ejecutable correspondiente para instalar el producto. Lance el programa de instalación mediante el argumento `-q` y un argumento `-varfile` que especifique la ubicación de `response.varfile`.

   Por ejemplo, para instalar el servidor de sesión en una plataforma Linux de 64 bits con un archivo response.varfile ubicado en el mismo directorio, utilice este comando, donde `<2.4.x.nnnn>` indica la versión del producto y el número de compilación:

   ```
   hacloud-<2.4.x.nnnnn>-linuxx64.sh -q –varfile response.varfile
   ```

   También puede añadir la opción `-c` para realizar la instalación en el modo de consola, que proporcionará información como, por ejemplo, "Extrayendo archivos" y "Finalizando la instalación".

3.6.2 Configuración de una instalación incompleta

Si el servidor de sesión no puede recuperar un certificado de MSS o no puede completar el proceso de registro, es posible que se produzca una instalación incompleta. Siga los pasos para añadir servidores de sesión adicionales a fin de completar la instalación.

3.6.3 Actualización de versiones anteriores

> **Precaución**
>
> Si está realizando una actualización, es importante que elimine todos los archivos de activación de MSS asociados a versiones anteriores de Host Access for the Cloud. Dejar los archivos de activación obsoletos sin eliminar puede limitar el acceso a las sesiones.

1. Antes de continuar, realice una copia de seguridad de todos los cambios efectuados en `hacloud\sessionserver\conf\container.properties` o `hacloud\sessionserver\conf\container.conf`..
2. Instale Host Access for the Cloud.
3. Restaure los archivos de los que ha realizado una copia de seguridad en el paso 1 y reinicie el servidor de sesión.
4. Si no se ha realizado durante el proceso de instalación, instale el nuevo archivo o archivos de activación en MSS con ayuda de Consola Administrativa > Configurar parámetros > Activación del producto.

Configuración adicional

Para seguir utilizando los eventos del servidor en la versión 2.3.2 o anteriores de Reflection ZFE, copie los archivos JAR de eventos del servidor de `/webapps/zfe/WEB-INF/lib` en `/microservices/sessionserver/extensions/server` y vuelva a habilitar las extensiones.

3.6.4 Solución de problemas en la instalación

Para realizar una instalación correcta, asegúrese de haber tenido en cuenta los siguientes problemas comunes:

¿Están los archivos de activación instalados y activados en la Consola Administrativa?

MSS utiliza archivos de activación para habilitar la funcionalidad del producto. Con su instalación usted recibió un archivo de activación asociado con el tipo de host al que se está conectando. Por ejemplo, si tiene licencia para la edición Unisys y no se ha tratado como parte del proceso de instalación, deberá abrir la Consola Administrativa, ir a Configurar parámetros > Activación del producto y verificar que se encuentre en su ubicación el archivo de activación de Host Access for the Cloud Unisys.

¿Está configurado el MSS para HTTPS?

Conecte con el sistema en el que esté instalado el Servidor Administrativo y entre a este. En la Consola Administrativa, abra la sección Security Setup (Configuración de Seguridad) y anote la selección de protocolo.

✓ Compruebe que tanto MSS como Host Access for the Cloud utilizan certificados de confianza.

MSS importa certificados y claves privadas a `C:\ProgramData\Micro Focus\MSS\MSSData\certificates`. Consulte "Protección de las conexiones". Si no está utilizando certificados de confianza, ¿ha configurado Host Access for the Cloud para ejecutarse con HTTP?

✓ ¿Están configuradas correctamente las propiedades de conexión?

En el caso improbable de que tenga que verificar la información de conexión, el archivo `container.properties` del componente de administración y el servidor de sesión contiene las propiedades de conexión necesarias para establecer la conexión del servidor de sesión a MSS, así como la conexión del navegador al servidor de sesión. Puede encontrar el archivo en la instalación de Host Access for the Cloud, en `<directorio-de-instalación>/sessionserver/conf/container.properties`.

✓ La instalación no se completa en plataformas UNIX o Linux.

Debido a las bibliotecas de cifrado actualizadas, los clientes que utilizan instalaciones basadas en servidor sin periféricos pueden experimentar retrasos en el sistema si la entropía del sistema es demasiado baja. La entropía es la aleatoriedad recopilada por un sistema operativo para su uso en la criptografía. Esta aleatoriedad suele recopilarse de fuentes de hardware, como los movimientos del ratón. Una entropía insuficiente puede provocar que se bloquee el proceso de instalación o se reduzca el rendimiento del servidor. Algunas plataformas ya instalan y habilitan por defecto un servicio de entropía, por lo que el problema no se notará. Si es necesario, una solución de hardware o software puede corregir el problema.

> **Consejo**
>
> Puede mejorar la generación de entropía mediante la herramienta Haveged. Se trata de una herramienta que ayuda a solucionar situaciones de baja entropía en un dispositivo aleatorio de Linux, lo que puede producirse con algunas cargas de trabajo y, sobre todo, en servidores sin periféricos. Consulte https://wiki.archlinux.org/index.php/Haveged para obtener más información acerca de esta herramienta.

Consulte el artículo de Knowledge Base, Ensuring Sufficient Entropy to Avoid System Delays (Garantizar suficiente entropía para evitar retrasos del sistema).

✓ ¿El servidor en el que va a realizar la instalación está protegido para impedir el acceso al directorio temporal?

Consulte "Installation fails due to server preventing access to TEMP directory" (La instalación falla debido a que el servidor impide el acceso al directorio TEMP) en la sección de problemas conocidos para obtener información sobre este problema.

> **Consejo**
>
> Para otros problemas conocidos e información de solución de problemas, consulte Referencias técnicas.

3.7 Puertos

Los siguientes puertos se utilizan en Host Access for the Cloud y MSS.

3.7.1 Servidor de sesión de Host Access for the Cloud

Puerto	Componente	Acceso remoto necesario
7443	HTTPS: cliente web y conectores relacionados	Sí
32000-32001	Empaquetador de servicios	No

3.7.2 Servidor de Administración y Seguridad

Puerto	Componente	Acceso remoto necesario
443	HTTPS: Consola Administrativa, administración de ID de terminal, medición y administración de medición	Sí
7001	Comunicación TLS entre nodos de Cassandra	Sí [1]
7199	Supervisión de JMX de Cassandra	Sí [1]
8000	Autenticación X.509 en MSS mediante gestión centralizada	[4]
8001, 8002	AJP de Tomcat utilizado para la integración de IIS	Sí [3]
8003	Subsistema de confianza X.509	Sí [1]
8089	Servidor de cómputo	No [2]
8761	Registro de servicios	Sí [1]
9042	Puerto de cliente de Cassandra	No
9043	Cassandra sidecar	No
32000-32001	Monitorización del empaquetador de servicios	No
44000	Monitorización de JMX de MSS	No
Aleatorio	Puerto aleatorio requerido por JMX RMI de MSS	No
Aleatorio	Puerto aleatorio requerido por JMX RMI de Cassandra	No

[1] Se utiliza exclusivamente para la comunicación de backend entre servidores de sesión de MSS y HACloud.

[2] Normalmente se accede al servicio de medición a través del puerto 443.

[3] Solo se utiliza con la integración de IIS.

[4] No utilizado por los servidores de sesión de HACloud.

Los puertos del Servidor Administrativo de MSS y Host Access for the Cloud se pueden cambiar en función de sus necesidades de red. Para cambiar los puertos del servidor de sesión, consulte Cambio de puertos.

3.8 Configuración de la distribución

3.8.1 Configuración de la distribución

Al empezar a configurar una distribución de Host Access for the Cloud, deben tenerse en cuenta una serie de opciones posteriores a la instalación, así como cuestiones relacionadas con la seguridad.

3.8.2 Autenticación y autorización

Autenticación y autorización

En HACloud, la autenticación y la autorización las proporciona el Servidor de Administración y Seguridad (MSS) de Host Access y se configuran mediante la Consola Administrativa.

La autenticación valida la identidad de un usuario a partir de determinadas credenciales, como una combinación de nombre de usuario/contraseña o un certificado de cliente. A continuación, la autorización se utiliza para determinar las sesiones a las que puede acceder cada usuario.

HACloud admite los siguientes métodos de autenticación: None (Ninguno), LDAP, Single Sign-on through IIS (Entrada única mediante IIS), Windows Authentication via Kerberos (Autenticación de Windows mediante Kerberos), Windows Authentication via NTLMv2 (Autenticación de Windows mediante NTLMv2, obsoleto), X.509 Client Certificates (Certificados de cliente X.509), SiteMinder y SAML.

Para obtener información general sobre cómo seleccionar y configurar los métodos de autenticación, consulte Authentication and Authorization (Autenticación y autorización) en la documentación de MSS.

El modelo de distribución de alta disponibilidad contiene información importante sobre algunos métodos de autenticación durante la distribución en un entorno de HA.

> **Nota**
>
> Algunos métodos de autenticación requieren una configuración específica de HACloud. Para obtener más información, consulte los temas de este apartado en el índice.

Entrada única mediante IIS

MSS Consulte Single Sign-on through IIS (Entrada única mediante IIS) en la documentación de la Consola Administrativa de MSS para obtener más información.

Esta opción utiliza el servidor web Microsoft IIS.

Para habilitar Host Access for the Cloud para que funcione con este método de autenticación, añada la siguiente propiedad al archivo `<directorio de instalación>/sessionserver/conf/container.properties`:

```
management.server.iis.url=<url>
```

El valor de esta propiedad es la dirección del servidor web IIS y el puerto junto con la ruta / MSS. Por ejemplo: `http://server/mss`. Si la autenticación falla, es posible que deba eliminar el nombre de dominio para que las credenciales de dominio se ajusten a `IIS: http://server/mss`.

Autenticación de Windows: Kerberos

Kerberos es un protocolo de autenticación que utiliza tickets criptográficos para evitar la transmisión de contraseñas de texto sin formato. Los clientes obtienen tickets de concesión de tickets del Centro de distribución de claves Kerberos (KDC) y presentan esos tickets como sus credenciales de red para obtener acceso a los servicios.

En Host Access for the Cloud, Kerberos permite a los usuarios finales acceder a sus sesiones de host en el servidor de sesión sin que se soliciten las credenciales.

> **Nota**
>
> También se admite la autenticación Kerberos en los hosts AS/400, pero esta funcionalidad aún no está integrada en Kerberos para autenticar a los usuarios finales que acceden al servidor de sesión.

La autenticación Kerberos se habilita y se configura en MSS y, a continuación, se activa en cada servidor de sesión de la distribución. Consulte la documentación de Kerberos en MSS para obtener más información sobre los requisitos, además de sobre la configuración y el uso de Kerberos.

A continuación, se detallan los pasos generales para utilizar la autenticación Kerberos en Host Access for the Cloud.

PASOS PARA HABILITAR Y CONFIGURAR KERBEROS

1. Enable and configure Kerberos in MSS (Habilitar y configurar Kerberos en MSS)
2. Configurar cada servidor de sesión de HACloud para Kerberos
3. Configurar el navegador para Kerberos
4. Lanzar sesiones

Configurar Kerberos en el servidor de sesión

Para configurar un servidor de sesión para ejecutar Kerberos, edite el archivo service.yml y añada el perfil oauth:

1. Abra `<directorio de instalación>/sessionserver/microservices/sessionserver/service.yml` .
2. Añada oauth al conjunto de perfiles activos:

```
- name: SPRING_PROFILES_ACTIVE
  value: tls, oauth
```

3. Reinicie el servidor de sesión.

De forma opcional, si se configura una distribución de alta disponibilidad con equilibradores de carga, deben configurarse el perfil oauth (paso anterior) y las siguientes propiedades en el archivo service.yml de cada servidor de sesión.

1. Configure la dirección URL del equilibrador de carga de MSS. El servidor de sesión redirigirá a los usuarios a esta dirección URL para la autenticación.

```
- name: AUTHSVC_HOST
  value: {dirección URL del equilibrador de carga de MSS}
```

2. Configure el nombre de dominio del equilibrador de carga del servidor de sesión. MSS redirigirá de nuevo a este servidor después de que se autentique un usuario.

```
- name: PROXY_DOMAIN
  value: {nombre completo del equilibrador de carga del servidor de sesión}
```

3. Configure el puerto que se utilizará cuando se acceda al servidor de sesión a través del equilibrador de carga del servidor de sesión.

```
- name: PROXY_PORT
  value: {número de puerto del equilibrador de carga del servidor de sesión}
```

4. Reinicie el servidor de sesión.

Ejemplo

```
    - name: SPRING_PROFILES_ACTIVE
       value: tls, oauth
    (Si se utilizan equilibradores de carga...)
    - name: AUTHSVC_HOST
      value: https://mss-load-balancer.mydomain.com
    - name: PROXY_DOMAIN
      value: sessionserver-load-balancer.mydomain.com
    - name: PROXY_PORT
      value: 7443
```

Configurar el navegador para Kerberos

Para poder entrar a la sesión mediante Kerberos, el navegador debe estar configurado correctamente para la autenticación de Windows mediante Kerberos y el equipo debe ser miembro del dominio adecuado (dominio de Kerberos). Consulte la ayuda del navegador para obtener instrucciones sobre cómo habilitar Kerberos.

Lanzar sesiones

> **Nota**
>
> Actualmente, la autenticación Kerberos no es compatible con la lista de sesiones asignadas. Solo está disponible cuando se entra a través del servidor de sesión.

Las sesiones de HACloud no necesitan ninguna configuración adicional para iniciarse y autenticarse con Kerberos, siempre que el navegador se haya configurado correctamente para la autenticación de Windows / Kerberos. Solo tiene que ir a https://session-server-lb.mydomain.com:7443 y entrará automáticamente al servidor de sesión de HACloud.

SAML

SAML (Lenguaje de marcado de aserción de la seguridad) es un formato estándar abierto basado en XML que intercambia datos de autenticación y autorización entre un proveedor de identidad, (el servidor que emite las aserciones SAML y realiza la autenticación) y un proveedor de servicios, (el servidor web desde el que se accede a la información o los servicios). MSS actúa como el proveedor de servicios.

MSS Consulte SAML Configuration Steps (Pasos de configuración de SAML) en la documentación de la Consola Administrativa de MSS para obtener más información.

> **Nota**
>
> El indicador SameSite se debe ajustar cuando se utiliza SAML detrás de un equilibrador de carga. Consulte Definición del atributo SameSite.

SOLUCIÓN DE PROBLEMAS DE CONFIGURACIÓN

Si tiene problemas de autenticación o ve errores de tiempo límite de la sesión, consulte Troubleshooting SAML Setup en la Guía del administrador de MSS.

Autenticación X.509

La autenticación de cliente X.509 permite a los clientes autenticarse en servidores con certificados en lugar de con un nombre de usuario y una contraseña aprovechando la infraestructura de clave pública X.509 (PKI) estándar.

MSS incluye información adicional sobre la configuración de X.509.

HABILITAR LA AUTENTICACIÓN DE CLIENTE X.509

- Cuando el usuario accede al cliente Web mediante TLS, el navegador envía un certificado al servidor de sesión que identifica al usuario final y completa el protocolo de enlace TLS.
- El servidor de sesión hace referencia a su almacén de confianza para comprobar el certificado del cliente y verificar su confianza.
- Una vez completada la negociación TLS (el servidor de sesión confía en el usuario final), el servidor de sesión envía el certificado público del usuario final a MSS para su posterior validación.
- MSS también comprueba que se confía en el certificado de los usuarios finales mediante su almacén de confianza.
- Cuando MSS finalice la validación, el usuario final se habrá autenticado correctamente.

La cadena de certificado completa del cliente debe estar presente en el servidor de sesión y en los almacenes de confianza de MSS o también puede estar firmada por una autoridad certificadora presente en los almacenes de confianza.

El navegador determina el certificado de cliente que se enviará mediante una configuración específica del navegador o la tarjeta inteligente.

Pasos básicos

1. Confíe en los certificados en el servidor de sesión y MSS si aún no lo ha hecho.
2. Reinicie los servidores.
3. Configure X.509 en la Consola Administrativa de MSS.

Confiar en el certificado en MSS y el servidor de sesión

- Confiar en el certificado en MSS

  El almacén de confianza de MSS puede contener ya su certificado de autoridad firmante. Éste suele ser el caso con autoridades firmantes de certificados bien conocidas y, de ser así, puede saltarse este paso.

  Para comprobarlo:

- Abra la Consola Administrativa, haga clic en Configurar parámetros y abra la ficha Certificados de confianza. Abra Trusted Root Certificate Authorities (Autoridades certificadoras raíz de confianza) para ver una lista de los certificados disponibles.
- Si el certificado no se encuentra en la lista, deberá instalar la CA raíz firmante en MSS mediante las indicaciones y la documentación de la Consola Administrativa.
- Confiar en el certificado en el servidor de sesión

  Para instalar el certificado en el servidor de sesión:

  En `<directorio_de_instalación>\sessionserver\etc`, importe el certificado:

```
keytool -importcert -file <cert-file> -alias <alias-to-store-cert-under>
-keystore trustcerts.bcfks -storetype bcfks -providername BCFIPS
-providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
-providerpath ../lib/bc-fips-*.jar
-storepass changeit
```

Reinicie todos los servidores

Para que la configuración tenga efecto, deberá reiniciar todos los servidores.

Configurar X.509 con LDAP a prueba de fallos en la Consola Administrativa de MSS

Una vez instalados los certificados, puede habilitar X.509 con la opción para volver a la autenticación LDAP en Consola Administrativa del Servidor de Administración y Seguridad | Configurar parámetros | Autenticación y autorización. Consulte la ayuda en línea de la Consola Administrativa para obtener descripciones de las opciones de configuración.

HABILITACIÓN DE X.509 MEDIANTE UN EQUILIBRADOR DE CARGA CONFIGURADO PARA LA FINALIZACIÓN DE TLS

En esta configuración, el equilibrador de carga proporciona autenticación de usuario final al validar su certificado de cliente. Sin embargo, el certificado de cliente debe enviarse a todos los sistemas de MSS para poder identificar al usuario de entrada.

Si el equilibrador de carga se ha configurado para finalizar la conexión TLS, el certificado del usuario puede añadirse a un encabezado HTTP; el servidor de sesión puede extraerlo y, a continuación, transferirlo a MSS para la autorización. Para transferir el certificado en un encabezado, defina primero el nombre del encabezado en el archivo `container.properties` del servidor de sesión de HACloud:

Para transferir el certificado en un encabezado

1. Defina el nombre del encabezado en el archivo container.properties del servidor de sesión de HACloud:

   `x509.header.client.cert=X-SSL-Client-Cert`

2. Defina el valor de encabezado en el certificado del usuario, en la configuración del equilibrador de carga. Por ejemplo, mediante una iRule de BigIP:

   `HTTP::header insert X-SSL-Client-Cert [URI::encode $client_cert]`

   En este caso, se presupone que `$client_cert` se ha definido en el certificado del usuario en formato PEM. Si el certificado del usuario está en formato DER, utilice la codificación Base64:

```
HTTP::header insert X-SSL-Client-Cert [b64encode $client_cert]
```

La codificación del certificado garantiza que el valor del encabezado sea una línea de texto ASCII. Esto es necesario para que el servidor de sesión de HACloud lea el valor.

> **Nota**
>
> La autenticación del certificado de cliente debe realizarse entre el equilibrador de carga y el servidor de sesión. El equilibrador de carga debe configurarse para que envíe su certificado al servidor de sesión y la CA del equilibrador de carga debe estar presente en el almacén de confianza del servidor de sesión.

3. Después de configurar el equilibrador de carga para que envíe su certificado al servidor de sesión de HACloud y de configurar el certificado del usuario para que se transfiera en el encabezado, reinicie el servidor de sesión.

Si se conecta con un certificado o una tarjeta inteligente a través del equilibrador de carga, la autenticación y la autorización como el usuario representado por el certificado se completarán correctamente. Para verificar el funcionamiento correcto, defina el nivel de registro del servidor de sesión en DEBUG (depuración) y examine el archivo sessionserver.log en busca de entradas como las siguientes:

```
Intentando extraer el certificado del encabezado X-SSL-Client-cert.
El valor <valor de DN> del usuario se ha autenticado previamente desde <dirección IP>.
```

Configuración adicional

Por defecto, el almacén de confianza del servidor de sesión de HACloud contiene los certificados de CA de Java. Por lo tanto, el servidor de sesión de HACloud aceptará cualquier certificado de cliente firmado por CA conocidas. Para garantizar que solo los equilibradores de carga deseados se conecten al servidor de sesión, debe eliminar los certificados de CA de Java del almacén de confianza y asegurarse de que solo los certificados necesarios estén instalados en el almacén de confianza.

Para filtrar los certificados de cliente permitidos por nombre completo (DN) del emisor, defina las siguientes propiedades del archivo `container.properties` del servidor de sesión de HACloud:

```
X509.client.cert.issuer=<Valor de DN>
X509.client.cert.subject=<Valor de DN del asunto>
X509.client.cert.serial=<Número de serie>
X509.client.cert.sha1=<Huella SHA1>
X509.client.cert.sha256=<Huella SHA256>
```

Los valores de DN deben coincidir exactamente con el emisor de certificado o el nombre completo (DN) del asunto del equilibrador de carga. El valor de número de serie debe ser un valor decimal (base 10). Los valores de huella SHA1 y SHA256 se deben especificar en formato hexadecimal. Una vez que se haya definido alguna de estas propiedades, se comprobarán los atributos del certificado entrante para garantizar que coincidan con los valores de propiedades especificados. No se podrá completar la autorización si alguno de estos valores no coinciden.

3.8.3 Configuración de la medición

MSS ofrece funciones de cómputo para supervisar las sesiones de host. Consulte Metering (Medición).

El Servidor de Administración y Seguridad ofrece capacidad de medición para supervisar sesiones de host.

Antes de configurar el cómputo para Host Access for the Cloud, compruebe que se ha habilitado el cómputo para MSS. Puede encontrar instrucciones completas en la Guía de instalación.

En Host Access for the Cloud, la medición se establece de forma general para todas las sesiones de emulación creadas por el servidor de sesión. Los ajustes se configuran en el archivo `sessionserver/conf/container.properties`.

Propiedad	Descripción
metering.enabled	Active o desactive la medición con el valor "true" o "false". Cualquier valor distinto de "true" desactiva la medición.
metering.host.required	Determina si la sesión puede conectarse con el host incluso si no se pueden contactar con el servidor de medición. "True" significa que las conexiones de sesión fallarán si el host de medición no está disponible. "False" significa que las conexiones de sesión seguirán funcionando si el host de medición no está disponible.
metering.server.url	Especifica el nombre o la dirección del servidor de medición, el puerto, el protocolo y el contexto webapp. La sintaxis es `host:puerto|protocolo|contexto`. La sintaxis es la misma que utiliza el servidor MSS en el archivo `MssData/serverconfig.props` para el registro de servidores de medición. La sección host:port de la URL debe escapar el carácter ":". Por ejemplo, `10.10.11.55\:443`.

Adiciones de ejemplo a `sessionserver/conf/container.properties`

```
metering.enabled=true
metering.host.required=false
metering.server.url=10.10.11.55\:443|https|meter
```

Nota

En el caso de que todas las licencias estén en uso y que intente establecer una conexión, la sesión se desconectará. Para determinar si el host se ha desconectado o si el servicio de medición ha interrumpido la conexión, consulte el archivo `<directorio_de_instalación>/sessionserver/logs/sessionserver.log` .

3.8.4 Configuración del Administrador de ID de Terminal

MSS La configuración del Administrador de ID de Terminal requiere que esta función esté habilitada en MSS.

El Servidor de Administración y Seguridad ofrece un Administrador de ID de Terminal para agrupar IDs de terminal, monitorizar el uso de IDs y gestionar los valores de tiempo de espera de inactividad para usuarios específicos, conservando así los recursos de ID de terminal y reduciendo considerablemente los costes operativos.

El complemento Administrador de ID de Terminal requiere una licencia por separado.

Antes de configurar el Administrador de ID de Terminal para Host Access for the Cloud, asegúrese de que ha habilitado esta opción para MSS. Encontrará instrucciones completas en la Guía de Instalación de MSS.

> **Consejo**
>
> Si MSS y Host Access for the Cloud están instalados en el mismo equipo, no se necesita ninguna configuración adicional.

Configuración del Administrador de ID de Terminal para Host Access for the Cloud

Para configurar el Administrador de ID de Terminal para Host Access for the Cloud, debe indicar la dirección correcta al Administrador de ID de terminal.

1. Abra el archivo `sessionserver/conf/container.properties`.
2. Actualice `id.manager.server.url=https://localhost:443/tidm` para reflejar la dirección del Administrador de ID de Terminal configurada en el Servidor de Administración y Seguridad.
3. Reinicie el servidor de sesión.

3.8.5 Configuración del inicio de sesión único automatizado para mainframe

MSS Automated Sign-On for Mainframe - Administrator Guide (Inicio de sesión automatizado para mainframe: guía del administrador) contiene información adicional sobre la configuración de esta opción.

El Inicio de Sesión Automatizado para Mainframe es un complemento del Servidor de Administración y Seguridad que habilita a un usuario final para autenticarse en un cliente de emulación de terminal y cerrar sesión automáticamente en una aplicación de host en el mainframe de z/OS.

1. Instale y configure el complemento Inicio de sesión automatizado para mainframe para el Servidor de Administración y Seguridad. Puede encontrar instrucciones completas en Automated Sign-On for Mainframe - Administrator Guide (Inicio de sesión automatizado para mainframe: guía del administrador).
2. Después de haber concluido la configuración del Servidor de Administración y Seguridad, abra la Consola Administrativa para añadir sesiones y asignar usuarios a esas sesiones. Durante este proceso, puede completar la configuración adicional necesaria para implementar el inicio de sesión automatizado.
3. Una macro de Host Access for the Cloud envía el nombre de usuario de mainframe del usuario y el ticket de paso a la aplicación de host. El usuario inicia sesión entonces automáticamente. Como ayuda para crear la macro:
    - La API de macros contiene el objeto AutoSignon que proporciona los métodos necesarios para crear una entrada a la sesión de Host Access for the Cloud que se utilizará con la función de inicio de sesión único para mainframe).
    - También puede hacer referencia a la macro de ejemplo Inicio de sesión único para mainframe, que utiliza el objeto AutoSignon para crear una macro que utiliza las credenciales asociadas a un usuario para obtener un ticket de paso del servidor de acceso a certificados digitales (DCAS).

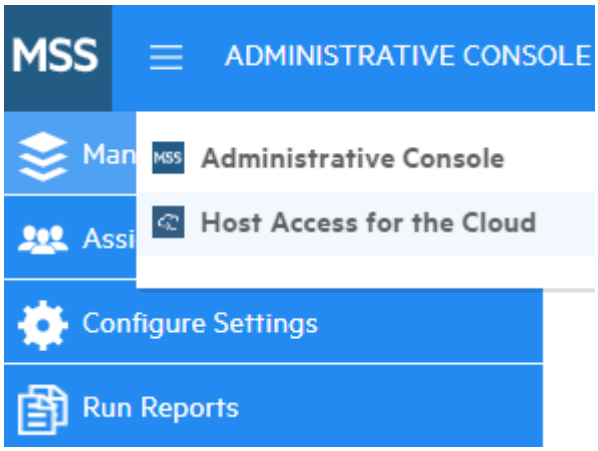
3.8.6 Configuración de Kerberos para el inicio de sesión único de AS/400

Kerberos es un protocolo de autenticación que utiliza tickets criptográficos para evitar la transmisión de contraseñas de texto sin formato. Los servicios de cliente obtienen tickets de concesión de tickets del Centro de distribución de claves Kerberos (KDC) y presentan esos tickets como sus credenciales de red para obtener acceso a los servicios.

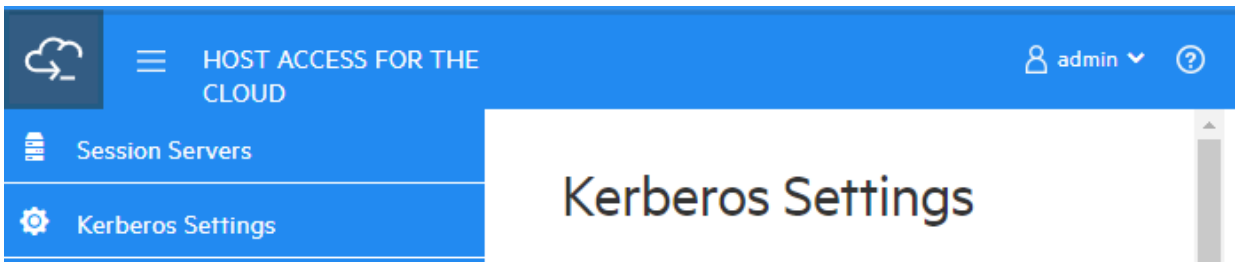
> **Nota**
>
> También se admite la autenticación Kerberos para los usuarios finales que acceden al servidor de sesión, aunque esta funcionalidad aún no está integrada en la autenticación Kerberos para AS/400. Esta función permite la entrada automática desde el servidor de sesión a un host AS/400. MSS debe configurarse con un método de autenticación que proporciona un principio de usuario que pueda resolverse en el dominio de Active Directory de Kerberos, por ejemplo, LDAP, SAML o SiteMinder. Se requiere un servidor de Active Directory de Windows.

Al utilizar Kerberos, después de un inicio de sesión de dominio inicial, no será necesario que los usuarios introduzcan sus credenciales cuando accedan a sesiones de AS/400 en Host Access for the Cloud.

Puede encontrar una descripción general de cómo habilitar y utilizar esta función en la documentación del panel Consola Administrativa de MSS > Host Access for the Cloud.



Seleccione Host Access for the Cloud en la lista desplegable y, a continuación, seleccione Configuración de Kerberos y haga clic en el botón Ayuda:



3.9 Protección de las conexiones

3.9.1 Proteger conexiones

Host Access for the Cloud utiliza la Seguridad de la capa de transporte (TLS) para proteger de forma criptográfica la comunicación entre los navegadores web de los clientes, el servidor de sesión, MSS y los hosts de backend.

Descripción general

Infraestructura de clave pública (PKI)

TLS utiliza la infraestructura de clave pública (PKI) para implementar la seguridad. PKI utiliza claves tanto públicas como privadas para proteger la comunicación entre el cliente y el servidor. Las claves públicas y privadas están relacionadas matemáticamente, pero no son las mismas. Esto significa que un mensaje cifrado con una clave pública solo se puede descifrar mediante la clave privada. Estas claves se conocen de forma conjunta como par de claves.

Certificados

Los certificados digitales son credenciales que verifican las identidades de individuos, equipos y redes. Proporcionan el enlace entre una clave pública y una empresa verificada (firmada) por un tercero de confianza, que se conoce como autoridad certificadora (CA). Los certificados digitales permiten distribuir cómodamente claves de cifrado públicas de confianza.

Almacenes de claves

Los certificados y las claves privadas se almacenan en los almacenes de claves de Java. Todas las entradas del almacén de claves se determinan mediante un identificador único conocido como alias. A menudo, las claves privadas y los certificados, con su correspondiente clave pública, se almacenan en ubicaciones distintas a la de los certificados recibidos de otras partes que se utilizan por motivos de confianza. A este almacén de claves independiente se le conoce como almacén de confianza. Un almacén de confianza contiene certificados de partes con las que espera comunicarse o de autoridades certificadoras en las que confía para identificar a otras partes.

La instalación segura por defecto

Durante la instalación de HACloud y MSS, los certificados autofirmados se generan, se intercambian y, a continuación, se utilizan para proteger todas las comunicaciones entre el servidor de sesión, los navegadores Web y MSS. Los certificados autofirmados son certificados de identidad que están firmados por la misma entidad cuya identidad certifican.

Tanto los servidores de sesión como los de MSS utilizan los certificados autofirmados generados para identificarse en clientes remotos como, por ejemplo, navegadores Web, y otros servidores de

sesión y de MSS. Estos certificados autofirmados y sus claves privadas se almacenan en sus respectivos almacenes de claves.

Para que se establezca la comunicación segura entre clientes (navegadores Web, servidores de sesión y servidores MSS), los clientes deben confiar en el certificado autofirmado generado. El servidor de sesión confía en el certificado de MSS durante la instalación y lo guarda en el almacén de confianza. Del mismo modo, durante la instalación, MSS recupera el certificado del servidor de sesión, confía en él y lo guarda en el almacén de confianza.

Consulte Almacenes utilizados por el servidor de sesión

MSS La Ayuda de la Consola Administrativa de MSS incluye información detallada sobre la seguridad general y los certificados en General Security and Certificates.

3.9.2 Almacenes utilizados por el servidor de sesión

Certificados de identidad

Para mayor comodidad, los certificados de identidad de cada tipo de servidor están disponibles en las siguientes ubicaciones, fuera de sus respectivos almacenes de claves que se mencionan a continuación.

- Certificado del servidor de sesión HACloud: `HACloud/sessionserver/etc/<nombre-equipo>.cer`
- Certificado de MSS: `MSS/server/etc/<nombre-equipo>.cer`

Almacenes de claves y de confianza del servidor de sesión

Los almacenes de claves y de confianza utilizados por el servidor de sesión se describen en la tabla siguiente.

- Ubicación: `HACloud/sessionserver/etc/`
- Tipo: `bcfks` (almacén de claves Bouncy Castle FIPS)
- Contraseña por defecto: `changeit`

Almacén de claves	Función
keystore.bcfks	• Almacén de credenciales para las conexiones TLS entrantes • Contiene el certificado servido por el servidor de sesión. • Se utiliza para el servidor web incrustado (Jetty). • Se crea al inicio.
trustcerts.bcfks	• Almacén de confianza para las conexiones TLS salientes. • Se utiliza para verificar los servidores a los que se conecta el servidor de sesión, como MSS. • Almacén de confianza para verificar las conexiones entrantes de equilibrador de carga cuando se utiliza la autenticación X.509 a través de un equilibrador de carga. • Se crea al inicio.

> **Nota**
>
> MSS administra la confianza de las conexiones de emulación de host. Consulte Establecer una conexión de emulación segura en un host de confianza.

Para cambiar una contraseña del almacén de claves o el almacén de confianza

En `HACloud/sessionserver/conf/container.properties`, actualice estos parámetros:

- `server.ssl.key-store-password`
- `server.ssl.trust-store-password`

Por motivos de seguridad, lo mejor es utilizar una contraseña ofuscada. Para generar una, ejecute el siguiente comando desde el directorio HACloud/sessionserver:

```
../java/bin/java -cp ./lib/jetty-util-<versión>.jar
org.eclipse.jetty.util.security.Password passwordToObfuscate
```

3.9.3 Herramientas

- KeyStore Explorer - Puede beneficiarse de la utilidad KeyStore Explorer para proporcionar una interfaz de usuario sencilla para crear peticiones de firma (CSR) e importar certificados firmados por una CA en Host Access for the Cloud.
- Para lanzar KeyStore Explorer en Windows, ejecute `\HACloud\utilities\keystore-explorer.bat` como administrador o como usuario con derechos administrativos.
- Para lanzar KeyStore Explorer en UNIX, ejecute `hacloud\utilities\keystore-explorer.sh` como administrador o como usuario con derechos administrativos.

La utilidad tiene un sistema de ayuda online para guiarle por la interfaz de usuario.

- Java Keytool - La Herramienta de Gestión de Claves y Certificados de Java gestiona un almacén de claves criptográficas, cadenas de certificados X.509 y certificados de confianza. Utiliza una interfaz de línea de comandos. La documentación de la Herramienta de Gestión de Claves y Certificados de Java está disponible para ambas plataformas Unix y Windows:
  - Unix
  - Windows

3.9.4 ¿Cómo puedo...?

Solicitar un certificado de identidad digital (petición de firma del certificado)

Términos utilizados:

- Clave privada: una clave secreta conocida solo por el propietario, que se utiliza con un algoritmo para cifrar o descifrar datos.
- Par de claves: clave privada y su cadena de certificado asociada.
- Nombre completo: la información de identificación de un certificado. Un certificado contiene información de DN tanto del propietario/solicitante del certificado (denominado Nombre completo del sujeto) como de la CA que ha emitido el certificado (denominado Nombre completo del emisor).
- Certificado X. 509: un certificado digital que utiliza la norma internacional de infraestructura de clave pública (PKI) X.509 ampliamente aceptada para comprobar que una clave pública pertenece al usuario.

Antes de crear una petición de firma del certificado (CSR), el solicitante debe generar primero un par de claves, manteniendo el secreto de la clave privada. La CSR contiene información que identifica al solicitante (como un nombre completo en el caso de un certificado X.509), que debe firmarse mediante la clave privada del solicitante. La CSR contiene también la clave pública seleccionada del solicitante.

CÓMO CREAR UNA CSR UTILIZANDO EL KEYSTORE EXPLORER

Para crear una CSR, deberá crear un par de claves y generar entonces una solicitud de certificado. Si no necesita actualizar la información del certificado, puede omitir la creación del par de claves y proceder con la generación de la solicitud del certificado.

- Crear un nuevo par de claves
  - **a.** En el menú Herramientas, seleccione Generar par de claves.
  - **b.** En el cuadro de diálogo Generar par de claves, introduzca la información adecuada del algoritmo y los detalles del certificado. Haga clic en Aceptar.
  - **c.** Especifique el alias pertinente (*servlet-engine*) y la contraseña por defecto (*changeit*).
- Generar una solicitud de certificado
  - **a.** Seleccione el par de claves que acaba de crear.
  - **b.** En el menú contextual, seleccione Generar CSR.
  - **c.** Navegue hasta la ubicación de la instalación en la que desee generar la CSR e introduzca el nombre de archivo. Haga clic en Aceptar.

CÓMO CREAR UNA CSR UTILIZANDO LA JAVA KEYTOOL

- Cree un par de claves (sustituya el parámetro `dname` por uno propio) en la carpeta `sessionserver/etc` :

```
 ..\..\java\bin\keytool.exe -genkeypair -dname "CN=hacloud-1.microfocus.com, O=Micro Focus, C=US"
-alias servlet-engine -keyalg RSA -keysize 2048 -keystore keystore.bcfks -validity 1095 -
storetype bcfks -storepass changeit -keypass changeit -providername BCFIPS -providerpath ../lib/
bc-fips-*.jar -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

- Generar solicitud de certificado:

```
  ..\..\java/bin\keytool -certreq -alias servlet-engine -keystore keystore.bcfks -file
cert_request.csr -ext ExtendedkeyUsage=serverAuth -storetype bcfks -storepass changeit -
providername BCFIPS -providerpath ../lib/bc-fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

Después de recibir el certificado de la CA, lo importará en Host Access for the Cloud.

Sustituir el certificado del servidor de sesión

La instalación está protegida mediante certificados autofirmados. No se confía automáticamente en los certificados autofirmados, aunque sean tan seguros como los certificados comerciales. Por lo tanto, son difíciles de administrar. Los certificados comerciales son necesarios cuando se requiere compatibilidad general con el certificado; afortunadamente, la mayoría de los navegadores Web y sistemas operativos ya son compatibles con muchas autoridades certificadoras comerciales.

Información que debe conocer:

- Ubicación del almacén de claves: `/etc/keystore.bcfks`
- Formato del almacén de claves: `bcfks` (Bouncy Castle FIPS)
- Contraseña por defecto: *changeit*
- Alias del par de claves: *servlet-engine*

La forma de reemplazar el certificado autofirmado varía en función de si sustituye el certificado autofirmado por uno obtenido a través de una CSR en el almacén de claves por defecto o si lo sustituye por su propio almacén de claves y certificado que no son por defecto.

Más información

- Sustituir el certificado autofirmado por la respuesta del certificado de la autoridad certificadora (CA)
- Sustituir el certificado por el almacén de claves que no es por defecto

Sustituir el certificado autofirmado por la respuesta del certificado de la autoridad certificadora

1. Cree una petición de firma del certificado (CSR) para el servidor de sesión y envíela a la autoridad certificadora (CA) de su elección. Cuando haya recibido el certificado firmado de la CA:
2. Importe la cadena o el certificado firmados por la CA en el almacén de claves del servidor de sesión.

   Puede realizar estas tareas mediante las instrucciones de la línea de comandos de Java Keytool o KeyStore Explorer. Independientemente de la herramienta utilizada, si la respuesta de la CA contiene archivos de certificados raíz y de certificados intermedios independientes, importe primero el certificado raíz en el almacén de claves y, a continuación, el certificado intermedio.

   - **Utilizar el KeyStore Explorer**
   - Abra `keystore.bcfks` en KeyStore Explorer. Utilice la contraseña *changeit*.
   - Si se dispone de certificados raíz e intermedios separados, desde la barra de herramientas seleccione Importar certificado de confianza para importar certificados.
   - Seleccione el par de claves servlet-engine. Haga clic derecho y seleccione Importar respuesta de CA para importar el archivo al par de claves.
   - Si se le pide, introduzca la contraseña *changeit*.
   - Navegue hasta la ubicación en la que esté guardado el archivo CA Reply, seleccione el archivo y haga clic en Importar.
   - **Utilizar Java Keytool**

   Estos ejemplos utilizan el comando keytool en el directorio `sessionserver/etc`.

   - Para Windows:

   Importar certificados raíz de CA y certificados intermedios

```
   ..\..\java\bin\keytool.exe -importcert -alias rootca -trustcacerts -file <RootCA.cer> -keystore
keystore.bcfks –storetype bcfks -storepass changeit
   ..\..\java\bin\keytool.exe -importcert -alias intermediateca -trustcacerts -file
<IntermediateCA.cer> -keystore keystore.bcfks –storetype bcfks -storepass changeit -providername
BCFIPS -providerpath ../lib/bc-fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

   Importar CA Reply

```
  ..\..\java\bin\keytool.exe -importcert -alias servlet-engine -trustcacerts -file
<CertChainFromCA.p7b> -keystore keystore.bcfks –storetype bcfks -storepass changeit -providername
BCFIPS -providerpath ../lib/bc-fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

   - En Unix:

   Importar certificados raíz de CA y certificados intermedios

```
  ../../java/bin/keytool -importcert -alias rootca -trustcacerts -file <RootCA.cer> -keystore
keystore.bcfks –storetype bcfks -storepass changeit -providername BCFIPS -providerpath ../lib/bc-
fips-*.jar -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

```
../../java/bin/keytool -importcert -alias intermediateca -trustcacerts -file <IntermediateCA.cer>
-keystore keystore.bcfks -storetype bcfks -storepass changeit -providername BCFIPS -providerpath ../
lib/bc-fips-*.jar -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

Importar CA Reply

```
../../java/bin/keytool -importcert -alias servlet-engine -trustcacerts -file <CertChainFromCA.p7b>
-keystore keystore.bcfks -storetype bcfks -storepass changeit -providername BCFIPS -providerpath ../
lib/bc-fips-*.jar -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

3. Confíe en el nuevo certificado en MSS.

- Como administrador, entre en MSS.
- En el panel izquierdo, haga clic en Configurar parámetros > Certificados de confianza.
- Seleccione Subsistema de confianza. La lista contiene los certificados que son de confianza para MSS.
- Haga clic en IMPORTAR para añadir el certificado del servidor de sesión a la lista.
- No es necesario repetir el procedimiento en cada instancia de MSS. Los cambios se replican automáticamente en otras instancias de MSS del clúster.

Puede encontrar información detallada en la Ayuda de la Consola Administrativa: Trusted Certificates (Certificados de confianza/).

Sustituir el certificado por el almacén de claves que no es por defecto

Puede utilizar un almacén de claves que no sea por defecto (`sessionserver/etc/keystore.bcfks` `sessionserver/etc/keystore.bcfks`) para guardar los certificados firmados por la CA.

Especifique las siguientes propiedades en `sessionserver/conf/container.properties` :

```
server.ssl.key-store
server.ssl.key-store-password
```

Donde la ruta del almacén de claves se ha establecido en el nombre de archivo del almacén de claves que no es por defecto y la contraseña del almacén de claves se ha establecido en el valor ofuscado generado por el siguiente comando del directorio `sessionserver` :

```
../java/bin/java -cp ./lib/jetty-util-<versión>.jar org.eclipse.jetty.util.security.Password passwordToObfuscate
```

Por ejemplo:

```
server.ssl.key-store=${server.home}/etc/custom.bcfks
server.ssl.key-store-password=OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0
```

> **Consejo**
>
> Para evitar confusiones, suprima el almacén de claves por defecto.

Para impedir que se genere el almacén de claves por defecto cuando se inicie el servidor, abra `/conf/product-core-ctx.xml` en un editor de texto y elimine o marque con comentarios la sección *servletEngineKeystoreGenerator*. Reinicie el servidor de sesión.

Sustituir el certificado de MSS

Consulte cómo sustituir el certificado de MSS en el tema General Security and Certificates (Seguridad general y certificados).

Durante la instalación, para establecer una comunicación segura, el servidor de sesión ha confiado en el certificado de MSS existente. Si se actualiza el certificado de MSS, todos los servidores de sesión de HACloud deben volver a confiar en él.

Para sustituir el certificado de MSS

- Para confiar en el nuevo certificado de MSS, impórtelo en el almacén de confianza del servidor de sesión con el alias mss. Consulte Importar un certificado en el almacén de confianza del servidor de sesión.
- Debe importar el nuevo certificado de MSS en cada servidor de sesión.

Establecer una conexión de emulación segura en un host de confianza

Siga estos pasos para configurar una conexión TLS entre el servidor de sesión de Host Access for the Cloud y un host que admita TLS:

1. Configure el almacén de claves de confianza en MSS.
2. Configure la sesión de terminal.

CÓMO CONFIGURAR EL ALMACÉN DE CLAVES EN MSS

MSS Abra la Consola Administrativa del MSS > Configurar parámetros > Certificados de Confianza y seleccione Clientes de Emulador de Terminal. Puede acceder a la documentación para la Consola Administrativa haciendo clic en el icono de Ayuda en la parte superior derecha de la página.

Para que una sesión confíe en el host TLS al que se conecta, el certificado público del host se debe añadir a un almacén de claves de confianza con ayuda del Servidor de Administración y Seguridad (MSS). La sesión de Host Access for the Cloud recupera este certificado la primera vez que se conecta una sesión.

Si el certificado se ha añadido correctamente al almacén de claves de confianza del servidor de MSS, regresará a la lista de certificados, en la que debe encontrarse el nuevo host.

CÓMO CONFIGURAR UNA SESIÓN DE TERMINAL DE HACLOUD

En función del tipo de host, puede configurar una sesión de terminal mediante diferentes protocolos de seguridad.

Tipo	Procedimiento
Utilizar TLS	Para conectarse al nuevo host de confianza mediante TLS, configure como siempre una sesión de terminal y, en el cuadro de diálogo Configuración, especifique TLS como protocolo de seguridad. Asegúrese de especificar el puerto TLS correcto para la conexión.
Utilizar Secure Shell (SSH) con tipos de host VT	Secure Shell ofrece comunicaciones cifradas entre el cliente y un host VT. MSS tiene una lista de hosts conocidos que contiene las claves públicas de los hosts a los que se puede conectar para utilizar SSH. Las conexiones SSH se pueden establecer sólo a hosts que ya son de confianza de un administrador. La primera vez que se establece una conexión SSH de una sesión a un host, el archivo de hosts conocidos se descarga desde MSS en el servidor de sesión. Cuando usted intente crear o editar una sesión utilizando SSH en el panel de administración de sesión, se le avisará si la clave no es reconocida como de confianza y se le consultará si desea confiar en la clave y continuar. • Si ingresa Sí, se confiará en el host y será añadido a la lista de hosts conocidos y a usted se le pedirá ingresar la contraseña del host SSH. • Si no responde Sí, el host seguirá sin ser de confianza y la sesión se desconectará. También puede configurar manualmente el archivo de hosts conocidos SSH. Para ello, establezca una conexión SSH desde una sesión al host y añada la huella digital de la clave del host remoto a la lista de hosts conocidos en MSS.
Configurar el archivo de hosts conocidos para conexiones SSH en MSS	

1. Localice el archivo de clave pública en el nuevo host SSH como, por ejemplo, `/etc/ssh/ssh_host_rsa_key.pub`. Solamente `ssh-rsa` y `ssh-dss` son válidos como tipos de clave pública para entradas known_hosts de MSS. El formato de la clave pública del host puede ser OpenSSH, Base64-encode, .DER o .PFX. El archivo debe seguir el formato: nombre de host, dirección IP tipo de clave clave. Por ejemplo, una entrada de clave pública debe tener este aspecto: `alpsuse132, 10.117.16.232 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA.....`
2. Inicie sesión en MSS (por ejemplo, `http://mycompany.com/adminconsole`).
3. Abrir la Consola Administrativa.
4. Haga clic en Configurar parámetros > Secure Shell e importe la clave pública. Después de que la clave pública se importe al archivo de hosts conocidos, regresará a la página Secure Shell Known Hosts (Host conocidos de Secure Shell) y el nuevo host aparecerá en la lista.
5. Siga las direcciones en MSS para importar un host conocido. Después de que la clave pública se importe al archivo de hosts conocidos, regresará a la página Secure Shell Known Hosts (Host conocidos de Secure Shell) y el nuevo host aparecerá en la lista.

Configurar eventos del servidor para realizar llamadas TLS salientes desde el servidor de sesión

Al escribir el código Java que se ejecuta en los eventos del servidor, es posible que desee realizar llamadas salientes a servidores remotos mediante TLS. Si se conoce el servidor remoto, el servidor de sesión ya puede confiar en él y no hay nada más que configurar. Sin embargo, a veces no se conoce el servidor remoto, por lo que deberá confiar en él al importar el certificado en el almacén de confianza del servidor de sesión.

Para confiar en el servidor remoto

Importe el certificado público en el almacén de confianza del servidor de sesión mediante estas instrucciones, Importar un certificado en el almacén de confianza del servidor de sesión.

Añadir más servidores MSS en la instalación

Durante la instalación, los servidores MSS y HACloud han intercambiado sus certificados y han confiado en ellos. Al añadir servidores MSS adicionales, también es necesario confiar en sus certificados.

MSS Es necesario realizar la configuración en la Consola Administrativa de MSS > Configurar parámetros > Certificados de confianza > Subsistema de confianza.

PARA CONFIGURAR LA CONFIANZA ENTRE LOS SERVIDORES DE SESIÓN Y MSS

- Confíe en el nuevo servidor MSS. Para ello, importe el certificado de MSS en el almacén de confianza del servidor de sesión. Consulte .Importar un certificado en el almacén de confianza del servidor de sesión.
- El nuevo servidor MSS debe confiar en cada uno de los servidores de sesión.
  a. Como administrador, entre en MSS.
  b. En el panel izquierdo, haga clic en Configurar parámetros > Certificados de confianza.
  c. Seleccione Subsistema de confianza. La lista contiene los certificados que son de confianza para MSS.
  d. Haga clic en Importar para añadir el certificado del servidor de sesión a la lista.
  e. Repita este proceso para cada servidor de sesión.

Añadir servidores de sesión adicionales a la instalación con varios servidores MSS

Durante la instalación, el servidor de sesión y MSS ya han intercambiado sus certificados y han confiado en ellos; todos los servidores de MSS ya confían en todos los servidores de sesión existentes. Sin embargo, al añadir más servidores de sesión, se debe establecer una relación de confianza entre los nuevos servidores de sesión y los servidores MSS existentes..

PARA AÑADIR MÁS SERVIDORES DE SESIÓN

1. Importe el certificado del servidor de MSS en el almacén de confianza del servidor de sesión.
2. Importe el certificado del servidor de sesión en el almacén de confianza del servidor de MSS. Consulte "General Security and Certificates" (Seguridad general y certificados) en la documentación de MSS.
3. Recupere el parámetro `service.registry.password` del archivo `container.properties` del servidor de MSS.
4. Defina el parámetro `service.registry.password` del archivo `container.properties` del servidor de sesión.

Más información

- Importar un certificado en el almacén de confianza del servidor de sesión
- General Security and Certificates (Seguridad general y certificados) en la documentación de MSS

Importar un certificado en el almacén de confianza del servidor de sesión

Cuando el servidor de sesión intenta establecer conexiones salientes seguras a servidores remotos, comprueba la identidad del servidor remoto mediante los certificados de su almacén de confianza. Se confiará en todos los certificados importados en este almacén de confianza.

Información que debe conocer:

- Ubicación del almacén de confianza: `/etc/trustcerts.bcfks`
- Formato del almacén de claves: `bcfks` (Bouncy Castle FIPS)
- Contraseña por defecto: *changeit*

UTILIZAR EL KEYSTORE EXPLORER

1. Abra `trustcerts.bcfks` mediante la contraseña *changeit*.

2. En la barra de herramientas, seleccione Importar certificado de confianza.

UTILIZAR JAVA KEYTOOL

En el directorio `sessionserver/etc`:

```
```java
  ../../java/bin/keytool -importcert -alias <import-cert> -trustcacerts -file <import-cert.cer> -keystore trustcerts.bcfks -storetype bcfks -
storepass changeit -providername BCFIPS -providerpath ../lib/bc-fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```
```

3.10 Uso de Docker

La plataforma de código abierto Docker cuenta con una excelente documentación que debe leer y comprender.

3.10.1 ¿Por qué usar Docker?

Docker es una plataforma basada en contenedores que permite desarrollar, distribuir y ejecutar aplicaciones dentro de un contenedor. La aplicación, además de las dependencias que esta necesite, como archivos binarios y bibliotecas, y la información de configuración se guardan en el contenedor. Puede distribuir varios contenedores, que se ejecutan en Docker y sobre el sistema operativo.

Con Docker, puede ampliar las aplicaciones verticalmente, lo que significa que puede haber varias instancias del servidor de sesión en un servidor y cada una de ellas presentará exactamente el mismo rendimiento que cuando se creó y probó.

3.10.2 ¿Cuáles son las ventajas?

La organización en contenedores ofrece muchas ventajas:

- Rendimiento

  Las máquinas virtuales son una alternativa a los contenedores. Sin embargo, los contenedores no contienen un sistema operativo (a diferencia de las máquinas virtuales). Esto significa que los contenedores se pueden crear e iniciar de forma más rápida y presentan un formato más pequeño.

- Agilidad

  Debido a que los contenedores son más portátiles y ofrecen un mayor rendimiento, puede aprovechar los procedimientos de desarrollo más ágiles y con mayor capacidad de respuesta.

- Aislamiento

  Los contenedores de Docker son independientes entre sí. Esto es importante porque un contenedor de Docker que contenga una aplicación, incluidas las versiones necesarias del software compatible, no interferirá con otro contenedor de la misma aplicación que requiera un software compatible diferente. Puede tener total confianza de que, en cada etapa del proceso de desarrollo y distribución, la imagen que cree presentará el rendimiento esperado.

- Capacidad de ampliación

  La creación de nuevos contenedores es un proceso rápido y sencillo. La documentación de Docker proporciona información sobre cómo gestionar varios contenedores.

3.10.3 Terminología

Existen términos básicos con los que debe familiarizarse al trabajar con Docker. Para obtener más información, consulte el sitio de documentación de Docker.

Contenedor

Una instancia en tiempo de ejecución de una imagen. Por lo general, un contenedor está completamente aislado del entorno del host y solo puede acceder a los archivos y puertos del host si se ha configurado para realizar esta acción. Para ejecutar una imagen en un contenedor, utilice el comando "run" de Docker.

Nodo central de Docker

Un recurso de la comunidad basada en la nube para trabajar con Docker. El nodo central de Docker se utiliza normalmente para alojar imágenes, pero se puede usar para autenticar usuarios y automatizar la creación de imágenes. Cualquier usuario puede publicar imágenes en el nodo central de Docker.

Herramienta de composición de Docker

Se trata de una herramienta de composición que utilizan los archivos YAML para configurar los servicios de la aplicación y, a continuación, definir y ejecutar aplicaciones de Docker de varios contenedores. Para obtener más información sobre la herramienta de composición, visite la documentación de Docker sobre esta herramienta.

Archivo de Docker

Un documento de texto que contiene los comandos para crear una imagen de Docker. Puede especificar comandos complejos (como especificar una imagen existente para utilizarla como base) o simples (como copiar archivos de un directorio en otro). Para crear una imagen desde un archivo de Docker, utilice el comando "build" de Docker.

Imagen

Un paquete ejecutable independiente que se ejecuta en un contenedor. Una imagen de Docker es un archivo binario que incluye todo lo necesario para ejecutar un único contenedor de Docker, incluidos sus metadatos. Puede crear sus propias imágenes (mediante un archivo de Docker) o utilizar imágenes que hayan creado otros usuarios y que estén disponibles a continuación en un registro (como, por ejemplo, el nodo central de Docker). Para crear una imagen desde un archivo de Docker, utilice el comando "build" de Docker. Para ejecutar una imagen en un contenedor, utilice el comando "run" de Docker.

3.10.4 Primeros pasos con Docker y Host Access for the Cloud

Si decide utilizar Docker durante la instalación de HACloud, el paquete de instalación incluirá un archivo de Docker inicial y un archivo jar de la aplicación complementario para que pueda empezar

a utilizar el servidor de sesión en los contenedores. Estos archivos están disponibles antes de la instalación.

> **Nota**
>
> Asegúrese de que esté ejecutando la versión más reciente de Docker y la herramienta de composición de Docker.

Puede encontrar ejemplos en la carpeta `docker/samples`. Consulte Ejemplos para obtener instrucciones.

Para crear la imagen base, es necesario realizar cuatro pasos:

1. Instale Docker. Siga las instrucciones del sitio web de Docker.
2. Extraiga el archivo del paquete de descarga y busque `Dockerfile,entrypoint.sh` y `sessionserver.jar` en la carpeta Docker. El archivo `entrypoint.sh` debe tener el conjunto de bits ejecutable.
3. Cree la imagen de Docker.
4. Ejecute la imagen de Docker.

Cree la imagen de Docker.

Si ha seguido los pasos 1 y 2, ha instalado Docker, y ha extraído y localizado el archivo de Docker y el archivo sessionserver.jar, el siguiente paso consiste en crear la imagen base de Docker del servidor de sesión.

1. Ejecute este comando desde la carpeta que contiene el archivo de Docker:

   `docker build -t hacloud/sessionserver:<versión>.`

   Sustituya `<versión>` por la versión del servidor de sesión. Si no hay disponible una versión, la etiqueta por defecto `(-t)` es `la más reciente`.
2. Compruebe que la imagen se haya creado correctamente. Ejecute:

   `docker images`

   La salida debería contener información acerca de la imagen que acaba de crear.

Ejecute la imagen.

Antes de poder ejecutar la imagen del servidor de sesión en un contenedor de Docker, debe llevar a cabo los siguientes pasos:

- **Especifique la dirección del servidor MSS.**

  Para especificar la ubicación del servidor MSS, transfiera una variable de entorno al servidor de sesión mediante Docker. Por ejemplo, `--env MSS_SERVER=mss.server.com`

- **Especifique la contraseña de registro de servicios.**

  Para especificar la contraseña de registro de servicios, transfiera una variable de entorno al servidor de sesión mediante Docker. Por ejemplo, `--env SERVICE_REGISTRY_PASSWORD=<su_contraseña>.`

  Puede recuperar la contraseña desde la propiedad `service.registry.password` ubicada en . `/mss/server/conf/container.properties` en el servidor MSS. Utilice la propiedad `service.registry.password` completa.

- **Indicar a MSS que confíe en el certificado de identidad del servidor de sesión**

  Para llevar a cabo este paso, puede utilizar Consola Administrativa > Configurar parámetros > Certificados de confianza. Consulte la documentación de la Consola Administrativa de MSS, Trusted Certificates (Certificados de confianza). El certificado del servidor de sesión está disponible en el directorio sessionserver/etc.

- **Proporcionar el almacén de claves que contiene el certificado de identidad del servidor de sesión.**

  El servidor de sesión se identifica mediante un certificado. Se espera que el certificado esté presente en el almacén de claves de Java, `/sessionserver/etc/keystore.bcfks`, ubicado en el contenedor. La entrada de par de claves servlet-motor debe contener la cadena de certificados completa.

- **Proporcionar el almacén de confianza que contiene el certificado de MSS**

  Cuando el servidor de sesión establece conexiones TLS salientes, comprueba la confianza de los servidores remotos (como, por ejemplo, MSS) mediante certificados de su almacén de confianza. Se confiará en los certificados presentes en el almacén de claves de Java, `/sessionserver/etc/trustcerts.bcfks`, ubicado en el contenedor.

- **Asignación del almacén de claves y el almacén de confianza a los que se encuentran en el contenedor**

  Tiene dos opciones para proporcionar estos almacenes de claves en el contenedor:

  - Uso de un montaje de volumen

    o bien

  - Ampliación de una imagen de Docker existente

Uso de un montaje de volumen

Un montaje de volumen monta un archivo o un directorio del equipo host en un contenedor. Se hace referencia al archivo o el directorio mediante su vía completa o relativa en el equipo host.

Este volumen monta los archivos de los almacenes de claves y de confianza del host en el contenedor de Docker.

```
docker run -d \
--env MSS_SERVER=<nombre_servidor_mss> \
--env SERVICE_REGISTRY_PASSWORD=<introduzca la contraseña aquí> \
--env MANAGEMENT_SERVER_URL=https://<nombre_servidor_mss>:<puerto>/mss \
--env HOST_NAME=<nombre de DNS del servidor Docker> \
--volume ~/demo_keystore.bcfks:/sessionserver/etc/keystore.bcfks \
--volume ~/demo_truststore.bcfks:/sessionserver/etc/trustcerts.bcfks \
--publish 7443:7443 \
sessionserver
```

Ampliación de una imagen de Docker existente

Con este método, puede crear un nuevo archivo de Docker para copiar los archivos que necesita en la imagen de Docker. Esto permite que la imagen de Docker sea más portátil.

- Cree primero un archivo de Docker que se extenderá desde la imagen de Docker `hacloud/sessionserver` .
- FROM hacloud/sessionserver: `<por ejemplo, hacloud/sessionserver:latest o hacloud/sessionserver:version>`
- COPY `<su-ruta>/keystore.bcfks /sessionserver/etc/keystore.bcfks`
- COPY `<su-ruta>/truststore.bcfks /sessionserver/etc/trustcerts.bcfks`
- A continuación, cree la imagen de Docker ampliada y asígnele el nombre demo.

  `docker build -t demo .`
- Por último, ejecute la imagen demo.

```
docker run -d \
--env MSS_SERVER=<nombre_servidor_mss> \
--env SERVICE_REGISTRY_PASSWORD=<introduzca la contraseña aquí> \
--env MANAGEMENT_SERVER_URL=https://<nombre_servidor_mss>:<puerto>/mss \
--env HOST_NAME=<nombre de DNS del servidor Docker> \
--publish 7443:7443 \
demo
```

- **Especificar el nombre de host y el puerto de Docker**

  El servidor de sesión debe difundir su nombre de host para que MSS pueda encontrarlo. Como Docker genera un nombre exclusivo aleatorio al que no se puede acceder fuera del contenedor, debe especificar el nombre del host de Docker para MSS. También es necesario indicar al servidor de sesión el puerto que se va a publicar en el host de Docker. Los clientes que accedan al servidor de sesión acabarán encontrando `<nombre_de_host_de_Docker>:<puerto_publicado_de_Docker>` .

```
--env HOST_NAME=docker_host_name
--env SERVER_PORT=docker_published_port
```

3.10.5 Ejemplos

Los ejemplos, ubicados en la carpeta docker/samples, le guiarán por las cuatro situaciones mediante la herramienta de composición de Docker. La herramienta de composición utiliza un archivo YAML para configurar y ejecutar las aplicaciones con un único comando.

Requisitos previos

Para ejecutar los ejemplos:

- Instale la herramienta de composición de Docker. Revise la información sobre la herramienta de composición de Docker en la documentación de Docker antes de continuar.
- Un servidor MSS en ejecución.
- Un archivo de almacén de claves para proteger las conexiones TLS al servidor de sesión en el que confía MSS.
- Un archivo de almacén de confianza que disponga de un certificado de servidor MSS.
- Para crear la imagen de Docker del servidor de sesión

Entre los ejemplos, se incluyen:

- Básico: un ejemplo básico que proporciona archivos de almacén de claves y de confianza de demostración en los que puede importar un certificado de servidor MSS.
- Híbrido: un ejemplo híbrido que presupone una instalación local de Host Access for the Cloud y monta los archivos de almacén de claves y de confianza existentes del disco en el contenedor de Docker.
- Extensiones: un ejemplo de extensión que muestra cómo actualizar, modificar y personalizar el cliente web.
- Equilibrio de carga: un ejemplo de equilibrador de carga que muestra cómo establecer el equilibro entre contenedores enlazados.

Básico

En este ejemplo básico, se muestra cómo ejecutar la imagen de Docker del servidor de sesión en la herramienta de composición de Docker. En este ejemplo, deberá importar el certificado del servidor MSS en la muestra proporcionada `./certs/demo_truststore.bcfks` mediante una herramienta similar a KeyStore Explorer. Por defecto, el certificado de MSS se encuentra en `/mss/server/etc/<nombre-equipo>.cer`. Consulte Importar un certificado en el almacén de confianza del servidor de sesión.

Antes de ejecutar el ejemplo, actualice los valores de MSS_SERVER, HOST_NAME y SERVICE_REGISTRY_PASSWORD en `docker-compose.yml`.

- Para iniciar el servicio del servidor de sesión:

  `docker-compose up`

- Para ejecutar el servicio en un daemon (modo desconectado):

  `docker-compose up -d`

- Para examinar los contenedores en ejecución:

  `docker ps`

Híbrido

En este ejemplo, hay presente una instalación local de Host Access for the Cloud con archivos de los almacenes de claves y de confianza en el disco. Estos archivos se montarán (copiarán) en el contenedor de Docker.

Antes de ejecutar el ejemplo, actualice los valores de MSS_SERVER, HOST_NAME, SERVER_PORT y SERVICE_REGISTRY_PASSWORD en el archivo .env.

Para iniciar el servicio del servidor de sesión:

- Copie `.env` y `docker-compose.yml` en `sessionserver/microservices/sessionserver/`.
- En este directorio, ejecute: `docker-compose up -d`

Extensiones

Mediante el uso de extensiones y su propio código HTML, CSS o JavaScript, puede actualizar, modificar y personalizar la presentación del cliente Web desde el navegador. Consulte "Ampliación del cliente web" para obtener más información.

En este ejemplo, se establece SPRING_PROFILES_ACTIVE en extensions_enabled y se asigna la ubicación de las extensiones en `docker-compose.yml`.

Antes de ejecutar el ejemplo, actualice los valores de MSS_SERVER, HOST_NAME y SERVICE_REGISTRY_PASSWORD en el archivo .env.

Para iniciar el servicio del servidor de sesión:

`docker-compose up -d`

También puede optar por extender la imagen base de Docker, "hacloud/sessionserver", y copiar los archivos de extensión en el contenedor de Docker:

1. Cree el archivo de Docker que se extenderá desde la imagen de Docker, "hacloud/sessionserver".

```
FROM hacloud/sessionserver

COPY ./certs/keystore.bcfks /sessionserver/etc/keystore.bcfks
COPY ./certs/trustcerts.bcfks /sessionserver/etc/trustcerts.bcfks
COPY ./extensions /sessionserver/extensions/
```

2. Cree la imagen de Docker ampliada y asígnele el nombre *extensions*.

```
docker build -t extensions .
```

3. Actualice `docker compose.yml` para utilizar la nueva imagen de extensiones.

```
version: '3'
services:
  sessionserver:
    image: extensions
    environment:
        - LOGGING_FILE_NAME=./logs/sessionserver.log
        - LOGGING_FILE_MAXSIZE=10MB
        - LOGGING_FILE_MAXHISTORY=10
        - MSS_SERVER=${MSS_SERVER}
        - SERVICE_REGISTRY_PASSWORD=${SERVICE_REGISTRY_PASSWORD}
        - SPRING_PROFILES_ACTIVE=extensions_enabled
    ports:
        - ${SERVER_PORT}:7443
```

Equilibrio de carga

HAProxy es un equilibrador de carga. Obtenga más información sobre HAProxy en su sitio web.

En este ejemplo, se incluye un servicio haproxy en el archivo `docker-compose.yml`. Este ejemplo utiliza una imagen de haproxy para el equilibro entre contenedores enlazados. En este ejemplo, se utilizan puentes SSL para enlazar los contenedores.

Para proporcionar una comunicación segura entre los clientes y el equilibrador de carga, debe actualizar la propiedad `LOAD_BALANCER_CERT` del archivo `.env` con la ubicación del certificado del equilibrador de carga.

Para ayudarle con la prueba, puede generar un certificado autofirmado:

1. Genere una clave privada exclusiva (KEY):

```
sudo openssl genrsa -out mydomain.key 2048
```

2. Genere una petición de firma de certificado (CSR):

```
sudo openssl req -new -key mydomain.key -out mydomain.csr
```

3. Cree un certificado autofirmado (CRT):

```
sudo openssl x509 -req -days 365 -in mydomain.csr -signkey mydomain.key -out
mydomain.crt
```

4. Añada KEY y CERT a loadbalancer.pem:

```
sudo cat mydomain.key mydomain.crt >./certs/loadbalancer.pem
```

Para iniciar los servicios del servidor de sesión y HAProxy:

```
docker-compose up -d
```

-o bien-

```
docker-compose up --scale sessionserver=n -d
```

Donde n es el número de instancias del servidor de sesión.

Puede cambiar el número de instancias del servidor de sesión después de que se inicien los servicios:

```
docker-compose scale sessionserver=n
```

Para acceder a la página de estadísticas del servidor de sesión y HAProxy:

- https://server:7443
- http://server:1936/haproxy?stats

En uso:

- usuario: *admin*
- contraseña: *password*

4. Administración

4.1 Administración

La creación y la configuración de sesiones, y la garantía de que todo funciona bien y de forma segura permitirán a los usuarios alcanzar el éxito. La información siguiente le ayudará a administrar y gestionar las sesiones y las conexiones de host.

- Creación de sesiones de host
- Proporcionar acceso a las sesiones de host
- Gestión de las Preferencias de usuario
- Personalización de las sesiones de host
- Registro

4.2 Creación de sesiones de host

Host Access for the Cloud admite los hosts IBM 3270, 5250 y VT, así como los tipos de host UTS, T27 y ALC.

Los usuarios consiguen acceso al host mediante las sesiones que crea y configura. Las sesiones las crea un administrador en la Consola Administrativa del MSS. Cuando usted inicia una sesión desde la Consola Administrativa, el panel Conexión del cliente web se abre en una ventana del navegador aparte. Usted configura opciones de conexión desde este panel. Las opciones varían en función del tipo de host.

Para crear una sesión:

1. Cree sesiones en la Consola Administrativa de MSS. Consulte Add a Session (Añadir una sesión) en la documentación de MSS.
2. En el cuadro de diálogo **Crear sesión nueva** del cliente web HACloud, seleccione el tipo de host al que desea conectarse en la lista desplegable.
3. En el panel Conexión, identifique el nombre del host al que desea conectarse. Puede utilizar el nombre de host completo o su dirección IP.
4. Escriba el número del puerto que desea utilizar.
5. Complete la información necesaria para la conexión host.
6. Guarde sus parámetros de conexión.
7. Una vez que haya finalizado la configuración y la prueba de la sesión, haga clic en Salir para volver a la Consola Administrativa de MSS.
8. Mediante la vista Asignar acceso de la Consola Administrativa de MSS, asigne la sesión que ha creado para los usuarios.
9. Una vez asignadas las sesiones a los usuarios, puede indicarles cómo acceder a las sesiones.

Compruebe la configuración del tipo de sesión.

- Parámetros de conexión comunes
- Parámetros de conexión 3270 y 5250
- Configuración de conexión VT
- Parámetros de conexión UTS
- Parámetros de conexión T27
- Parámetros de conexión ALC

4.3 Ajustes de conexión

4.3.1 Ajustes de conexión

Host Access for the Cloud admite los hosts IBM 3270, 5250 y VT, así como los tipos de host UTS, T27 y ALC.

Los usuarios consiguen acceso al host mediante las sesiones que crea y configura. Puede configurar las opciones de conexión desde el panel de configuración. Hay una serie de configuraciones que son comunes a todos los tipos de host; de lo contrario, las opciones varían en función del tipo de host.

Más información

- Parámetros de conexión comunes
- 3270 y 5250
- VT
- UTS
- T27
- ALC

4.3.2 Parámetros de conexión comunes

Estas opciones son comunes para todos los tipos de host soportados.

- **Conectar al iniciar**

  De forma predeterminada, las sesiones se configuran para conectarse automáticamente al host cuando usted crea o abre una sesión. También puede configurar una sesión para que no se conecte automáticamente al host. Elija No para conectarse al host manualmente.

- **Reconectar cuando el host finaliza la conexión**

  Si se establece en Sí, Host Access for the Cloud intentará volver a conectarse tan pronto como finalice la conexión del host.

- **Protocolo**

  Seleccione el protocolo que desee utilizar para comunicar con el host de la lista desplegable. Para establecer una conexión de host, el cliente Web y el equipo host deben utilizar el mismo protocolo de red. Los valores disponibles dependen del host al que se esté conectando. Son los siguientes:

Protocolo	Descripción
TN3270	TN3270 es una forma del protocolo Telnet que es un conjunto de especificaciones para la comunicación general entre el escritorio y los sistemas de host. Utiliza TCP/IP como transporte entre las computadoras de escritorio y los mainframes IBM.
TN3270E	TN3270E o Telnet Extendido es para usuarios de TCP/IP que se conectan a su mainframe IBM mediante un gateway Telnet que implementa RFC 1647. El protocolo TN3270E le permite especificar el nombre del dispositivo de conexión (conocido también como nombre LU) y ofrece soporte para la clave ATTN, la clave SYSREQ y la gestión de la respuesta SNA. Si intenta utilizar Telnet Extendido para conectarse a un gateway que no soporta este protocolo, se utilizará el estándar TN3270 en su lugar.
TN5250	TN5250 es una forma del protocolo Telnet que es un conjunto de especificaciones para la comunicación general entre el escritorio y los sistemas de host. Utiliza TCP/IP como transporte entre las computadoras de escritorio y las computadoras AS/400.
Secure Shell (VT)	Puede configurar las conexiones SSH cuando se necesite una comunicación segura y cifrada entre un host VT de confianza y la computadora a través de una red no segura. Las conexiones SSH garantizan que tanto el usuario cliente como la computadora del host se autentiquen, así como el cifrado de todos los datos. Hay dos opciones de autenticación disponibles: • **Teclado interactivo** - Puede utilizar este método de autenticación para implementar distintos tipos de mecanismos de autenticación. Cualquier método de autenticación soportado que requiera sólo la entrada del usuario se puede realizar con el Teclado interactivo. • **Contraseña** - Esta opción le pide al cliente una contraseña al host después de haber establecido la conexión host. La contraseña se envía al host a través del canal cifrado.
Telnet (VT)	Telnet es un protocolo de la suite TCP/IP de protocolos abiertos. Como protocolo de secuencia de caracteres, Telnet transmite de carácter en carácter las entradas del usuario desde aplicaciones de modo de caracteres a través de la red hasta el host, donde se procesan y se devuelven a través de la red.
INT1 (UTS)	Ofrece acceso a hosts Unisys 1100/1200 que utilizan el protocolo de red TCP/IP.
TCPA (T27)	Utilice este protocolo para conectarse a hosts de la serie Unisys ClearPath NX/LX o de la serie A. La autenticación TCPA es el proceso de verificar la

	información del inicio de sesión del usuario. Cuando está configurada correctamente, puede solicitar una credencial de seguridad de su servidor de credenciales de aplicación y transmitir la credencial de vuelta al servidor. Si la credencial es válida, su aplicación iniciará sesión; no tendrá que introducir un ID de usuario o una contraseña. Si la credencial no es válida, se le pedirá utilizar un ID de usuario y una contraseña.
MATIP (ALC)	Mapping of Airline Traffic Over Internet Protocol (MATIP) utiliza TCP/IP para reservas en líneas aéreas, billetaje y tráfico de mensajes.

- **Seguridad TLS**

  Los protocolos TLS permiten al cliente y al servidor establecer una conexión segura y cifrada a través de una red pública. Cuando se conecta mediante TLS, Host Access for the Cloud autentica el servidor antes de abrir una sesión y todos los datos transmitidos entre él y el host se cifran mediante el nivel de cifrado seleccionado.

  > **Consejo**
  >
  > Cuando la seguridad TLS se ha establecido en TLS 1.3 o TLS 1.2, tiene la opción de verificar el nombre de host en relación con el nombre del certificado del servidor. Le recomendamos expresamente que habilite la verificación del nombre del host para todas las sesiones.

  Están disponibles las siguientes opciones:

Opciones de seguridad	Descripción
Nada	No se requiere conexión segura.
TLS 1.3	Conectar mediante TLS 1.3. Cuando **Verificar identidad del servidor** se ha definido en **Sí**, el cliente comprueba el nombre del servidor o del host en relación con el nombre del certificado del servidor. Le recomendamos expresamente que habilite la verificación del nombre del host para todas las sesiones.
TLS 1.2	Conectar mediante TLS 1.2. Cuando **Verificar identidad del servidor** se ha definido en **Sí**, el cliente comprueba el nombre del servidor o del host en relación con el nombre del certificado del servidor. Le recomendamos expresamente que habilite la verificación del nombre del host para todas las sesiones.

  > **Nota**
  >
  > Consulte la sección sobre conexiones seguraspara obtener información sobre la adición de certificados de confianza, almacenes de claves, el uso de SSH y otra información de seguridad avanzada.

- **Habilitar Rastreo de Emulación**

  Puede seleccionar generar rastreos de host para una sesión. El valor por defecto es No. Seleccione Sí para crear un nuevo rastreo del host de emulación cada vez que se inicie la sesión. El archivo de rastreo se guarda en `<install directory>/sessionserver/logs/hosttraces/<date (yyyymmdd>/<trace-file>`.

Uso del Administrador de ID de Terminal

MSS Para utilizar el Administrador de ID de Terminal, debe tener configurado un servidor de Administrador de ID de Terminal. Consulte Configuración del Administrador de ID de Terminal.

Si ha seleccionado **Administrador de ID de Terminal**, puede utilizarlo para proporcionar ID a las aplicaciones cliente en tiempo de ejecución y gestionar ID agrupados para diferentes tipos de host. Un ID son datos de conexión únicos para una sesión de host individual.

Si decide utilizar el Administrador de ID de Terminal y ha configurado el servidor del mismo, puede seleccionar entre las opciones siguientes para configurar los criterios para obtener un ID. Se deben cumplir todos los criterios para obtener un ID.

> **Nota**
>
> Recuerde que cuando especifica un criterio, indica que el ID se debe asignar solo si se encuentra un ID con ese valor específico.

El conjunto de criterios seleccionados debe coincidir exactamente con el conjunto de criterios especificados en una Agrupación de IDs en el Administrador de ID de Terminal para que la solicitud de ID se pueda realizar.

Criterios del Administrador de ID de Terminal

Criterio	Descripción
Nombre de agrupación	Incluya este atributo e ingrese el nombre de la agrupación para limitar la búsqueda de ID a una agrupación específica.
Dirección IP de cliente	La dirección IP del equipo del cliente se incluirá como parte de la solicitud de un ID.
Dirección de host	La dirección del host configurado para esta sesión se incluirá como parte de la solicitud de un ID.
Puerto de host	El puerto para el host configurado para esta sesión se incluirá como parte de la solicitud de un ID.
Nombre de sesión	Cuando esta opción está seleccionada, requiere que el ID se configure para ser utilizado por esta sesión exclusivamente.
Tipo de sesión	El tipo de sesión (por ejemplo, IBM 3270, IBM 5250, UTS, ALC o T27) se incluye siempre como parte de cualquier solicitud de un ID.
Nombre de usuario	Utilice este criterio para asegurarse de que sólo se asignarán IDs creados para el uso exclusivo de usuarios específicos. El nombre de usuario actual, que se debe encontrar en un ID antes de que pueda ser asignado, es el nombre del usuario al que está asignada la sesión en ejecución. Para configurar una sesión basada en nombres de usuario, se dispone de un nombre de usuario por defecto como marcador de posición: tidm-setup. Para que el administrador pueda configurar sesiones mediante tidm-setup, el Administrador de ID de Terminal debe disponer de ID para tidm-setup. Puede sobrescribir el nombre por defecto por uno propio. Para ello, modifique el archivo `&ltinstall-dir>/sessionserver/conf/container.properties` del siguiente modo: `id.manager.user.name=custom-username`, donde `custom-username` se sustituye por el nombre que desea utilizar.
Nombre de aplicación (UTS)	El nombre de la aplicación de host se incluirá como parte de la solicitud de un ID.

Para determinar el comportamiento de intento de conexión si el Administrador de ID de Terminal no asigna con éxito un ID para esta sesión, utilice **Si ID no está asignado**:

- **Fallar intento de conexión**: si la opción está seleccionada, la sesión no intenta establecer conexión si un ID no está asignado.
- **Permitir intento de conexión**: si la opción está seleccionada, la sesión intenta establecer conexión si un ID no está asignado. El intento debe ser rechazado por el host. Hay algunos tipos de host que permiten al usuario conectarse sin ID.

  Para confirmar que el Administrador de ID de Terminal puede proveer un ID utilizando las selecciones de criterios y valores que ha hecho, haga clic en Probar los criterios del Administrador de ID de Terminal.
- **Enviar paquetes Keep Alive** - Seleccione esta configuración para realizar una comprobación constante entre la sesión y el host, para así detectar inmediatamente los problemas de conexión. Seleccione entre los siguientes tipos de paquetes Keep Alive:

Esta opción	Tiene esta función...
Nada	El valor por defecto. No se envían paquetes.
Sistema	La pila TCP/IP mantiene el seguimiento de la conexión host y envía paquetes Keep Alive con poca frecuencia. Esta opción utiliza menos recursos del sistema que Enviar paquetes NOP o Enviar paquetes de marca de sincronización.
Enviar paquetes NOP	Se envía periódicamente un comando No Operation (NOP) al host. No es obligatorio que el host responda a estos comandos, pero la pila TCP/IP puede detectar si hay algún tipo de problema con la entrega del paquete.
Enviar paquetes de marca de sincronización	Se envía periódicamente un comando de Marca de sincronización para determinar si la conexión continúa activa. El host debe responder a estos comandos. Si no se recibe respuesta o si se produce un error durante el envío del paquete, la conexión se cierra.

- **Tiempo de espera de Keep Alive (segundos)** - Si elige utilizar una de las opciones Enviar paquetes NOP o Enviar paquetes de marca de sincronización, seleccione el intervalo entre peticiones Keep Alive. Los valores están en el rango de 1 a 36000 segundos (1 hora); el valor predeterminado es 600 segundos.

Probar los criterios del Administrador de ID de Terminal

El Administrador de ID de Terminal provee IDs a las aplicaciones del cliente en ejecución. Para confirmar que el Administrador de ID de Terminal puede proveer un ID utilizando las selecciones de criterios y valores que ha hecho, utilice esta opción.

Los criterios para la sesión actual se especifican en el panel Conexión después de haber seleccionado **Utilizar Administrador de ID de Terminal** en el campo Nombre de Dispositivo (tipos de host 3270, 5250), en el campo ID de terminal (UTS) o en el campo ID de estación (T27). Los criterios seleccionados para la sesión actual se visualizan de forma predeterminada.

Haga clic en **Test** para confirmar que el Administrador de ID de Terminal puede proveer un ID que coincida con las selecciones de criterios y valores configuradas. La prueba devuelve el nombre de un ID disponible que satisface los valores de atributo seleccionados.

Comprobar para otros criterios y valores

También puede utilizar este panel para comprobar criterios diferentes de los asociados a la sesión actual.

1. Seleccione cualquiera de los tipos de sesión de la lista Tipo de sesión y seleccione los criterios que desea comprobar. Puede probar valores alternativos que desee utilizar en un ejemplo de solicitud al Administrador de ID de Terminal.
2. Haga clic en **Test** para confirmar que el Administrador de ID de Terminal puede proveer un ID que coincida con las selecciones de criterios y valores. La prueba devuelve el nombre de un ID disponible que satisface los valores seleccionados.

4.3.3 Parámetros de conexión 3270 y 5250

Además de los parámetros de configuración comunes, los tipos de host 3270 y 5250 requieren estos parámetros específicos.

- **Modelo de terminal**

  Especifique el modelo de terminal (conocido también como estación de visualización) que desee que emule Host Access for the Cloud. Dependiendo del tipo de host, hay distintos modelos de terminal.

  Si elige **Modelo personalizado**, puede especificar el número de columnas y filas para personalizar el modelo de terminal.

- **Usar inicio de sesión automático de Kerberos (solo para 5250)** MSS

  Si se establece en **Sí** el usuario no tiene que introducir las credenciales de entrada la sesión. El inicio de sesión automático de Kerberos se configura en Consola Administrativa de MSS > Host Access for the Cloud. Al configurar HACloud para utilizar el protocolo de autenticación Kerberos, hay términos que debe conocer y requisitos previos que debe cumplir antes de configurar esta opción. Estas opciones se explican detalladamente en la documentación del panel Consola Administrativa de MSS > Host Access for the Cloud, disponible desde el botón Ayuda. Consulte Configuración de Kerberos para el inicio de sesión único de AS/400 para obtener más información.

- **ID de terminal** (sólo 3270)

  Cuando Host Access for the Cloud se conecta a un host Telnet, el protocolo Telnet y el host negocian un ID de terminal que se utilizará durante la conexión Telnet inicial. En general, de esta negociación resulta el uso del ID de terminal correcto, por lo que este cuadro se debe dejar vacío.

- **Seguridad TLS**

  Los protocolos TLS permiten al cliente y al servidor establecer una conexión segura y cifrada a través de una red pública. Cuando se conecta mediante TLS, Host Access for the Cloud autentica el servidor antes de abrir una sesión y todos los datos transmitidos entre él y el host se cifran mediante el nivel de cifrado seleccionado. Consulte Parámetros de conexión comunes para obtener información sobre este parámetro común.

- **Nombre de dispositivo**

Si ha seleccionado TN3270, TN3270E o TN5250 como protocolo, especifique el nombre de dispositivo a utilizar cuando la sesión se conecte al host. El nombre de dispositivo es conocido también como host LU o pool. También puede elegir:

- **Generar nombre de dispositivo único**: genera automáticamente un nombre de dispositivo único.
- **Utilizar el Administrador de ID de Terminal**: muestra parámetros adicionales para completar. Consulte Uso del Administrador de ID de Terminal.
- **Solicitar siempre el ID al usuario**: se solicita al usuario final el ID del dispositivo cada vez que se intenta establecer una conexión.
- **Solicitar al usuario si no se ha especificado el ID**: se le solicita al usuario final la primera vez que se intenta establecer una conexión; después de este intento, se guardará el valor. El valor guardado se seguirá utilizando sin que se solicite de nuevo.

Si usted no especifica un nombre de dispositivo para la sesión, el host asigna dinámicamente uno a la sesión. Un nombre de dispositivo ajustado dentro de una macro sobrescribe este parámetro.

4.3.4 Parámetros de conexión VT

Además de los parámetros de conexión comunes, los hosts VT requieren estos parámetros adicionales. Estos parámetros varían en función del protocolo que esté utilizando: Telnet o SSH. Los parámetros son aplicables a ambos protocolos, a menos que se indique lo contrario.

Opciones de configuración de sesión VT

Parámetros de VT	Descripción
ID de terminal	Este parámetro determina la respuesta que Host Access for the Cloud envía al host tras una petición de atributos de dispositivo (DA) primaria. Esta respuesta informa al host sobre las funciones de terminal que puede llevar a cabo. La respuesta de Host Access for the Cloud para cada ID de terminal es exactamente la misma que la respuesta del terminal VT; algunas aplicaciones pueden requerir una respuesta de DA específica. Este parámetro de ID de terminal no depende del valor de Tipo de terminal. Las opciones son: VT220, VT420, VT100, DEC-VT100 y VT52.
Todos los hosts desconocidos (SSH)	Esta opción permite al administrador con capacidad de decisión determinar si el cliente Web permitirá los hosts desconocidos. Las opciones son: • **Sí**: se permiten los hosts desconocidos y todas las conexiones SSH. No se pregunta a los usuarios del cliente Web si debe confiarse en los hosts. • **Preguntar**: se le pregunta al usuario del cliente web si debe confiarse en el host cuando se conecte a un host desconocido con el que no se haya encontrado antes. Si decide confiar en el host, su clave pública se almacenará en las preferencias de usuario y las conexiones posteriores no generarán un aviso a menos que la clave del host cambie. • **No**: no se admiten los hosts desconocidos. Solo se permiten los hosts en los que el administrador haya decidido confiar al configurar la sesión. No se le pregunta nunca a los usuarios y la sesión se conecta o no en función de las opciones seleccionadas por el administrador.
Suprimir mensajes de banner (SSH)	Cuando la opción está activada, el banner SSH no se visualiza. Esta opción es útil cuando se graban macros de inicio de sesión SSH.
Eco local (Telnet)	Automático (valor por defecto). Cómo responde Host Access for the Cloud al eco remoto enviado por un host Telnet: la opción Automático intenta negociar el eco remoto, pero realiza lo que ordena el comando. La opción Sí implica que Host Access for the Cloud negocia el eco local con el host, pero siempre establece el eco, mientras que la opción No implica que Host Access for the Cloud negocia el eco remoto con el host, pero no establece el eco.

Volver a negociar eco (Telnet)	No (predeterminado). Si el valor es Sí, las contraseñas no se visualizan en la pantalla local, pero todo el texto que se escriba está visible. Host Access for the Cloud admite la opción de Telnet Suppress Local Echo (SLE) (Suprimir eco local) cuando está conectado al host en el modo half-dúplex. Esto significa que Host Access for the Cloud suprimirá el eco de caracteres en el equipo host y, con compatibilidad con SLE, Host Access for the Cloud puede recibir instrucciones para suprimir el eco localmente.
Definir Tamaño de Ventana de Host	Sí (predeterminado). Este parámetro envía el número de filas y columnas al host Telnet siempre que cambian. Esto permite al host Telnet controlar correctamente el cursor si el tamaño de la ventana cambia.
Utilizar Modo Binario (Telnet)	No (predeterminado). Telnet define una ruta de datos de 7 bits entre el host y el terminal. Este tipo de ruta de datos no es compatible con algunos juegos de caracteres nacionales. Afortunadamente, muchos hosts utilizan los datos de 8 bits sin poner a cero el bit 8, lo que permite resolver este problema. Sin embargo, en algunos casos puede que sea necesario seleccionar esta casilla de verificación para forzar al host a utilizar una ruta de datos de 8 bits.
Enviar Salto de línea después de Retorno de carro (Telnet)	No (predeterminado). Un "auténtico" host Telnet espera ver una secuencia de caracteres CrNu (retorno de carro/nulo) para indicar el final de línea enviado desde el terminal. Algunos hosts en Internet no son auténticos hosts Telnet, por lo que esperan ver un carácter Lf (salto de línea) después de un carácter Cr (retorno de carro) al final de una línea. Si se está conectando a este tipo de host Telnet, seleccione Sí.
Ctrl-Interrumpir envía (Telnet)	Seleccione qué envía la secuencia Ctrl-Interrumpir al host cuando se pulsa. Las opciones son: secuencia Interrupción Telnet (predeterminada), Interrupción del proceso o Nada.
Juego de Caracteres de Host	El valor predeterminado para el Juego de caracteres de host depende del tipo de terminal que esté emulando. Este parámetro refleja el estado actual del terminal de Juego de Caracteres de Host VT, que puede ser cambiado por el host. El parámetro predeterminado asociado guardado con el modelo es DEC Suplementario.
Respuesta Automática	No (predeterminado). Este parámetro especifica si el mensaje de respuesta (configurado con la propiedad Respuesta) se envía automáticamente al host tras una conexión de línea de comunicaciones.

Cadena de Respuesta	Este ajuste le permite ingresar un mensaje de respuesta si el host espera contestación como respuesta a un carácter ENQ. La cadena de respuesta soporta caracteres con códigos inferiores o iguales a 0xFFFF mediante secuencias de escape Unicode. La secuencia de escape empieza con \u seguida de exactamente cuatro dígitos hexadecimales. Usted puede integrar secuencias de escape Unicode en cualquier cadena. Por ejemplo, this embedded \u0045 se interpretará como this embedded E ya que 45 es el código hexadecimal para el carácter E. Para enviar secuencias de escape Unicode al host, escape la secuencia anteponiendo una barra invertida. Por ejemplo, para enviar la cadena literal \u001C al host, asigne una tecla a \\u001C. Host Access for the Cloud convertirá esto a la cadena \u001C cuando se pulse esa tecla y enviará los seis caracteres de la cadena resultante al host.

Más información

- Descripciones de TLS

4.3.5 Parámetros de conexión UTS

Además de los parámetros de conexión comunes, los hosts UTS requieren estos parámetros adicionales:

Opciones de configuración de sesión UTS INT1

Opciones de UTS INT1	Descripción
Aplicación	Nombre de la aplicación de host o del modo operativo del host al que se debe acceder. Esta es la palabra o la frase que la máquina local envía al host cuando establece comunicación con el host por primera vez. Si ha estado utilizando un terminal de host, éste debe ser el nombre $$OPEN de la aplicación. El nombre de la aplicación suele ser el mismo que el nombre del entorno, pero también pueden ser diferentes. Por ejemplo, el nombre del entorno puede ser MAPPER y el de la aplicación puede ser UDSSRC. Durante una sesión de emulación de terminal usted podría escribir $ $OPEN MAPPER en el indicador e INT1 enviaría UDSSRC al host una vez que la conexión se estableciera.
TSAP	Transport Service Access Point (TSAP) que se desea, hasta 32 caracteres (como TIPCSU para conexiones TIP, RSDCSU para conexiones Demand). Se requiere un TSAP sólo si se está conectando a un Host LAN Controller (HLC) o a un Distributed Communications Processor (DCP) en modo router IP. Si no está seguro de qué valor utilizar, póngase en contacto con su administrador de host.
Transacción inicial	Carácter, palabra o frase que la máquina local enviará al host cuando se establezca por primera vez la comunicación con el host (hasta 15 caracteres). Este parámetro es opcional y se utiliza principalmente con TIP. Por ejemplo, puede escribir ^ para ejecutar MAPPER. Este parámetro se puede utilizar también para transmitir contraseñas.
Iniciar transacción	Cuando usted configura una transacción inicial, de forma predeterminada los datos se envían en cuanto se ha establecido la conexión de sesión. Usted puede decidir cuándo se envía una transacción inicial utilizando una cadena particular para activar la transacción inicial. Por ejemplo, para esperar un inicio de sesión correcto antes de enviar los datos de la transacción inicial, escriba una cadena que se utilice para identificar un inicio de sesión correcto. Puede utilizar este parámetro en combinación con **Enviar transacción inicial**.
Enviar transacción inicial	Usted puede determinar cuándo se envía la transacción inicial. • **Inmediatamente** - predeterminado. • **Cuando se recibe el carácter de inicio de entrada (start of entry, SOE)** - esta opción es útil cuando se deben completar transacciones multilínea antes de enviar la cadena. • **Después de los milisegundos especificados**

ID de terminal	Seleccione las opciones para especificar un ID de terminal o utilizar el Administrador de ID de Terminal. Para especificar un ID de terminal, escríbalo en el campo **Especificar ID de Terminal**. • Especificar el ID de Terminal El ID de Terminal, un identificador de terminal (normalmente de hasta 8 caracteres alfanuméricos) que se utilizará para la sesión de comunicación asociada a esta ruta. Conocido también como TID o PID, cada ID de terminal debe ser único para el host. • Solicitar al usuario si no se ha especificado el ID Se le solicitará al usuario final la primera vez que se intente establecer una conexión; después de este intento, se guardará el valor. El valor guardado se seguirá utilizando sin que se solicite de nuevo. • Solicitar siempre el ID al usuario Si se selecciona esta opción, se le solicita al usuario final el ID de terminal cada vez que se intenta establecer una conexión. • Utilizar el Administrador de ID de Terminal Si elige **Utilizar Administrador de ID de Terminal**, se le pedirá que seleccione los atributos del ID de Terminal que desea utilizar para obtener un ID. Consulte Atributos del Administrador de ID de Terminal. Para probar los atributos, haga clic en **Test**.

Más información

- Atributos del Administrador de ID de Terminal
- Descripciones de TLS

4.3.6 Parámetros de conexión T27

Junto a los parámetros de conexión comunes, puede configurar estas opciones de conexión de T27 adicionales:

Parámetros de conexión T27

Opciones T27	Descripción
Tipo de terminal	Seleccione el tipo de terminal a emular durante la sesión. La emulación T27 soporta los tipos de terminal Unisys TD830, TD830 ASCII, TD830 INTL y TD830 NDL.
Utilizar Modo Binario	Debe habilitar la opción Utilizar Modo binario si usted requiere la impresión pass through. El valor por defecto es No. TCPA define una ruta de datos de 7 bits entre el host y el emulador de terminal. Este tipo de ruta de datos no es compatible con algunos juegos de caracteres nacionales. De todos modos, muchos hosts utilizan los datos de 8 bits sin poner a cero el bit 8, lo que permite resolver este problema. Sin embargo, puede que sea necesario seleccionar esta opción para forzar al host a utilizar una ruta de datos de 8 bits.
Ancho de línea	Seleccione el número de caracteres que el host enviará al cliente. El valor por defecto es 80 caracteres.
Seguridad TLS	Consulte **Descripciones de TLS** para obtener una descripción de las diversas opciones.
ID de estación	Seleccione una opción para especificar un ID de estación o utilizar el Administrador de ID de Terminal. Para especificar un ID de estación, seleccione **Especificar ID de estación** y teclee el nombre en el campo ID de estación. Cada ID de estación debe ser único para el host y suele constar de un máximo de ocho caracteres alfanuméricos. • Solicitar al usuario si no se ha especificado el ID Se le solicitará al usuario final la primera vez que se intente establecer una conexión; después de este intento, se guardará el valor. El valor guardado se seguirá utilizando sin que se solicite de nuevo. • Solicitar siempre el ID al usuario Si se selecciona esta opción, se le solicita al usuario final el ID de estación cada vez que se intenta establecer una conexión. • Utilizar el Administrador de ID de Terminal Si selecciona Utilizar el Administrador de ID de Terminal, verá un número de criterios de ID de terminal para configurar. Consulte **Criterios del Administrador de ID de Terminal** para obtener descripciones de las distintas opciones. Si no especifica un ID de estación para la sesión, el host asigna dinámicamente uno a la sesión.

Más información

- Descripciones de TLS
- Criterios del Administrador de ID de Terminal

4.3.7 Parámetros de conexión ALC

Además de los parámetros de conexión comunes, los hosts ALC requieren estos parámetros adicionales:

Parámetros de conexión ALC

Opciones ALC	Descripciones
Seguridad TLS	Consulte **Descripciones de TLS** para obtener una descripción de las diversas opciones.
Codificación de caracteres	Elija ASCII, EBCDIC o IPARS (predeterminado) como conjunto de códigos.
Archivo de configuración	Introduzca el archivo de configuración (CNF) que asocia la información de configuración apropiada para un host específico.
Dirección de terminal	Seleccione si desea especificar la dirección de terminal o utilizar el Administrador de ID de Terminal. • **Dirección de terminal**: especifique si desea utilizar el modo de direccionamiento de 2 o 4 bytes. Aunque se requiere una dirección única de 5 bytes cuando se especifica el ID del terminal en lugar de utilizar el Administrador de ID, esta opción especifica cuántos bytes de la dirección ID del terminal de 5 bytes se envían con cada mensaje con el fin de multiplexar. Si especifica el modo de direccionamiento de 2 bytes, sólo se envían los últimos 2 bytes de la dirección de grupo ASCU (Agent Set Control Unit) (A1, A2). Si especifica el modo de direccionamiento de 4 bytes, se envía la dirección de grupo ASCU completa (H1, H2, A1, A2). Especifique la dirección de terminal única de 5 bytes para esta sesión. La dirección del terminal se compone de cinco valores de 2 dígitos hex en este orden: H1, H2, A1, A2 y TA (dirección de terminal). Esta dirección única suele ser asignada por el administrador de la red. • **Administrador de ID de Terminal** - provee IDs a las aplicaciones del cliente en ejecución. Si elige esta opción, hay opciones de configuración adicionales a completar. Véase **Criterios del Administrador de ID de Terminal** para la descripción de estas opciones.

Más información

- Descripciones de TLS
- Criterios del Administrador de ID de Terminal

4.4 Proporcionar acceso a las sesiones de host

Los usuarios finales acceden a las sesiones a través de un servidor de sesión o del portal de listas de sesiones asignadas. Con ambas opciones, una vez autenticados, a los usuarios se les presenta una lista de sesiones a las que pueden acceder y que pueden lanzar correctamente.

> **Consejo**
>
> Es recomendable utilizar un equilibrador de carga para obtener una mayor disponibilidad y capacidad de ampliación. Consulte Planificación de la distribución para obtener más información.

4.4.1 Servidores de sesión

Por lo general, para acceder a las sesiones, los usuarios se desplazan a los servidores de sesión, normalmente a través de un equilibrador de carga.

El acceso de los usuarios finales a un servidor de sesión está disponible en `https://<servidor de sesión>:7443/`.

4.4.2 Lista de sesiones asignadas

Mediante la lista de sesiones asignadas, los usuarios pueden iniciar todas las sesiones desde un portal consolidado basado en HTML. Una vez que se haya autenticado un usuario, este verá la lista de sesiones asignadas.

La lista de sesiones asignadas está disponible en `https://<servidor MSS>/sessions/`.

Consulte Configuración de la lista de sesiones asignadas para obtener información sobre cómo configurar la lista de sesiones asignadas.

4.5 Gestión de las Preferencias de usuario

Como administrador, usted puede especificar qué opciones pueden configurar los usuarios para sus sesiones. Estas opciones se configuran para cada sesión individual y todos los usuarios que tienen acceso a una sesión en particular pueden configurar su propia instancia de la sesión.

1. En el panel de navegación izquierdo, seleccione **Reglas de Preferencias de Usuario**.

2. Seleccione qué opciones desea permitir configurar a sus usuarios.

3. Haga clic en Guardar.

Cada una de las configuraciones de los usuarios son específicas para su instancia de la sesión y no entrará en conflicto con las de otros usuarios.

La opción **Restablecer valores predeterminados** está disponible en los diversos paneles de visualización y parámetros. Como administrador, esta opción restablece el cliente Web a sus valores predeterminados. Para los usuarios finales, esta opción restablecerá los valores definidos por el administrador cuando se creó la sesión.

> ⚠ **Advertencia**
>
> Si el método de autenticación se ha establecido en «None» (Ninguno), tenga en cuenta que todos los usuarios comparten la misma configuración. Durante la configuración de la sesión, es recomendable no permitir que los usuarios modifiquen la configuración de la sesión (Reglas de Preferencias de Usuario) porque pueden sobrescribir las opciones de otros usuarios. Para solucionar este problema, es posible proporcionar identidades de usuario de distintas formas.

Más información

- Parámetros de pantalla
- Especificar las opciones de edición
- Transferir archivos
- Crear Macros

4.6 Personalización de las sesiones de host

4.6.1 Personalización de las sesiones de host

Puede elegir entre estas funciones para personalizar sesiones para sus usuarios finales:

- **Plus** - Habilitar controles personalizados para un flujo de trabajo más eficiente y para disponer de una interfaz de usuario más moderna y fácil de usar. Véase Utilizar Plus para personalizar pantallas.

  Con esta opción usted puede agregar sugerencias de herramienta a los campos, sustituir listas numeradas anticuadas por listas desplegables más modernas, agregar botones a la interfaz del host y programarlos para iniciar macros o ejecutar otras acciones y sustituir la entrada manual de fecha por un selector de fecha con calendario gráfico.

- **Eventos Lado Servidor** - Ofrece código de procedimiento Java que amplía y mejora la presentación de los datos del host.

  Utilizando eventos del lado del servidor, puede definir eventos específicos y suspender la aplicación del host sustituyéndola o interrumpiéndola con el código que haya indicado para la sesión, así como ampliar las opciones de manejo de errores. Por ejemplo, puede agregar un evento que reconozca cuándo se produce un error e implemente entonces el código para interceptar el error, tomar control sobre él y corregirlo. Consulte Eventos del servidor.

- **Avanzadas** - utilizar sólo como le indique el servicio técnico de Micro Focus.

Estas opciones se configuran en el panel Personalización.

1. Haga clic en Configuración en la barra de herramientas para abrir el panel de navegación izquierdo.
2. Haga clic en Personalización.

Más información

- Utilizar Plus para personalizar pantallas
- Usar eventos del servidor

4.6.2 Utilizar Plus para personalizar pantallas

> **Nota**
>
> El componente Plus requiere archivos de almacenamiento (`.rdar`) producidos por Micro Focus Screen Designer versión 9.5 o superior. El Screen Designer está disponible en Micro Focus Rumba Desktop 9.5. Reflection Desktop 16.1 incluye una versión limitada del Screen Designer. Para poder acceder a más controles y aprovechar Plus y el Screen Designer al completo, puede adquirir e instalar el complemento para Micro Focus Reflection Desktop Plus.

1. En el panel **Personalización**, haga clic en **Habilitar Plus**.
2. Seleccione el archivo de almacenamiento Plus que desea utilizar de la lista desplegable o cargue un archivo desde otra ubicación. Los archivos de almacenamiento se identifican por su extensión `rdar` .

   Los archivos de almacenamiento son la salida de un proyecto del Screen Designer y se utilizan para proporcionar los criterios de control personalizado.

   Si está actualizando el archivo de almacenamiento Plus (`.rdar`) asociado a su sesión con Plus habilitado, debe eliminar primero la carpeta que contiene el archivo .rdar antiguo del servidor de sesión. Una vez que haya eliminado la carpeta, puede abrir su sesión con Plus habilitado y el nuevo archivo rdar será descargado al servidor de sesión.
3. Compruebe que el número de milisegundos para el tiempo de retraso de establecimiento del host es preciso. Éste es el tiempo que el host espera una conexión síncrona antes de decidir que el host ha concluido el envío de datos.
4. Cuando usted vuelve a su sesión, Plus está disponible. Haga clic en  en la barra de herramientas para desactivar los controles personalizados.

Cuando usted habilita Plus para una sesión, todos los usuarios finales de esa sesión ven el icono Plus en la barra de herramientas y todos los controles disponibles mediante el archivo de personalización del Screen Designer.

Más información

- Personalización de las sesiones de host

4.6.3 Usar eventos del servidor

Mediante los eventos del servidor, se puede suministrar código Java de procedimiento que puede ampliar y mejorar la presentación de los datos del host.

El panel Personalización le indica al cliente web dónde encontrar el evento después de configurarlo. Consulte Uso del SDK de Java para obtener instrucciones sobre cómo usar el SDK y los ejemplos disponibles.

1. Abra el panel **Personalización**.

2. En **Eventos Lado Servidor**, escriba el nombre completo de clase para el evento.

3. Inicie la sesión y pruebe el evento.

Acceda a la documentación de la API y ejemplos de eventos.

Más información

- Personalización de las sesiones de host
- Uso del SDK de Java
- Desarrollo

4.7 Registro

4.7.1 Ubicar archivos de registro

Hay dos archivos de registro disponibles:

- `<directorio_de_instalación>/sessionserver/sessionserver.log` - el archivo de registro para la aplicación del servidor de sesión.
- `<directorio_de_instalación>/sessionserver/container.log` - el archivo de registro del contenedor que aloja la aplicación Host Access for the Cloud.

4.7.2 Configurar la rotación de registros

Para configurar la rotación de registros, edite los valores de `<directorio_de_instalación>\sessionserver\microservices\sessionserver\service.yml` :

```
LOGGING_FILE_MAXSIZE
LOGGING_FILE_MAXHISTORY
```

4.7.3 Configurar niveles de registro

Hay varios tipos de niveles de registro que usted puede utilizar para producir distintos tipos de información. Puede configurar niveles de registro en `<directorio_de_instalación>\sessionserver\microservices\sessionserver\service.yml` .

> **nota**
>
> Deben aplicarse sangrías a las líneas en `service.yml` mediante espacios.

Utilice el siguiente formato para establecer los niveles de registro:

```
- nombre: logging.level.<logger>
  valor: "<log level>"
```

Donde `<logger>` es el nombre del registrador a ajustar y `<log level>` es uno de los siguientes:

- **Trace**: designa eventos informativos de nivel granular más fino que "Debug".
- **Debug**: designa eventos informativos de nivel granular fino que son muy útiles para depurar una aplicación.
- **Info**: designa mensajes informativos que resaltan el progreso de la aplicación en un nivel granular grueso.
- **Warn**: designa situaciones potencialmente nocivas.
- **Error**: designa eventos de error que pueden permitir que la ejecución de la aplicación continúe.
- **Fatal**: designa eventos de error muy graves que posiblemente harán que la aplicación finalice.

> **Nota**
>
> Debe reiniciar el servidor de sesión después de realizar cambios en `service.yml`.

4.7.4 Cómo habilitar el registro de servidor de cliente web a sesión

Aunque el navegador proporciona un mecanismo básico para entrar a su consola de JavaScript, el cliente Web amplía esta función y, con algo de configuración, se pueden registrar eventos en el servidor de sesión para que los vea un administrador.

Por defecto, no se registra nada en el servidor de sesión. **Para poder habilitar esta función**, debe definir el nivel de registro mediante las instrucciones que se indican a continuación.

Los niveles de registro son: `debug` (depuración), `info` (información), `warn` (advertencia), `error` u `off` (desactivado). El nivel de registro por defecto es `off` (desactivado).

Ajuste del nivel de registro para los usuarios de todos los clientes web

Para ajustar el nivel de registro para todos los clientes Web, añada la siguiente entrada a `<directorio_de_instalación>\sessionserver\microservices\sessionserver\service.yml`

```
-name: <registrador>
 value: "<nivel de registro>"
```

Donde `<registrador>` es:

```
logging.level.com.microfocus.zfe.webclient.core.handler.ClientLoggingHandler-webclient
```

> **Nota**
>
> Tenga cuidado al aumentar el nivel de registro para los usuarios de todos los clientes web en un entorno de producción debido a que puede producirse un aumento en el tráfico de red.

Ajuste del nivel de registro para un usuario individual

Existen dos opciones para ajustar el nivel de registro de usuarios individuales:

- Para ajustar temporalmente el nivel de registro para una instancia de cliente Web de un usuario específico sin necesidad de reiniciar el servidor de sesión, indique al usuario que añada el siguiente parámetro de URL al cargar el cliente Web en el navegador:

  -`https://mysessionserver.com:7443/?log=<nivel de registro>`-

- Para ajustar el nivel de registro de un usuario individual sin necesidad de que este realice cambios, añada la siguiente entrada a `service.yml`:

  ```
  -name: <logger
   value: "<nivel de registro>"
  ```

  Donde `<registrador>` es:

  ```
  logging.level.com.microfocus.zfe.webclient.core.handler.ClientLoggingHandler-webclient-<nombre de usuario>
  ```

  Donde `<nombre de usuario>` es el nombre de usuario de la persona cuyos niveles de registro se van a ajustar.

> **Nota**
>
> El registro basado en un nombre de usuario requiere un modo de autenticación que incluya nombres de usuario.

5. Uso de HACloud

5.1 Uso de Host Access for the Cloud

Se dispone de múltiples opciones de sesión y pantalla que le permiten personalizar su sesión y asegurarse de que trabaja de forma eficiente.

- Parámetros de pantalla
- Asignar teclas
- Configurar macros de usuario
- Transferir archivos
- Especificar las opciones de edición
- Trabajar con sesiones
- Crear Macros
- Impresión

5.2 Parámetros de pantalla

Los ajustes de pantalla varían en función del tipo de host y son específicos para la sesión que usted está configurando.

5.2.1 Asignación de color

Puede personalizar el color de su pantalla y el aspecto de distintos atributos del host en la ventana del terminal. Puede seleccionar para cada elemento un color para el primer plano y los colores de fondo para las todas las conexiones host soportadas. Los colores se especifican utilizando la tabla de color o ingresando el formato de código hex.

Hay muchos sitios web que ofrecen un listado de los colores hex disponibles, para un ejemplo véase w3schools.com HTML Color Picker.

Podrá ver diferentes opciones en función del tipo de conexión host.

Opciones específicas de hosts UTS

- **Utilizar información de color del host** - Para utilizar los colores especificados aquí en lugar de otros colores especificados por el host, desactive esta casilla.
- **Habilitar parpadeo** - Para deshabilitar el parpadeo, desactive esta casilla.
- **Seleccionar atributo para editar** - En la emulación UTS, los colores son configurados directamente por el host. Puede especificar colores para texto asociado a opciones específicas de visualización de pantalla. Entre ellas se encuentran las siguientes combinaciones disponibles:

  Plano, Subrayado (UND), Tachar (STK), Separador de Columnas Izquierdo (LCS), Página de Control y Línea de Estado (OIA).
- **Intensidad de Vídeo** - Las intensidades de vídeo Parpadeo, Atenuar, Protegido y Negativo se combinan con los atributos para crear combinaciones adicionales. Por ejemplo, puede asignar colores de primer plano o de fondo a todas las celdas con Atenuar + Parpadeo + Subrayado o Negativo + Protegido + Tachar + Subrayado.

  Cuando usted selecciona una intensidad de vídeo (o una combinación de intensidades), estas intensidades se combinan con el valor de la lista desplegable de atributos para formar una asignación de color única.

Opciones específicas de hosts VT y T27

- **Habilitar parpadeo** - Para deshabilitar el parpadeo, desactive esta casilla.
- **Habilitar negrita** - Muestra el texto establecido con atributos en negrita como texto en negrita en la ventana del terminal. Para visualizar caracteres en negrita como texto plano, desactive esta opción.

- **Habilitar subrayado** - Muestra el texto subrayado.
- **Vídeo inverso (solo para VT)**: esa opción invierte los colores de primer plano y de fondo cuando el host VT envía una secuencia de escape de vídeo inverso. Si la opción no está habilitada, las secuencias de vídeo inverso enviadas por el host se ignoran.

Para personalizar colores para todos los tipos de host

1. En el panel de navegación izquierdo, haga clic en Visualizar.
2. En Asignaciones de Colores, haga clic en el campo de color de fondo para abrir la tabla de color. En la tabla de color, seleccione el color que dese utilizar como color de fondo del host. De forma alternativa, escriba el número de color hex que desee utilizar.
3. En la lista desplegable, seleccione el color de host predeterminado que desee cambiar. Por ejemplo, si selecciona Host Rosa en la lista desplegable y, a continuación, cambia el color de primer plano a rojo, siempre que se encuentre con un texto en color rosa, este aparecerá en color rojo.
4. Abra la tabla de color para el primer plano a fin de elegir un nuevo color y asignarlo al texto o escriba el código hexadecimal que desee utilizar. Seleccione Fondo para asignar el nuevo color al campo de fondo.
5. Haga clic en Guardar para cerrar el panel Visualización y reanudar la configuración de su conexión host.

Restablecer valores predeterminados borra todos los cambios que haya realizado y restablece los colores a la configuración del host por defecto.

5.2.2 Configurar zonas activas

Las zonas activas son botones que se muestran sobre comandos de host comunes en las sesiones de terminal. Cuando utiliza zonas activas, puede controlar la sesión de terminal con un ratón o toques con el dedo en lugar de con el teclado. La zona activa transmite una tecla o un comando de terminal al host. De forma predeterminada, las zonas activas están configuradas para los comandos 3270, 5250y VT más comunes.

Las zonas activas están habilitadas y visibles de forma predeterminada, sin embargo usted puede deshabilitar las zonas activas para una sesión particular o puede ocultarlas.

- Habilitar zonas activas

  Elija No para deshabilitar las zonas activas para la sesión a la que se está conectando.

- Mostrar zonas activas

  Elija No para ocultar las zonas activas en la pantalla. Las zonas activas siguen estando operativas.

Zonas activas para hosts 3270

Zona activa	Descripción
PF1...PF24	Transmite una PF1...PF24 al host
PA1, PA2 o PA3	Transmite una PA1, PA2 o PA3 al host
intro	Transmite una tecla Intro al host
más	Transmite una tecla Borrar al host

Zonas activas para hosts 5250

Zona activa	Descripción
intro	Transmite una tecla Intro al host
más	Transmite una tecla Subir al host (desplaza una página hacia abajo)
PF1...PF24	Transmite una PF1...PF24 al host

Zonas activas para hosts VT

Zona activa	Descripción
F1...F20	Transmite una F1...F20 al host

5.2.3 Configurar dimensiones de pantalla para hosts VT, UTS y T27

Como administrador, usted puede seleccionar el número de columnas y filas para las sesiones VT, UTS y T27.

1. Abra el panel Visualización.
2. En Dimensiones, especifique el número de columnas y filas que desea que tenga cada pantalla. Los valores por defecto son 80 columnas por 24 filas.

   Hay disponibles algunos parámetros de configuración específicos del host:

   - Páginas - Si se está conectando a una pantalla de host T27, puede establecer el número de páginas a visualizar. El valor por defecto es 2.
   - Borrar al cambiar de host - Si se está conectando a una pantalla de host VT, seleccione esta opción para borrar la ventana del terminal y mover el contenido al búfer de desplazamiento hacia atrás cuando el tamaño de la columna cambia.
3. Haga clic en Save (Guardar).

5.2.4 Configurar opciones de cursor

Utilice las opciones de cursor para configurar la apariencia y el comportamiento del cursor y de la regla.

Esta opción	Tiene esta función...
Tipo de cursor	• Subrayado muestra el cursor de texto como subrayado. • Barra vertical muestra el cursor como una línea vertical. • Bloque muestra el cursor de texto como bloque de vídeo inverso.
Tipo de regla	• Vertical muestra una regla vertical en la posición del cursor. • Horizontal muestra una regla horizontal en la posición del cursor. • Cruz muestra una regla horizontal y una vertical en la posición del cursor.
Color del cursor	Haga clic en el campo de color para abrir la tabla de color. En la tabla de color, seleccione el color que dese utilizar como color para el cursor y la regla. De forma alternativa, escriba el número de color hex que desee utilizar.
Parpadeos de cursor	De forma predeterminada, el cursor parpadea (en el modo de bloque o subrayado). Desactive esta opción para visualizar un cursor visible sin parpadeo.

5.2.5 Configurar opciones de fuente

Utilice estas opciones de fuente para asegurarse de que sus caracteres de terminal se visualizan en el tamaño de fuente y estilo que prefiera.

Esta opción	Tiene esta función...
Tamaño de fuente	• Auto (por defecto): se ajusta automáticamente la escala de la fuente de acuerdo con el tamaño de la ventana. Cuando esta opción está seleccionada, puede seleccionar Conservar proporciones, lo que significa que el tamaño de fuente se ajustará dinámicamente sin que la visualización del terminal se expanda o escale para llenar el espacio disponible. • Fijo Especifica el tamaño en píxeles para la visualización de la ventana del terminal.
Carácter cero	Para diferenciar entre el carácter cero predeterminado de la letra O, seleccione una de las siguientes opciones: • Por defecto • Cero con una barra • Cero con un punto

5.2.6 Configurar opciones de búfer de desplazamiento hacia atrás VT

El búfer de desplazamiento hacia atrás VT contiene los datos que se han salido de la pantalla y han dejado de estar accesibles para la computadora host. Cuando existe un búfer de desplazamiento hacia atrás, puede verlo utilizando la barra de desplazamiento vertical.

El búfer de desplazamiento hacia atrás está habilitado de forma predeterminada. Si esta opción está habilitada, la sesión mantiene un búfer de las líneas que se han desplazado fuera de la

pantalla de terminal. Esta opción está disponible para todos los usuarios que han obtenido permiso del administrador para modificar Parámetros de Visualización de Terminal.

Esta opción	Tiene esta función...
Límite de filas de desplazamiento hacia atrás	Limita el número de filas contenidas en el búfer de desplazamiento hacia atrás. El valor por defecto es 500 filas.
Guardar visualización antes de borrarla	Cuando la opción está seleccionada (valor predeterminado), los datos de la pantalla del terminal pasan al búfer de desplazamiento hacia atrás cuando usted o el host borran la pantalla del terminal. Si no desea guardar la pantalla del terminal en el búfer de desplazamiento hacia atrás, desactive esta opción; cuando la pantalla del terminal se borre, los datos se descartan
Guardar de zonas de desplazamiento	Cuando los márgenes superior e inferior de la pantalla están configurados (por ejemplo, por un editor de texto EDT o TPU o con la función DECSTBM), el área que se encuentra entre los márgenes se llama zona de desplazamiento. Cuando esta opción está desactivada, el texto que se haya desplazado dentro de esta zona no se guarda en el búfer de desplazamiento hacia atrás. Seleccione esta opción para guardar la información que encuentra dentro de las zonas de desplazamiento en el búfer de desplazamiento hacia atrás. Nota: Esto puede hacer que la memoria de pantalla se llene rápidamente.
Guardar antes de borrar de cualquier fila	Esta opción especifica si los datos que se han borrado de una parte de la ventana del terminal se guardan en la memoria de pantalla.
Comprimir filas en blanco	Seleccione esta opción para ahorrar espacio en la memoria de pantalla al comprimir varias filas en blanco en una sola.

5.2.7 Configurar opciones de teclado

Puede configurar las siguientes opciones de teclado:

- Opciones de 3270
- Opciones de 5250
- Opciones de VT
- Opciones T27

Opciones de 3270

- Anticipación de escritura

  Si se ha seleccionado esta opción, Host Access for the Cloud guarda en el búfer los caracteres que teclea en la ventana del terminal. La anticipación de escritura permite seguir escribiendo después de enviar los datos al host. Sin la anticipación de escritura, los caracteres que usted escribe se ignoran hasta que el host está preparado para recibir más datos.

- Ajuste de líneas

  Cuando esta opción está seleccionada, la funcionalidad de ajuste de líneas está habilitada en un campo multilínea no protegido. En el modo de ajuste de líneas, algunos de los espacios en blanco entre las palabras son sustituidos por saltos de línea de modo que cada línea está visible en la ventana del terminal y se puede leer sin necesidad de desplazamiento horizontal.

- La tecla de atención envía

  Especifica qué se envía cuando se pulsa la tecla ATTN. Las opciones son Interrupción Telnet, Anular salida e Interrupción del proceso.

Opciones de 5250

- Anticipación de escritura

  Si se ha seleccionado esta opción, Host Access for the Cloud guarda en el búfer los caracteres que teclea en la ventana del terminal. La anticipación de escritura permite seguir escribiendo después de enviar los datos al host. Sin la anticipación de escritura, los caracteres que usted escribe se ignoran hasta que el host está preparado para recibir más datos.

- Restablecer automáticamente error

  Cuando la opción está seleccionada, la tecla siguiente que se pulsa después de un error de teclado borra el error, restablece los datos de la línea previos al error e intenta ejecutar la pulsación de la tecla del siguiente modo:

Si el cursor se encuentra en un campo de entrada válido y la tecla es una tecla de datos, los datos se introducen allí si son datos válidos para ese campo (por ejemplo, un carácter numérico en un campo de entrada que sólo acepta números).

- Si el cursor está en un campo de entrada válido y la tecla es una tecla de función, la operación de la tecla se ejecuta.
- Si la posición actual del cursor no es un campo de entrada válido y la tecla es una tecla de datos, el cursor se mueve al siguiente campo de entrada válido y los datos se introducen allí si los datos son válidos para ese campo.
- Si la posición actual del cursor no es un campo de entrada válido y la tecla es una tecla de función, el cursor se mueve al siguiente campo de entrada válido y la tecla se ignora.
- Si la pantalla actual no contiene campos de entrada válidos, verá un mensaje de error cada vez que pulse una tecla y no se ejecuta ninguna tecla

Cuando la opción no está seleccionada, debe pulsar Reset para borrar el mensaje de error de la línea de error antes de poder reanudar la entrada de datos.

Esta opción no está seleccionada por defecto.

- El campo Waive comprueba la clave PF

  Seleccione esta opción para permitir el envío de claves PF al host desde los campos restringidos. Esta opción está borrada de forma predeterminada.

Opciones de VT

- Retroceso envía

  Configura la función que envía la tecla de retroceso. En el teclado del terminal VT, la tecla de flecha atrás `(<x)` se puede configurar: puede enviar un carácter para suprimir (ASCII 127) o un carácter de retroceso (ASCII 8).

- Eco local (VT)

  Esta opción hace que cada carácter que escriba con el teclado se muestre en la pantalla. Esta opción está desactivada de forma predeterminada ya que la mayoría de los hosts envían de vuelta los caracteres recibidos.

- Teclas de dirección

  Controla los caracteres que transmiten las cuatro teclas de dirección (en ambos teclados, el numérico y el de edición). Normalmente, la aplicación del host se encarga de establecer este valor. En general, debe mantener este valor en Normal.

  Si las teclas de dirección no funcionan correctamente, puede que esta opción se haya configurado erróneamente en Aplicación al cerrarse incorrectamente un programa del host. Al cambiar este valor a Normal, se debe solucionar el problema con las teclas de flecha.

- Teclado numérico

Controla los caracteres que transmiten las teclas del teclado numérico. Normalmente, la aplicación del host se encarga de establecer este valor. En general, debe mantener este valor en Numérico.

Si las teclas numéricas o de función del programa (PF) no funcionan correctamente, puede que esta opción se haya dejado erróneamente en Aplicación al cerrarse incorrectamente un programa del host. Cambiando este valor a Numérico debe quedar solucionado el problema con el teclado numérico.

Opciones T27

- Habilitar minúsculas (T27)

  Habilita la visualización de letras minúsculas y mayúsculas en la pantalla. Predeterminado. Si esta opción está deshabilitada, sólo se visualizan las letras mayúsculas.

5.2.8 Configuración del terminal

La configuración del terminal varía en función del tipo de host.

Configuración de terminal 3270 y 5250

- Juego de caracteres de host

  Seleccione el juego de caracteres de host 3270 o 5250 que desea utilizar. Este parámetro elige una tabla de conversión para convertir los caracteres de host (EBCDIC) en caracteres de PC (ANSI). Este parámetro debe coincidir con el juego de caracteres nacional utilizado por el sistema host. Si no coincide, puede que algunos caracteres, como los acentos, no se muestren correctamente. Consulte la documentación del host para ver la definición de los caracteres de cada juego. El valor por defecto es Inglés (EE. UU.) (037).
- Código de gráficos extendidos de país específico (solo 3270)

  Si se selecciona esta opción (predeterminada), aparecerán caracteres adicionales en el Juego de caracteres nacional configurado. Consulte la documentación del host para obtener más información.

Configuración del terminal VT

- Tipo de terminal (VT)

  Especifica el terminal que se debe emular. Estas opciones determinan los códigos que generará el teclado numérico, la interpretación de las funciones de control y la respuesta a las solicitudes de identificación del terminal.
- ID de terminal (VT)

  Especifica la respuesta que Host Access for the Cloud envía al host tras una petición de atributos de dispositivo (DA) primaria. Esta respuesta informa al host sobre las funciones de

terminal que puede llevar a cabo. Este valor no depende del valor de tipo de terminal. Si se establece en el valor por defecto de Reflection, Host Access for the Cloud responde a una petición de DA primaria con el conjunto de funciones que admite. Si su host requiere un ID de terminal más específico, seleccione otro valor de la lista.

- Nueva línea (VT)

  Seleccione esta opción para enviar un retorno de carro y un salto de línea cuando pulsa Intro. Cuando Host Access for the Cloud recibe un salto de línea, un salto de página o un tabulador vertical, mueve el cursor a la primera columna de la siguiente línea. Si esta opción está desactivada (predeterminada), la tecla Intro envía sólo un retorno de carro. El salto de línea, salto de página o tabulador vertical recibido del host mueve el cursor una línea hacia abajo en la columna actual. Si las líneas en pantalla se sobrescriben (es decir, el host no envía un salto de línea con el retorno de carro), seleccione esta opción. Si se selecciona la opción Nueva línea, pero el host no espera recibir un salto de línea con cada retorno de carro, las líneas aparecen con doble espaciado en la pantalla.

Configuración del terminal T27

- Juego de caracteres de host (T27)

  Con esta opción puede especificar la conversión de host a pantalla. Seleccione el lenguaje utilizado para convertir los caracteres recibidos del host antes de que se visualicen en la máquina local. El valor predeterminado es Sin conversión.

5.2.9 Configurar otras opciones de visualización

Esta opción	Tiene esta función...
Separador de columnas (5250)	Utilice esta opción para especificar qué carácter (de proceder) se debe utilizar para representar separadores de columnas en sesiones de terminal 5250. Las opciones son: • Puntos- Se utilizan puntos para separar columnas. El valor por defecto. • Barras verticales - Utilizar líneas verticales para separar las columnas. • Ninguno - No se utilizan caracteres para separar columnas
Subrayar campos de entrada (3270, 5250)	Puede determinar cómo tratar el subrayado de los campos de entrada del host: • El host controla el subrayado (por defecto) • Subrayar siempre los campos de entrada • No subrayar nunca los campos de entrada
Línea de estado (VT)	Para habilitar una línea de estado en la parte inferior de la pantalla. • Ninguna para deshabilitar la línea de estado. (Por defecto) • Indicador para visualizar la página, la posición del cursor y el estado de la impresora. • Host de escritura para tener la información de pantalla de la aplicación host en la línea de estado.
Conservar proporciones	Seleccione esta opción para conservar las proporciones de la pantalla del host independientemente del tamaño de la ventana del navegador. Las proporciones describen la relación proporcional entre la anchura y la altura de una imagen.
Mostrar OIA (3270, 5250)	Seleccione esta opción para visualizar los mensajes de funcionamiento y de estado en el Área de Información del Operador (OIA) en la parte inferior de la ventana del terminal. De forma predeterminada, la visualización del OIA está habilitada.
Mostrar línea de estado (ALC)	Activa una línea de estado en la parte inferior de la pantalla.
Ignorar clic de ratón al activar ventana	Cuando un clic de ratón activa la ventana del terminal, esta opción especifica si las acciones como actualizar la posición del cursor del terminal, borrar una selección o ejecutar una zona activa, se deben ejecutar también. De forma predeterminada, estas acciones no se ejecutan.

Ajuste automático (VT)	Cuando la opción está seleccionada, los caracteres se ajustan automáticamente en el margen derecho y se continúa en la línea siguiente. Cuando la opción está desactivada, los caracteres no se ajustan cuando alcanzan el margen derecho de la pantalla. Los caracteres nuevos sobrescriben el carácter en el margen derecho hasta que se introduce un retorno de carro.

5.3 Asignar teclas

5.3.1 Asignar teclas

Puede crear accesos directos de teclado que realicen cualquier acción asignable durante una sesión. La página Asignación de Teclado ofrece una vista de la asignación de teclado predeterminada para cada tipo de host y las teclas personalizadas asignadas para esa sesión en negrita.

Consulte Asignación de teclado de host para obtener información sobre las diferentes asignaciones de teclado.

Asignar teclas como administrador y como usuario final

Hay algunas diferencias en el comportamiento entre el administrador y el usuario final cuando se asignan teclas.

- Los usuarios finales solo pueden añadir o modificar asignaciones de teclas si el administrador les concede permiso mediante el panel Reglas de Preferencias de Usuario.
- Cualquier cambio que haga el administrador se mostrará al usuario final como indistinguible de las asignaciones de teclas del host predeterminadas. Una vez concedido el permiso, la persona puede modificar, añadir o eliminar cualquier asignación, independientemente de los cambios del administrador. Sin embargo, cuando se restablecen las asignaciones de teclas sólo se restablecen al estado modificado creado por el administrador para la sesión actual.

Añadir o modificar teclas asignadas

1. En la barra de herramientas, haga clic en Configuración.
2. En el panel de navegación izquierdo, abra el panel Asignaciones de Teclado. Las teclas asignadas para el tipo de host al que se está conectando están visibles.
3. Para añadir una nueva asignación de tecla:
   - Haga clic en . Puede elegir entre escribir la secuencia de teclas que desea utilizar o utilizar el teclado alternando entre las dos opciones.
   - En la lista desplegable Acción, seleccione la acción que desee asociar a la selección de tecla. Si selecciona Enviar texto, ingrese la cadena que desea enviar al host en el campo Valor. De forma similar, si selecciona Ejecutar macro, seleccione la macro que desea activar con el método abreviado de teclado. Debe crear la macro antes de poder asignarla a la acción Ejecutar Macro.

     La acción Enviar texto admite la asignación de caracteres con códigos inferiores o iguales a `0xFFFF` mediante secuencias de escape Unicode. La secuencia de escape empieza con `\u` seguida de exactamente cuatro dígitos hexadecimales. Usted puede integrar secuencias de escape Unicode en cualquier cadena. Por ejemplo, este elemento `\u0045` incrustado se interpretará como esta E incrustada, ya que 45 es el código hexadecimal del carácter E.

     Para enviar secuencias de escape Unicode al host, escape la secuencia anteponiendo una barra invertida. Por ejemplo, para enviar la cadena literal \u001C al host, asigne una tecla a `\\u001C`. Host Access for the Cloud convertirá esto a la cadena `\u001C` cuando se pulse esa tecla y enviará los seis caracteres de la cadena resultante al host.

     La acción Deshabilitar deja la tecla inoperable. Cuando se pulsa la tecla no se inicia ninguna acción. Esto difiere de la acción Desasignar, que elimina la asignación de tecla, pero conserva un acceso directo del navegador si está definido.
   - Haga clic en la marca de verificación azul para aceptar la asignación y añadir la asignación de la tecla a la sesión.
4. Para modificar una asignación existente:

   Seleccione la fila que contiene la tecla que desea modificar.

   Siga los pasos para añadir una nueva asignación de teclas. Para ello, haga clic en a fin de guardar la nueva asignación. Alternativamente, puede hacer clic fuera de la fila modificada y el cambio se guardará. Todas las asignaciones nuevas y modificadas se indican en negrita. Puede restablecer la asignación de teclas original en cualquier momento. Para ello, haga clic en .

Filtrar la lista

El campo Filtro facilita la visualización de las asignaciones en las que está interesado. El filtro se basa en palabras clave y afecta a cada columna de la tabla. Por ejemplo, si introduce Enviar texto en el campo Filtro, solo se mostrarán teclas asignadas a la acción Enviar texto.

Si utiliza la opción Mostrar sólo asignaciones modificadas, únicamente verá las asignaciones que se hayan modificado previamente.

Algunas cosas que recordar:

- Asignar las teclas modificadoras derecha e izquierda a acciones individuales

  Puede asignar las teclas modificadoras derecha e izquierda a acciones individuales. De todos modos, cuando se combinan con otras teclas no se distingue entre las teclas derecha e izquierda. Por ejemplo, Alt-Izquierda se puede asignar a la Acción-A mientras que Alt-Derecha está asignada a la Acción-B, pero Alt-Izquierda+H se guardará como Alt+H y ambas combinaciones Alt-Izquierda+H Alt-Derecha+H se asociarán con a sola acción asignada.

- Combinaciones de teclas y operaciones de copiar/pegar

  Hay distintas combinaciones de teclas que se utilizan también para operaciones de copiar/pegar. Por ejemplo, en una pantalla de host VT, Ctrl+ Mayús + A inicia una acción de Seleccionar Todo. Consulte "Edición de la pantalla" para obtener una lista de las acciones de las teclas de copiar y pegar.

- Accesos directos de teclado y navegadores

  Los teclados utilizan accesos directos de teclado para ahorrar tiempo y clics de ratón. A la hora de asignar pulsaciones de teclas es importante recordar lo siguiente. Accesos Directos de Teclado Útiles ofrece un resumen de los accesos directos de teclado utilizados por distintos navegadores. En la mayoría de los casos, las asignaciones de teclas de Host Access for the Cloud tienen prioridad sobre los accesos directos de teclado del navegador. Ocasionalmente, cuando este no es el comportamiento que se desea para una combinación específica de teclas, puede elegir Quitar asignación en la lista de acciones para anular la asignación del acceso directo. Esto permite que el evento de tecla pase al navegador.

5.3.2 Asignación de teclado de host

Las siguientes tablas muestran las teclas predeterminadas, el nombre y la descripción de las teclas para las distintas asignaciones de teclado de host.

- Asignación de teclado IBM 3270
- Asignación de teclado IBM 5250
- Asignación de teclado VT
- Asignación de teclado UTS
- Asignación de teclado T27
- Asignación de teclado ALC

Asignación de teclado IBM 3270

Tecla	Asignar a	Descripción
Ctrl + F1	Atención	Envía la tecla ATTENTION al host
Mayús + Tabulador	Tecla retroceso	Mueve el cursor al campo desprotegido anterior
Ctrl + F2	Borrar	Borra la pantalla y envía la tecla CLEAR al host
Alt + Flecha izquierda	Cursor doble izquierda	Mueve el cursor dos posiciones hacia la izquierda
Alt + Flecha derecha	Cursor derecha doble	Mueve el cursor dos posiciones hacia la derecha
Ctrl + F3	Selección de cursor	Simula una selección de lápiz óptico en el campo actual
Alt + Eliminar	Borrar palabra	Borra tres caracteres del campo actual
Ctrl + 5	Duplicar	Inserta el carácter DUP en la posición del cursor
Intro	Intro	Envía la tecla INTRO al host.
Fin	Eliminar final de campo	Borra todos los datos desde la posición del cursor hasta el final del campo actual
Alt + F5	Eliminar entrada	Borra todos los datos en todos los campos no protegidos de la pantalla actual
Ctrl + Alt + F	Delimitador de campo	Alterna la visualización o no visualización de los delimitadores de campo en la pantalla
Ctrl + 6	Marca de campo	Inserta el carácter Marca de campo en la posición del cursor
Inicio	Inicio	Mueve el cursor al primer campo sin protección de la pantalla
Insertar	Insertar	Alterna el modo Insertar.
Mayús + Intro	Nueva línea	Mueve al siguiente campo sin protección
Ctrl + 1	PA1	Envía la tecla PA1 al host
Re Pág	PA1	Envía la tecla PA1 al host
Ctrl + 2	PA2	Envía la tecla PA2 al host
Av Pág	PA2	Envía la tecla PA2 al host

Tecla	Asignar a	Descripción
Ctrl + 3	PA3	Envía la tecla PA3 al host
F1 - F10	PF1 - PF10	Envía la tecla PF1, PF2...PF10 al host
Alt + 1 o F11	PF11	Envía la tecla PF11 al host
Alt + 2 o F12	PF12	Envía la tecla PF12 al host
Mayús + F1	PF13	Envía la tecla PF13 al host
Mayús + F2	PF14	Envía la tecla PF14 al host
Mayús + F3	PF15	Envía la tecla PF15 al host
Mayús + F4	PF16	Envía la tecla PF16 al host
Mayús + F5	PF17	Envía la tecla PF17 al host
Mayús + F6	PF18	Envía la tecla PF18 al host
Mayús + F7	PF19	Envía la tecla PF19 al host
Mayús + F8	PF20	Envía la tecla PF20 al host
Mayús + F9	PF21	Envía la tecla PF21 al host
Mayús + F10	PF22	Envía la tecla PF22 al host
Alt3	PF23	Envía la tecla PF23 al host
Mayús + F11	PF23	Envía la tecla PF23 al host
Alt4	PF24	Envía la tecla PF24 al host
Mayús + F12	PF24	Envía la tecla PF24 al host
Ctrl + P	Imprimir	Imprime el contenido de la pantalla a la impresora
Escape	Reset	Resetea las condiciones de error del teclado
Ctrl + S	Solicitud de sistema	Envía la tecla SYSTEM REQUEST al host

Asignación de teclado IBM 5250

Tecla	Asignar a	Descripción
Escape	Atención	Envía la tecla ATTENTION al host
Ctrl + F2	Borrar	Borra la pantalla y envía la tecla CLEAR al host
Ctrl + F3	Selección de cursor	Simula una selección de lápiz óptico en el campo actual
Ctrl + Retroceso	Borrar al utilizar Retroceso	Mueve el cursor una posición hacia la izquierda
Ctrl + 5	Duplicar	Inserta el carácter DUP en la posición del cursor
Ctrl + Fin	Final de campo	Mueve el cursor al final de la línea
Fin	Eliminar final de campo	Borra todos los datos desde la posición del cursor hasta el final del campo actual
Alt + Fin	Eliminar entrada	Borra todos los datos en todos los campos no protegidos de la pantalla actual
Alt + F5	Eliminar entrada	Borra todos los datos en todos los campos no protegidos de la pantalla actual
Ctrl + Intro	Salir del campo	Saca el cursor de un campo de entrada
KP + Sustraer	Final de campo menos	Saca el cursor de un campo numérico firmado o de un campo sólo numérico, insertando un signo menos en la última posición de un campo numérico con signo o cambiando la última posición de un campo solo numérico a un carácter alfabético que indica al sistema que este campo tiene un valor negativo.
Ctrl + Sustraer	Final de campo menos	Saca el cursor de un campo numérico firmado o de un campo sólo numérico, insertando un signo menos en la última posición de un campo numérico con signo o cambiando la última posición de un campo solo numérico a un carácter alfabético que indica al sistema que este campo tiene un valor negativo.
KP + Sumar	Final de campo más	En un campo numérico con signo, esta función desplaza el cursor al campo siguiente, quitando un signo menos si hay uno en la última posición. En un campo solo numérico, esta función desplaza el cursor

Tecla	Asignar a	Descripción
		al campo siguiente, cambiando la última posición a un carácter alfabético que indica al sistema que este campo tiene un valor positivo.
Ctrl + Sumar	Final de campo más	En un campo numérico con signo, esta función desplaza el cursor al campo siguiente, quitando un signo menos si hay uno en la última posición. En un campo solo numérico, esta función desplaza el cursor al campo siguiente, cambiando la última posición a un carácter alfabético que indica al sistema que este campo tiene un valor positivo.
Ctrl + 6	Marca de campo	Inserta el carácter Marca de campo en la posición del cursor
Ctrl + H	Ayuda	Envía la tecla Help al host.
Alt + F7	Modo Hex	Pone el terminal en el modo Hex
Inicio	Inicio	Mueve el cursor al primer campo sin protección de la pantalla
Insertar	Insertar	Alterna el modo Insertar.
Mayús + Intro	Nueva línea	Mueve al siguiente campo sin protección
Ctrl + 1	PA1	Envía la tecla PA1 al host
Ctrl + 2	PA2	Envía la tecla PA2 al host
Ctrl + 3	PA3	Envía la tecla PA3 al host
F1 - F11	PF1 - PF11	Envía la tecla PF1, PF2...PF11 al host
Alt + 1	PF11	Envía la tecla PF11 al host
Alt + 2	PF12	Envía la tecla PF12 al host
F12	PF12	Envía la tecla PF12 al host
Mayús + 1	PF13	Envía la tecla PF13 al host
Mayús + F2...F10	PF14...PF22	Envía la tecla PF14...PF22 al host
Alt + 3	PF23	Envía la tecla PF23 al host

Tecla	Asignar a	Descripción
Mayús + F11	PF23	Envía la tecla PF23 al host
Alt + 4	PF24	Envía la tecla PF24 al host
Mayús + F12	PF24	Envía la tecla PF24 al host
Ctrl + P	Imprimir	Imprime el contenido de la pantalla a la impresora
Control	Reset	Resetea las condiciones de error del teclado
Re Pág	Bajar	Envía la tecla Bajar al host.
Av Pág	Subir	Envía la tecla Subir al host.
Ctrl + Inicio	Inicio de campo	Mueve el cursor al principio del campo
Ctrl + S	Solicitud de sistema	Envía la tecla SYSTEM REQUEST al host

Asignación de teclado VT

Tecla	Asignar a	Descripción
Ctrl + Cancelar	Interrup	Envía la tecla Interrup al host.
Ctrl + Intro	Intro	Envía la tecla Intro al host.
Alt + F1	F1	Envía la tecla F1 al host
Ctrl + F1...F10	F11...F20	Envía la tecla F11...F20 al host.
Inicio	Buscar	Envía la tecla Buscar al host.
F1	Retención	Envía la tecla Detener Pantalla al host
Pausa	Retención	Envía la tecla Detener Pantalla al host
Insertar	Insertar	Envía la tecla Insertar al host
Ctrl + Insertar	Teclado numérico 0	Envía la tecla 0 del teclado numérico al host
Ctrl + Fin	Teclado numérico 1	Envía la tecla 1 del teclado numérico al host
Ctrl + Flecha abajo	Teclado numérico 2	Envía la tecla 2 del teclado numérico al host
Ctrl + Av Pág.	Teclado numérico 3	Envía la tecla 3 del teclado numérico al host
Ctrl + Flecha izquierda	Teclado numérico 4	Envía la tecla 4 del teclado numérico al host
Ctrl + Borrar	Teclado numérico 5	Envía la tecla 5 del teclado numérico al host
Ctrl + Flecha derecha	Teclado numérico 6	Envía la tecla 6 del teclado numérico al host
Ctrl + Inicio	Teclado numérico 7	Envía la tecla 7 del teclado numérico al host
Ctrl + Flecha arriba	Teclado numérico 8	Envía la tecla 8 del teclado numérico al host
Ctrl + Re Pág	Teclado numérico 9	Envía la tecla 9 del teclado numérico al host
Ctrl + Alt-suma	Teclado numérico Coma	Envía la coma del teclado numérico al host

Tecla	Asignar a	Descripción
Ctrl + sumar	Teclado numérico -	Envía el signo de resta del teclado numérico al host
Ctrl + decimal	Periodo de teclado numérico	Envía el periodo del teclado numérico al host
Ctrl + Supr	Periodo de teclado numérico	Envía el periodo del teclado numérico al host
Ctrl + Alt + Flecha arriba	Fila arriba	Mueve una fila arriba en el búfer de desplazamiento hacia atrás
Ctrl + Alt + Flecha abajo	Fila abajo	Mueve una fila abajo en el búfer de desplazamiento hacia atrás
Av Pág	Siguiente	Envía la tecla Pantalla Siguiente al host
Ctrl + Pausa	PF1	Envía la tecla PF1 al host
Ctrl + Dividir	PF2	Envía la tecla PF2 al host
Ctrl + Multiplicar	PF3	Envía la tecla PF3 al host
Ctrl + Sustraer	PF4	Envía la tecla PF4 al host
Re Pág	Anterior	Envía la tecla Pantalla Anterior al host
Suprimir	Eliminar	Envía la tecla Suprimir al host
Fin	Seleccionar	Envía la tecla Seleccionar al host
Mayús + F6...F10	UDK6...10	Envía la Tecla Definida por el Usuario 6...10 al host
Mayús + Ctrl + F1...F10	UDK11...20	Envía la Tecla Definida por el Usuario 11...20 al host

Asignación de teclado UTS

Tecla	Asignar a	Descripción
F4	Borrar Bit de Cambio	Envía la tecla CLEARCHANGEBIT al host
Teclado numérico+Intro	Retorno de Carro	Envía un retorno de carro al host
Ctrl+Av Pág.	Eliminar Final de Pantalla	Borra el texto desde la posición del cursor hasta el final de pantalla
Ctrl+Re Pág	Eliminar Final de Pantalla FCC	Borrar todos los datos (información FCC incluida) desde el cursor hasta el final de la pantalla
Ctrl+Fin	Eliminar Final de Campo	Borra el texto desde la posición del cursor hasta el final del campo
Ctrl+Mayús+Fin	Eliminar Final de Línea	Borra el texto desde la posición del cursor hasta el final de la fila
F7	Borrar FCC	Borra el carácter de control de campo
Ctrl+Inicio	Eliminar Inicio	Envía la tecla CLEAR_HOME al host
Ctrl+H	Separador de Columna Derecha	Envía la tecla COLUMN_SEP_RIGHT al host
Ctrl+F1	Página de Control	Envía la tecla CONTROL_PAGE al host
Teclado numérico 2	Cursor Abajo	Mueve el cursor una fila hacia abajo
Teclado numérico 4	Cursor Izquierda	Mueve el cursor una columna hacia la izquierda
Teclado numérico 6	Cursor Derecha	Mueve el cursor una columna hacia la derecha
Teclado numérico 8	Cursor Arriba	Mueve el cursor una fila hacia arriba
Suprimir	Borrar en Línea	Envía la tecla DELETE_IN_LINE al host
Ctrl + Supr	Borrar en Página	Envía la tecla DELETE_IN_PAGE al host
Ctrl+Mayús+Borrar	Borrar Línea	Borra la fila en la posición del cursor
Ctrl+Flecha abajo	Duplicar Línea	Duplica la fila en la posición del cursor

Tecla	Asignar a	Descripción
F8	Habilitar FCC	Habilita el carácter de control de campo
Teclado numérico+-	Final de Mostrar y Transmitir	Envía la tecla EOD_AND_TRANSMIT al host
Mayús+Fin	Final de Campo	Mueve el cursor al final de la línea
Fin	Final de Línea	Mueve el cursor al final de la fila
Ctrl+Flecha derecha	Final de Página	Mueve el cursor al final de la página
Mayús+Espacio	Borrar Carácter	Borra el carácter en la posición del cursor.
Ctrl+Mayús+E	Carácter Euro	Envía el carácter Euro al host
Ctrl+1...Ctrl+9	F1...F9	Envía la tecla F1...F9 al host.
Ctrl+0	F10	Envía la tecla F10 al host
Ctrl+-	F11	Envía la tecla F11 al host
Ctrl+=	F12	Envía la tecla F12 al host
Ctrl+Q	F13	Envía la tecla F13 al host
Ctrl+W	F14	Envía la tecla F14 al host
Ctrl+E	F15	Envía la tecla F15 al host
Ctrl+R	F16	Envía la tecla F16 al host
Ctrl+T	F17	Envía la tecla F17 al host
Ctrl+Y	F18	Envía la tecla F18 al host
Ctrl+U	F19	Envía la tecla F19 al host
Ctrl+I	F20	Envía la tecla F20 al host
Ctrl+O	F21	Envía la tecla F21 al host
Ctrl+P	F22	Envía la tecla F22 al host
Mayús+F3	FF	Envía un salto de impresión al host
F9	Generar FCC	Genera un carácter de control de campo
Inicio	Inicio	Mueve el cursor al primer campo de la pantalla

Tecla	Asignar a	Descripción
Ctrl+Mayús+Espacio	Insertar en Línea	Envía la tecla INSERT_IN_LINE al host
Ctrl+Espacio	Insertar en Página	Envía la tecla INSERT_IN_PAGE al host
Ctrl+Mayús+Insertar	Insertar línea	Inserta una nueva fila en la memoria de pantalla
Insertar	Modo de inserción	Alterna el modo de inserción de carácter
F5	Localizar FCC	Deshabilita los caracteres de control de campo y mueve al primer carácter del siguiente campo a la derecha del cursor
F3	Mensaje Esperar	Envía la tecla MESSAGE_WAIT al host
Mayús+F2	Nueva Línea	Mueve el cursor a una fila nueva.
Teclado numérico+Mayús+2	Campo Siguiente	Mueve el cursor al campo siguiente
Teclado numérico+Mayús+4	Campo Siguiente	Mueve el cursor al campo siguiente
Av Pág	Retroceder página	Envía la tecla Avance Página al host
Re Pág	Re Pág	Envía la tecla Re Pág al host
Teclado numérico+Mayús+6	Campo Anterior	Mueve el cursor al campo anterior
Teclado numérico+Mayús+8	Campo Anterior	Mueve el cursor al campo anterior
Borrar	Carácter SOE	Envía el carácter SOE al host
F12	Carácter SOE	Envía el carácter SOE al host
Ctrl+Borrar	Definir Tabulador	Envía la tecla SET_TAB al host
Ctrl+Tabulador	Definir Tabulador	Envía la tecla SET_TAB al host
Mayús+Inicio	Inicio de Campo	Mueve el cursor al principio del campo
Ctrl+Flecha izquierda	Inicio de Línea	Mueve el cursor al principio de la fila

Tecla	Asignar a	Descripción
Ctrl+[	Modo De Sistema	Envía la tecla SYSTEM_MODE al host
Ctrl+J	Alternar Separador de Columna	Alterna el separador de columna
Ctrl+F12	Alternar Pitido para Mensaje de Espera	Envía la tecla TOGGLEMSGWAITBEEP al host
Ctrl+L	Alternar Tachar	Alterna el modo tachar
Ctrl+K	Alternar Subrayar	Alterna el modo subrayar
Ctrl+Intro	Transmisión	Transmite el contenido de la pantalla al host
Bloq. despl	Transmisión	Transmite el contenido de la pantalla al host
Tecla++	Transmisión	Transmite el contenido de la pantalla al host
Teclado numérico+Ctrl+	Transmisión	Transmite el contenido de la pantalla al host
Escape	Desbloquear	Envía la tecla UNLOCK al host
Ctrl+]	Modo Estación de Trabajo	Envía la tecla WORKSTATION_MODE al host

Asignación de teclado T27

Tecla	Asignar a	Descripción
Retroceso	Retroceso	Mueve el cursor una columna hacia la izquierda
Mayús+Tabulador	TabAtrás	Mueve el cursor al campo anterior
Ctrl + Supr	Eliminar Final de Línea	Borra el texto desde la posición del cursor hasta el final de la fila
Mayús+Inicio	Borrar página Inicio	Borra la página y lleva el cursor a la posición inicial
Ctrl Izq	Página de Control	Cambia la sesión al modo Control
Flecha abajo	Cursor Abajo	Mueve el cursor una fila hacia abajo
Flecha izquierda	Cursor Izquierda	Mueve el cursor una columna hacia la izquierda
Flecha derecha	Cursor Derecha	Mueve el cursor una columna hacia la derecha
Flecha arriba	Cursor Arriba	Mueve el cursor una fila hacia arriba
Ctrl+flecha izq	Cursor Palabra Izquierda	Mueve el cursor a la palabra anterior
Ctrl+flecha der	Cursor Palabra Derecha	Mueve el cursor a la palabra siguiente
Ctrl+D	Borrar Línea	Borra la fila en la posición del cursor
Ctrl+Fin	Final de Línea	Mueve el cursor al final de la fila
Fin	Final de Página	Mueve el cursor al último campo de la página.
Mayús+Ctrl+E	Carácter Euro	Envía un carácter Euro al host
Inicio	Inicio	Mueve el cursor al primer campo de la pantalla
Insertar	Modo de inserción	

Tecla	Asignar a	Descripción
		Cambia la sesión al modo Insertar
Ctrl+I	Insertar línea	Inserta una nueva fila en la memoria de pantalla
Ctrl+1	PF1	Envía la tecla PF1 al host
Ctrl+10	PF10	Envía la tecla PF10 al host
Ctrl+2	PF2	Envía la tecla PF2 al host
Ctrl+3	PF3	Envía la tecla PF3 al host
Ctrl+4	PF4	Envía la tecla PF4 al host
Ctrl+5	PF5	Envía la tecla PF5 al host
Ctrl + 6	PF6	Envía la tecla PF6 al host
Ctrl+7	PF7	Envía la tecla PF7 al host
Ctrl+8	PF8	Envía la tecla PF8 al host
Ctrl+9	PF9	Envía la tecla PF9 al host
Av Pág	Retroceder página	Muestra la página siguiente
Re Pág	Re Pág	Muestra la página anterior
Ctrl+E	Establecer ETX	Inserta el carácter de fin de texto y lleva el cursor a la posición inicial
Teclado numérico /	Establecer Local	Cambia la sesión al modo Local
Teclado numérico *	Establecer Recibir	Cambia la sesión al modo Recibir
Introduzca	Regresar	Envía la tecla de regresar al host
Teclado numérico Intro	Regresar	Envía la tecla de regresar al host
Ctrl+A	Seleccionar todo	Selecciona todo el texto
Mayús+Flecha abajo	Seleccionar Abajo	Selecciona texto hacia abajo
Mayús+Flecha izquierda	Seleccionar Izquierda	Selecciona texto a la izquierda

Tecla	Asignar a	Descripción
Mayús+Flecha derecha	Seleccionar Derecha Selecciona texto a la derecha	
Mayús+Flecha arriba	Seleccionar Arriba	Selecciona texto hacia arriba.
Mayús+Ctrl+1	Mayús F1	Envía la tecla Mayús+F1 al host
Mayús+Ctrl+0	Mayús+F10	Envía la tecla Mayús+F10 al host
Mayús+Ctrl+2	Mayús+F2	Envía la tecla Mayús+F2 al host
Mayús+Ctrl+3	Mayús+F3	Envía la tecla Mayús+F3 al host
Mayús+Ctrl+4	Mayús+F4	Envía la tecla Mayús+F4 al host
Mayús+Ctrl+5	Mayús+F5	Envía la tecla Mayús+F5 al host
Mayús+Ctrl+6	Mayús+F6	Envía la tecla Mayús+F6 al host
Mayús+Ctrl+7	Mayús+F7	Envía la tecla Mayús+F7 al host
Mayús+Ctrl+8	Mayús+F8	Envía la tecla Mayús+F8 al host
Mayús+Ctrl+9	Mayús+F9	Envía la tecla Mayús+F9 al host
F5	Especifique	Transmite la ubicación del cursor al host
Tabulador	Tabulador	Mueve el cursor al campo siguiente
F2	Transmisión	Transmite la página al host.
Teclado numérico +	Transmisión	Transmite la página al host.
Ctrl + F2	Transmitir Línea	Transmite la fila actual al host
Teclado numérico -	Transmitir Línea	Transmite la fila actual al host

Asignación de teclado ALC

Tecla	Asignar a	Descripción
Ctrl+M	Bajar automático	Alterna la capacidad de la sesión de recibir múltiples páginas
Retroceso	Retroceso	Mueve el cursor una columna hacia la izquierda
Mayús+Tabulador	TabAtrás	Mueve el cursor al campo anterior
Ctrl+Inicio	Borrar	Borra la pantalla y envía la tecla CLEAR al host
Ctrl+B	Borrar difusión	Borra el mensaje de difusión SITA
:	Dos puntos	Inserta un carácter de dos puntos en la posición del cursor
Ctrl+L	Cruz de Lorena	Inserta el carácter de Cruz de Lorena en la posición del cursor
↓	Cursor Abajo	Baja el cursor una fila
Teclado numérico ↓	Cursor Abajo	Baja el cursor una fila
←	Cursor Izquierda	Mueve el cursor a la palabra anterior
Teclado numérico ←	Cursor Izquierda	Mueve el cursor a la palabra anterior
→	Cursor Derecha	Mueve el cursor a la palabra siguiente
Teclado numérico →	Cursor Derecha	Mueve el cursor a la palabra siguiente
↑	Cursor Arriba	Sube el cursor una fila
Teclado numérico ↑	Cursor Arriba	Sube el cursor una fila
Suprimir	Eliminar carácter	Elimina el carácter en la posición del cursor
Ctrl + Supr	Borrar Línea	Elimina la línea en la posición del cursor
=	Visualización	Inserta el carácter de visualización en la posición del cursor
Ctrl+N	Mostrar Nueva línea	Inserta el carácter de visualización en una nueva línea
]	Dólar	Inserta el carácter del signo del dólar USA en la posición del cursor

Tecla	Asignar a	Descripción
.	Elemento final	Inserta el carácter de elemento final en la posición del cursor
Fin	Final de Línea	Mueve el cursor al final de la línea
Ctrl+T	Transacción final	Cierra el PNR
Ctrl+E	Borrar Final de Pantalla	Borra todos los datos desde la posición del cursor hasta el final de la pantalla
Ctrl+Fin	Borrar Final de línea	Borra todos los datos desde la posición del cursor hasta el final de la línea
Inicio	Inicio	Mueve el cursor al primer campo sin protección de la pantalla
Ctrl+I	Ignorar	Cancela todos los cambios realizados en el PNR actual
Ctrl + Insertar	Insertar Línea	Inserta una nueva línea en la memoria de pantalla
Insertar	Insertar Espacio	Inserta un espacio en la memoria de pantalla
\	Nueva Línea	Inserta el carácter de nueva línea en la posición del cursor
[	Almohadilla	Inserta el carácter de almohadilla en la posición del cursor
Ctrl+G	Libra	Inserta un carácter de libra esterlina en la posición del cursor
Ctrl+Intro	Imprimir Intro	Envía la respuesta a la impresora
Ctrl+P	Reset protegido	Mueve el cursor al primer campo no protegido
Ctrl+↑	Recordar entrada siguiente	Recuerda la entrada siguiente
Ctrl+↓	Recordar entrada anterior	Recuerda la entrada anterior
Ctrl+Z	Reintroducir	Reenvía al host el mensaje enviado previamente

Tecla	Asignar a	Descripción
Ctrl+R	Repita el	Muestra de nuevo el último mensaje enviado por el host
Escape	Reset	Resetea las condiciones de error del teclado
Mayús+Ctrl+↓	Recorrer línea hacia abajo	Baja la visualización una línea
Mayús+Ctrl+↑	Recorrer línea hacia arriba	Sube la visualización una línea
Av Pág	Recorrer página hacia abajo	Baja la visualización una página
Re Pág	Recorrer página hacia arriba	Sube la visualización una página
Ctrl+A	Seleccionar todo	Selecciona todo el texto
Mayús+↓	Seleccionar Abajo	Selecciona todo el texto hacia abajo
Mayús+↑	Seleccionar Arriba	Selecciona todo el texto hacia arriba
Mayús+←	Seleccionar Izquierda	Selecciona todo el texto hacia la izquierda
Mayús+→	Seleccionar Derecha	Selecciona todo el texto hacia la derecha
‘	Inicio del mensaje	Inserta un carácter de inicio de mensaje en la posición del cursor
F12	Estadísticas	Muestra las estadísticas de comunicación
Tabulador	Tabulador	Mueve el cursor al siguiente campo no protegido
Ctrl+F	Alternar CODACOM	Alterna el modo CODACOM
Introduzca	Transmisión	Transmite página al host
Teclado numérico Intro	Transmisión	Transmite página al host
Mayús + Intro	Transmisión	Transmite página al host

Tecla	Asignar a	Descripción
Mayús+Escape	Desbloquear teclado	Desbloquea el teclado
Ctrl+U	Mensaje no solicitado	Recupera un mensaje no solicitado del host

5.4 Transferir archivos

Host Access for the Cloud admite tres protocolos de transferencia de archivos diferentes:

- IND$FILE para transferencias de host 3270
- AS/400 para transferencias de host 5250
- Protocolo de transferencia de archivos (FTP), que permite que un equipo local actúe como cliente FTP.

Una vez que se haya conectado, puede visualizar archivos en el servidor y utilizar FTP para transferir archivos entre su computadora local (o cualquier unidad de la red) y el servidor FTP.

La transferencia de archivos en lote está disponible para transferencias FTP. Con esta opción puede descargar y cargar múltiples archivos en una operación.

Antes de poder transferir o enviar archivos, el administrador debe habilitar las opciones de transferencia y envío para la sesión actual y realizar las configuraciones necesarias. Esto se realiza en el panel de configuración Transferencia de Archivo.

Dependiendo del sistema del archivo del host y del método de transferencia que desee utilizar, podrá ver distintas opciones de configuración. Una vez configurado, el cuadro de diálogo de transferencia de archivos está accesible desde la barra de herramientas.

- IND$FILE
- AS/400
- FTP
- Transferencias por lotes

5.4.1 IND$FILE

IND$FILE es un programa de transferencia de archivos de IBM que se puede utilizar para transferir información entre su computadora y una computadora host 3270.

Desde la lista desplegable Sistema de Archivos de Host, seleccione en qué entorno operativo IBM 3270 se está ejecutando el host. Host Access for the Cloud admite TSO (opción para compartir la hora), CMS (sistema de supervisión conversacional) y CICS. La selección predeterminada es Ninguno.

Hay soporte para transferencias ASCII o binarias y, si está conectado a un host TSO, puede navegar directamente a un conjunto de datos TSO particular.

Opciones generales para tipos de archivo de host CICS, CMS y TSO

Mostrar archivos de host automáticamente - De forma predeterminada, la lista de archivos de host contiene todos los archivos de host disponibles para transferir. Para recuperar archivos de host

solo cuando los solicite, desactive esta opción. En el cuadro de diálogo Transferir, haga clic en Mostrar archivos de host para recuperar los archivos de host.

Opciones de transferencia para tipos de archivo de host CICS, CMS y TSO

Opción	Descripción
Método de transferencia	• Binario: utilice este modo para archivos de programa y otros tipos de archivos que no deben convertirse, como los que ya se han formateado para un determinado tipo de impresora o los que poseen un formato específico de la aplicación. Los archivos binarios contienen caracteres que no se pueden imprimir; con este método, el archivo no se convierte durante la transferencia. • ASCII : utilice este método para transferir archivos de texto que no tienen un formato especial. Los archivos ASCII de la PC se traducen al juego de caracteres EBCDIC en el host y los archivos de texto del host se convierten de EBCDIC a ASCII cuando se han descargado.
Procesamiento de CR/LF	Si esta opción está seleccionada, los pares de salto de línea de retorno de carro se eliminarán de los archivos enviados al host y se agregarán al final de cada línea en los archivos recibidos desde el host.
Comando de inicio	Especifica el programa de host utilizado para iniciar la transferencia de archivos. IND$File, el predeterminado, es adecuado para hosts CMS y TSO. En los hosts CICS, puede utilizarse IND$File o quizás deba especificar la transacción CICS de su sitio (por ejemplo, CFTR).
Parámetros de inicio	Utilice este campo para los parámetros específicos del programa IND$File de su sistema de host. El contenido de este campo se añade al final del comando de transferencia generado por Host Access for the Cloud. Host Access for the Cloud no valida los parámetros.
Máx. tamaño de campo	Seleccione un tamaño de campo para utilizar con el protocolo Write Structured Field. El valor por defecto es de 4 kilobytes. Normalmente, cuanto mayor es el tamaño de búfer, mayor será la velocidad de transferencia. La mayoría de los sistemas soportan 8K, si selecciona un valor demasiado grande para el host, se desconectará la sesión cuando intente enviar un archivo lo suficientemente grande como para llenar el búfer. La persona que instala el software de comunicación del host suele proporcionar este valor. Por ejemplo, el producto TCP/IP del host IBM obtiene este valor del parámetro DATABUFFERPOOLSIZE, que es el valor por defecto para búfers de 8K. Consulte a su administrador del sistema si no sabe qué introducir aquí.
Clave principal	Puede especificar ciertas acciones antes de transferir o listar archivos. Puede elegir entre Ninguna, Auto detección y Borrar. Si se ajusta Ninguna, LISTCAT se emite automáticamente. Si se ajusta

	Auto detección, los contenidos actuales de la pantalla se examinan para determinar si se debe enviar una LISTCAT o TSO LISTCAT. Si se ajusta Borrar, se envía la tecla Borrar antes de emitir el comando. Para TSO, Borrar significa también que "TSO" no se antepondrá al comando de archivos de solicitud.
Página de códigos de PC	El juego de caracteres a utilizar cuando se leen o escriben archivos locales durante una transferencia de archivos. El valor **Predeterminado** utiliza la página de códigos correspondiente a su sistema operativo local. Si necesita un juego de caracteres distinto para especificar la página de códigos de PC, selecciónelo de la lista.
Página de códigos del host	El juego de caracteres a utilizar cuando se traducen caracteres EBCDIC durante la trasferencia de archivos al host o desde él. El predeterminado, **Utilizar configuración NCS**, utiliza el juego de caracteres nacional especificado en el panel Visualización en Terminal. Si necesita un juego de caracteres distinto para especificar la página de códigos del host, selecciónelo de la lista.
Tiempo de espera de respuesta (segundos)	Especifica cuántos segundos debe esperar Host Access for the Cloud una respuesta del host antes de que se agote el tiempo de espera y devuelva un error. El valor por defecto es 60 segundos.
Tiempo de espera de inicio (segundos)	Especifica el número de segundos que debe esperar Host Access for the Cloud una respuesta del host cuando intenta conectarse a un host. Si finaliza la cantidad de tiempo especificada sin respuesta del host, se agota el tiempo de espera y Host Access for the Cloud devuelve un error. El valor por defecto es 25 segundos.

Opciones de envío para tipos de archivo de host CICS, CMS y TSO

Opción	Descripción	Se aplica a este tipo de host
Formato de registro	Utilice esta opción para especificar el formato de registro para los archivos enviados al host. • Predeterminado - El host determina el formato de registro. Ésta es la opción predeterminada. • Fijo - Hacer que el host cree registros de longitud fija. • Indefinido - Hacer que el host cree archivos sin un formato de registro específico (este valor sólo es para sistemas TSO). • Variable - Hacer que el host cree registros de longitud variable y mantenga el formato de un archivo binario.	TSO, CMS
Unidades de asignación	Especifica las subdivisiones de disco para las asignaciones de espacio primario y secundario. Si selecciona Predeterminado (opción predeterminada), el host determinará la unidad. También puede seleccionar Cilindro, Pista o Bloque. Si selecciona Bloque, utilice el cuadro Bloque promedio para definir el tamaño de un bloque promedio (en bytes).	TSO
Longitud de registro	El tamaño de registro (en bytes) del archivo que está creando en el host. Si se deja en blanco este cuadro, el host determinará el tamaño de registro. Puede ajustar cualquier valor entre 0 y 32767 para acomodar cualquier rango aceptado por su host. Esta opción no está disponible en hosts CICS. Para los archivos ASCII, defina este valor para que quepa la línea de mayor tamaño del archivo. Cuando se deja en blanco este cuadro, el host acepta generalmente líneas de hasta 80 caracteres.	TSO, CMS
Si existe archivo de host		TSO, CMS

	Especifica cómo debe operar la transferencia si ya existe un archivo con el mismo nombre. • Añadir - Añade el contenido del archivo local al archivo de host existente. • Sobrescribir - Sobrescribe el contenido del archivo de host Con los sistemas CICS no hay forma de decir si un archivo de host ya existe, por lo que Sobrescribir es la única opción disponible para enviar archivos a un sistema CICS.	
Tamaño de bloque (bytes)	En los hosts TSO especifica el tamaño de bloque para el archivo que se está creando en el host. Para los archivos con registros de longitud fija, este valor debe ser un múltiplo de la Longitud de registro, ya que los bloques están divididos en registros lógicos. Puede ajustar cualquier valor entre 0 y 32767 para acomodar cualquier rango aceptado por su host.	TSO
Bloque promedio (bytes)	Tamaño de un bloque promedio. Este valor sólo es relevante si se utilizan bloques como unidad de asignación.	TSO
Asignación primaria (unidades de asignación)	Tamaño de la asignación primaria para el archivo de host que se está creando.	TSO
Asignación secundaria (unidades de asignación)	Tamaño de cualquier asignación adicional en caso de que la asignación primaria no sea suficiente. Se pueden especificar varias asignaciones secundarias (denominadas "extensiones") hasta el límite especificado por el host (generalmente 15).	TSO

Nota

Cuando se utiliza CICS como el sistema de host, debe introducir manualmente los nombres de los archivos que está transfiriendo. No se dispone de una lista de archivos en la que elegir.

Transferencia de archivos (IND$FILE)

Debe estar conectado al host y haber iniciado sesión en él para transferir archivos para la sesión 3270 actual.

1. Verifique que el host está en estado 'ready' para aceptar el comando IND$FILE.
2. En la barra de herramientas, haga clic en el icono  .
3. En el cuadro de diálogo Transferencia de archivos, se muestra una lista de archivos y directorios del host que se pueden transferir. Los directorios y los archivos se indican mediante un icono cuando usted selecciona el archivo. Para los hosts CICS, introduzca los nombres de los archivos que desea transferir.
4. Seleccione el método de transferencia. Las opciones son:

   - Binario

     Utilice este modo para archivos de programa y otros tipos de archivos que no deben convertirse, como los que ya se han formateado para un determinado tipo de impresora o los que poseen un formato específico de la aplicación. Los archivos binarios contienen caracteres que no se pueden imprimir; con este método, el archivo no se convierte durante la transferencia.

   - ASCII

     Utilice este método para transferir archivos de texto que no tienen un formato especial. Los archivos ASCII de la PC se traducen al juego de caracteres EBCDIC en el host y los archivos de texto del host se convierten de EBCDIC a ASCII cuando se han descargado.

5. Si está conectado a un host TSO, haga clic en Nivel para especificar el conjunto de datos que desea ver. Host Access for the Cloud actualiza la lista de archivos remotos mediante el nivel de conjunto de datos que especifique.

> **Nota**
>
> Cuando se especifican archivos mediante *Cargar como* o *Descargar*, es necesario encerrar entre comillas simples un nombre completo de conjunto de datos. Los nombres de conjuntos de datos no encerrados entre comillas simples se prefijarán, de forma predeterminada, con un calificador de alto nivel especificado en el PERFIL TSO.

Puede actualizar la lista de archivos en todo momento haciendo clic en el icono Actualizar de la esquina superior izquierda del cuadro de diálogo Transferencia de Archivos.

- Descarga de archivos (IND$FILE)
- Carga de archivos (IND$FILE)
- Solución de problemas de sus transferencias de archivos

Descarga de archivos (IND$FILE)

1. En la lista, haga clic en el nombre del archivo para iniciar la transferencia.

   o bien

   Haga clic en **Descargar** e introduzca el nombre del archivo del host que desea transferir. Puede descargar de tipos de host TSO y CMS. Sin embargo, TSO y CMS representan los archivos de host de forma distinta; esto significa que el formato del nombre de archivo que usted introduce en el mensaje que aparece variará.

   - **TSO** - Encierra el nombre de la ruta del host entre comillas simples para especificar el nombre completo del conjunto de datos. Por ejemplo, `'BVTST03.DATA.TXT'`. Para especificar una ubicación de archivo relativa al nivel del conjunto de datos que estableció anteriormente, omita las comillas simples. Por ejemplo, `DATA.TXT`, que identifica el mismo conjunto de datos pero relativo a `BVTST03`.
   - **CMS** - Una entrada CMS típica sería `BVTSTT01 DATA A1`. No se necesitan comillas simples.
2. De ser necesario, puede cancelar la transferencia desde el panel de progreso de la transferencia.

Carga de archivos (IND$FILE)

> **Nota**
>
> Los sistemas de equipos mainframe IBM imponen ciertas convenciones de nomenclatura para los archivos. Para obtener información detallada sobre los requisitos de nomenclatura, consulte la Documentación de IBM.

Elija cualquiera de los métodos para cargar archivos:

- En el cuadro de diálogo **Transferencia de archivos**, haga clic en **Cargar**.

  Puede especificar un nombre diferente para el archivo cargado. Haga clic en Cargar como, navegue hasta el archivo que desea cargar y, cuando se le pida, escriba el nombre que desea utilizar. Recuerde que estando conectado a un host TSO, es necesario encerrar entre comillas simples un nombre de conjunto de datos completamente cualificado. Consulte el paso 5 en Transferencia de archivos.

  o bien

- Arrastre el archivo que desea cargar desde esta ubicación al cuadro de diálogo **Transferencia de archivos**. Haga clic en **Actualizar** para verificar que el archivo se ha actualizado correctamente.

Si cancela el proceso de carga antes de que un archivo se haya terminado de cargar, un archivo parcial se deja en el host.

Solución de problemas de sus transferencias de archivos

Ocasionalmente puede encontrar errores cuando intente realizar una transferencia de archivos. Estos errores pueden ser problemas de mainframe o pueden estar causados por la configuración de seguridad del navegador.

- Si la transferencia se completa pero el archivo no contiene los datos esperados, compruebe si el método de transferencia está correctamente ajustado a Binario o ASCII.
- Existe un límite de tamaño de archivo de 50 MB para las operaciones de carga de transferencia de archivos. Puede modificar este valor.
- Para obtener información sobre los errores específicos del host, consulte Mensajes de Error de Transferencia de Archivos IBM.

5.4.2 AS/400

Con la transferencia de archivos AS/400, puede transferir datos entre el equipo y un host iSeries.

Por lo general, las transferencias de archivos AS/400 son sencillas y no complejas. No obstante, dado que los datos del host se gestionan como una base de datos DB2, puede utilizar el Editor de SQL para crear consultas bastante complejas.

Para configurar la transferencia de archivos AS/400

1. Cree una sesión de terminal 5250 de HACloud, introduzca una dirección o un nombre de host y, a continuación, asigne un nombre a la sesión.
2. En el panel de configuración, seleccione Transferencia de archivos.
3. Seleccione Habilitar transferencia de archivos AS/400 y continúe con la configuración.

   - **Host**

     La dirección de host que ha proporcionado para la sesión de terminal se rellena previamente en el campo de host. Si es necesario, puede utilizar un host distinto. Para especificar un puerto distinto, añada el número de puerto a la dirección del host. Por ejemplo, host.mycompany.com:23.

   - **Seguridad TLS**

     En la lista desplegable, seleccione la opción de seguridad TLS que desee utilizar.

     Para utilizar esta opción: el certificado del servidor de base de datos AS/400 debe añadirse a la lista de certificados de confianza de MSS. Si aún no se ha añadido el certificado, consulte Trusted Certificates (Certificados de confianza) en la documentación de MSS para obtener instrucciones.

   - **Método de transferencia predeterminado**

     Defina el método de transferencia predeterminado preferido: Texto de anchura fija o Valores separados por comas (CSV). El método de transferencia se puede modificar al realizar una transferencia.

   - **Incluir encabezados de columna por defecto**

     Seleccione esta opción para incluir los encabezados de columna por defecto para todos los datos descargados. Puede modificar este parámetro en cada descarga del cuadro de diálogo Transferencia de archivos.

     Los encabezados de columna no se originan en el archivo de host, pero se añaden al descargar un archivo. Se eliminan automáticamente cuando se carga un archivo.

4. Haga clic en **Guardar** y conéctese a la sesión.

Transferencia de archivos (AS/400)

Una vez que haya configurado la sesión para utilizar la función de transferencia de archivos AS/400, haga clic en  en la barra de herramientas para abrir el cuadro de diálogo **Transferencia**

de archivos. Este cuadro de diálogo contiene una lista de los archivos de host que se pueden transferir. Si se le solicita, escriba la credenciales de entrada de AS/400.

- Descarga de archivos (AS/400)
- Descargar mediante SQL
- Carga de archivos (AS/400)
- Añadir una biblioteca

DESCARGA DE ARCHIVOS (AS/400)

El sistema de archivos AS/400 está formado por bibliotecas, archivos y miembros. Las bibliotecas se identifican mediante este icono: . Aunque no puede descargar bibliotecas, puede hacer clic en la biblioteca para ver los archivos y los miembros incluidos en ella.

Seleccione **Incluir encabezados de columna** para visualizar los encabezados de columna de los datos descargados.

1. Abra la biblioteca que contiene los archivos ( ).
2. Expanda el archivo que contiene el miembro que desea descargar.
3. Para descargar un miembro, haga clic en él.
4. Abra la carpeta de descarga del navegador para confirmar que el archivo se encuentra en esa ubicación. Abra el archivo en un editor de textos.

DESCARGAR MEDIANTE SQL

Puede crear consultas SQL para obtener solo los datos que necesita de un miembro de archivo en el host. Esto le permite seleccionar campos específicos y omitir otros.

1. Abra la biblioteca y el archivo que desea descargar.
2. Abra el menú de opciones y haga clic en **SQL**.

3. Se abre el Editor de SQL, que contiene la instrucción SELECT que permite descargar el miembro completo. Se hace referencia al miembro de archivo como NOMBREBIBLIOTECA/NOMBREARCHIVO(NOMBREMIEMBRO).
4. Haga clic en **Ejecutar** para descargar el miembro completo. O bien, edite el SQL y haga clic en Ejecutar para recuperar un subconjunto de los datos.

CARGA DE ARCHIVOS (AS400)

Solo se pueden cargar datos en archivos como miembros nuevos o de sustitución. El archivo AS/400 contiene una especificación que describe los datos de los miembros; cada miembro de un archivo especificado presenta la misma estructura. Por lo general, no se puede (o no se debe) descargar un miembro de un archivo y cargarlo en otro, a menos que ambos archivos tengan la misma especificación de datos.

Debido a que los datos solo se pueden cargar como miembros, debe abrir un archivo y visualizar sus miembros en el cuadro de diálogo de lista de archivos antes de habilitar el botón Cargar.

1. Abra el archivo en el que desee cargar. El botón Cargar está disponible ahora.
2. Realice una de las acciones siguientes:

   Haga clic en el botón **Cargar** y seleccione un archivo del sistema de archivos local que desee cargar.

   o bien

   Haga clic en la flecha hacia abajo del botón Cargar, seleccione **Cargar como...**, elija el archivo, asígnele un nuevo nombre y, a continuación, haga clic en Aceptar.

ADICIÓN DE UNA BIBLIOTECA

Por lo general, como usuario de AS/400, tendrá acceso a un determinado conjunto de bibliotecas que le haya asignado el administrador del sistema. Estas bibliotecas aparecen como entradas de nivel superior en el cuadro de diálogo de transferencia de archivos. Si necesita acceder a una biblioteca que no aparezca en la lista, el administrador del sistema puede actualizar la configuración para que la nueva biblioteca se añada a ella. En ocasiones, es posible que deba trabajar con una biblioteca de forma temporal; no es necesario que se añada de forma permanente a la lista de bibliotecas.

Para añadir una biblioteca

En el cuadro de diálogo de transferencia de archivos AS/400, haga clic en **Añadir biblioteca**. Este botón está disponible en el panel de lista de bibliotecas. Esta adición no es permanente y deberá añadir de nuevo la biblioteca si cierra y vuelve a abrir el cuadro de diálogo de transferencia de archivos.

5.4.3 FTP

Con Host Access for the Cloud, el equipo local puede actuar como un cliente FTP. Mediante el cliente FTP, puede conectarse a un servidor FTP que se esté ejecutando en otro equipo. Una vez que se haya conectado, puede visualizar archivos en el servidor y utilizar FTP para transferir archivos entre su computadora local (o cualquier unidad de la red) y el servidor FTP. Utilizando FTP, un cliente puede cargar, descargar, eliminar, cambiar de nombre, mover y copiar archivos en un servidor, bien individualmente, bien en lote, donde usted puede crear listas de archivos para transferir en una sola operación.

Sugerencia

Si tiene intención de utilizar una transferencia por lotes, seleccione y configure primero la opción Habilitar FTP.

Para configurar FTP

Seleccione Habilitar FTP y proceda con la configuración:

- **Protocolo**

  Utilizar FTP para iniciar una sesión FTP estándar. Utilizar SFTP para iniciar una sesión SFTP.

  Puede configurar un cliente FTP para utilizar el protocolo SFTP y realizar todas las operaciones mediante un transporte secure shell cifrado. Host Access for the Cloud utiliza el nombre de usuario y la contraseña para autenticarse.

- **Host**

  Especifique el nombre de host o la dirección IP del servidor FTP al que desea conectarse.

- **Puerto**

  El puerto del servidor FTP especificado.

- **Si el archivo remoto existe al cargar el archivo**

  Especifique cómo tratar la transferencia si ya existe un archivo con el mismo nombre.

Seleccione esta opción	Para...
Añadir	Añadir el archivo que se está enviando al archivo existente
Preguntar al usuario (predeterminado)	Solicita una decisión sobre cómo manejar el nombre del archivo duplicado
Cancelar	Cancelar la transferencia de archivos
Error	Cancelar la transferencia de archivos y recibir una notificación del error
Sobrescribir	Sobrescribir el archivo existente en la máquina remota
Omitir	Cuando una solicitud incluye múltiples archivos, omite el archivo que tiene el mismo nombre que un archivo existente, pero procede con la transferencia de los otros archivos.
Único	Crear un archivo nuevo con un nombre de archivo único

- **Directorio remoto inicial**

  Especificar la ruta a un directorio principal o predeterminado para el sitio FTP. Cuando se abre una conexión con el sitio FTP, el directorio de trabajo del servidor se establece automáticamente a la ruta principal especificada. Los archivos y las carpetas en el directorio principal del servidor aparecen en la ventana de sesión FTP. Si no se puede encontrar el directorio remoto inicial, se emite una advertencia y la conexión continúa.

- **Usuario anónimo**

Seleccione esta opción para iniciar sesión en el servidor FTP especificado con el nombre de usuario "Anónimo". Si el host al que se está conectando no soporta usuarios anónimos, puede ser necesario especificar sus credenciales.

- **Tiempo de espera de sesión (segundos)**

  Este valor informa al cliente FTP del número máximo de segundos de espera para los paquetes de datos que se están transfiriendo desde o hacia el host. Si no se recibe ningún dato al cabo del intervalo de tiempo especificado, se mostrará un mensaje de error de tiempo agotado y se cancelará la transferencia; en este caso, intente la operación de nuevo. Si recibe errores de tiempo de espera repetidamente, aumente el valor de tiempo de espera. Especifique 0 (cero) en este cuadro para evitar que el cliente FTP agote el tiempo de espera a una respuesta. Para las sesiones SFTP, el valor predeterminado es 0 (cero).

- **Tiempo de Keep Alive (segundos)**

  Seleccione esta opción e introduzca un tiempo en segundos si desea continuar su conexión al servidor después de trascurrido el tiempo de espera automático del servidor por inactividad. La mayoría de los servidores tienen un valor de tiempo inactividad que especifica el tiempo de espera de una sesión FTP antes de desconectarse cuando no se detecta ninguna actividad. Cuando el usuario supera el límite de tiempo definido, la conexión del servidor se cierra.

  Esta configuración permite indicar al cliente FTP que envíe un comando NOOP al servidor a intervalos periódicos para evitar que el servidor cierre la conexión por falta de actividad. Recuerde que al continuar su sesión debe prevenir a otros de usuarios de establecer una conexión con el servidor FTP.

- **Codificación de host**

  Especifica el juego de caracteres utilizado por el host para mostrar los nombres de los archivos que se transfieren. Por defecto, Host Access for the Cloud utiliza UTF-8 (Unicode). Si usted transfiere archivos con la configuración predeterminada y los nombres de archivo son irreconocibles, cambie la opción de codificación del host al juego de caracteres utilizado por el host. (Esta opción no afecta a la codificación de los contenidos de los archivos que se transfieren; se aplica sólo a los nombres de archivo).

Transferencia de archivos (FTP)

Después de que el administrador configure una sesión para incluir la funcionalidad FTP, haga clic en  en la barra de herramientas para abrir la ventana Transferencia de archivos FTP que

contiene una lista de archivos de host que se pueden transferir. Los directorios y los archivos se indican mediante un icono cuando usted selecciona el archivo.

1. Seleccione el método de transferencia. Las opciones son:

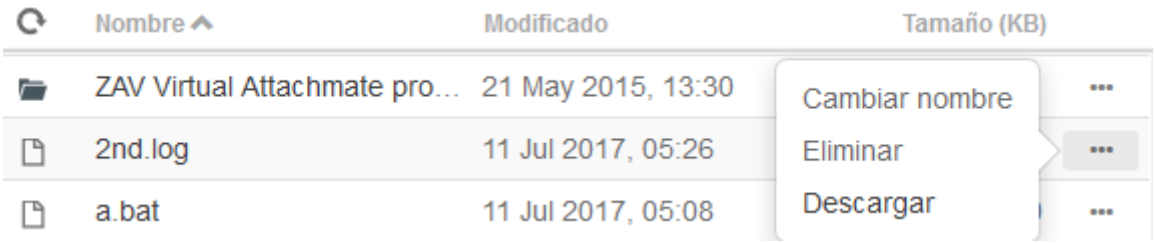
   - Binario

     Utilice este modo para archivos de programa y otros tipos de archivos que no deben convertirse, como los que ya se han formateado para un determinado tipo de impresora o los que poseen un formato específico de la aplicación. Los archivos binarios contienen caracteres que no se pueden imprimir; con este método, el archivo no se convierte durante la transferencia.

   - ASCII

     Utilice este método para transferir archivos de texto que no tienen un formato especial. Los archivos ASCII de la PC se traducen al juego de caracteres EBCDIC en el host y los archivos de texto del host se convierten de EBCDIC a ASCII cuando se han descargado.

2. Puede cambiar de nombre, eliminar o descargar un archivo de la lista de archivos.



3. Actualice la lista de archivos en todo momento haciendo clic en el icono Actualizar de la esquina superior izquierda del cuadro de diálogo Transferencia de Archivos.

Descarga de archivos (FTP)

1. En la lista, seleccione el archivo para iniciar la transferencia.
2. De ser necesario, puede cancelar la transferencia desde el panel de progreso de la transferencia.

Carga de archivos (FTP)

Elija cualquiera de los métodos para cargar archivos:

- En el cuadro de diálogo **Transferencia de archivos**, haga clic en **Cargar**.

  Seleccione el archivo que desea cargar en la ventana Examinar.

  O bien

- Arrastre el archivo que desea cargar desde esta ubicación al cuadro de diálogo **Transferencia de archivos**.

  Haga clic en **Actualizar** para verificar que el archivo se ha actualizado correctamente.

Haga clic en **Nuevo directorio** para crear un directorio nuevo en el servidor remoto. Se le pedirá introducir un nuevo nombre de directorio.

5.4.4 Transferencias por lotes

> **Nota**
>
> Primero debe habilitar FTP en el panel Configuración de transferencia de archivos de la pestaña FTP para poder configurar transferencias en lote.

Para transferir múltiples archivos en una operación, utilice la opción **Lote**.

1. Desde el panel Configuración > Transferencia de archivos > FTP, marque **Habilitar FTP**.
2. Haga clic en FTP **BATCH** para abrir el panel de transferencia de archivos por lotes.
3. Seleccione Cancelar lote cuando se produzca un error individual para detener la transferencia si se produce un fallo en la transferencia de un archivo.
4. Haga clic en  para crear la lista de archivos que desea transferir.

   a. Asigne un nombre a la lista. Para ayudar a crear listas similares, puede copiar una lista existente, cambiarle el nombre y, a continuación, agregar o eliminar archivos según sea necesario utilizando las opciones disponibles cuando se resalta la lista original.

   b. En el panel derecho, haga clic en  para abrir el cuadro de diálogo Añadir solicitud de transferencia.
5. En el panel Añadir solicitud de transferencia, empiece a crear la lista:

Opción	Descripción
Transferencias	Seleccione si desea cargar o descargar el archivo.
Nombre de archivo local	Identifique el archivo que desea transferir. Puede introducir el nombre del archivo o navegar hasta él.
Ruta de archivo remoto	Indique una ubicación para nombrar y guardar el archivo después de la transferencia. Puede: • **Conservar el nombre de archivo y utilizar el directorio remoto inicial** - deje el espacio en blanco • **Utilizar un nuevo nombre de archivo** - introduzca nuevonombredearchivo.txt. Guarda el archivo en el directorio remoto inicial utilizando el nombre dado. • **Conservar el nombre de archivo original pero utilizar una nueva ruta de directorio** - `/carpeta/`. Utiliza el nombre de archivo original con la nueva ruta. • **Utilizar un directorio nuevo y un nombre de archivo nuevo** - `/carpeta/nuevonombredearchivo.txt`.
Método de transferencia	Puede elegir entre métodos de transferencia binaria o ASCII.
Si existe archivo remoto	Especifique cómo tratar la transferencia de archivos si ya existe un archivo remoto. Las opciones son: • Sobrescribir (predeterminado) - Sobrescribir el archivo existente en la máquina remota • Añadir - Añadir el archivo que está siendo enviado al archivo existente • Preguntar al usuario - Solicitar una decisión sobre cómo manejar el nombre del archivo duplicado • Cancelar - Cancelar la transferencia de archivos • Fallo - Cancelar la transferencia de archivos y enviar una notificación del fallo • Omitir - Omitir el archivo que tiene el mismo nombre que un archivo existente, pero procede con la transferencia de los otros archivos del lote • Único - Crear un archivo nuevo con un nombre de archivo único

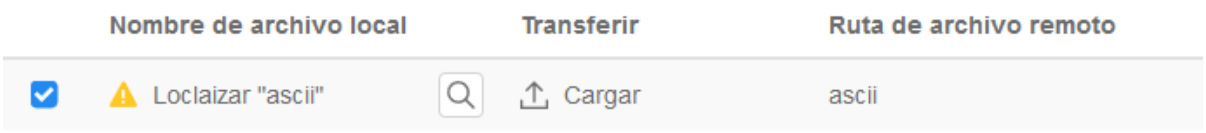
1. Haga clic en **Save** (Guardar).

Transferencia de archivos (Lote)

> **Sugerencia**
>
> Los administradores conceden permiso para transferir archivos mediante la opción **Reglas de Preferencias de Usuario** del panel Configuración.

Haga clic en  en la barra de herramientas para abrir la lista que contiene los archivos que desea transferir.

1. Debido a los requerimientos del navegador, tiene que especificar la ubicación de todos los archivos que desea cargar. Localice los archivos necesarios utilizando el icono Buscar. Estos archivos se identifican fácilmente con un icono amarillo como éste:



2. Los archivos del lote están seleccionados por defecto. Para editar el archivo antes de la transferencia, puede eliminar archivos de la operación de transferencia desactivando sus respectivas casillas de verificación o seleccionando **Todos** en el menú desplegable. También puede filtrar la lista de archivos transferibles en función de su estado de descarga o de carga.
3. Haga clic en **Iniciar** para iniciar la transferencia.

5.5 Especificar las opciones de edición

Las opciones de edición se utilizarán para las diferentes operaciones de copiar, pegar y cortar.

Opciones de copia

Seleccione el texto. Para ello, haga clic con el botón izquierdo y arrastre con el ratón o mantenga pulsada la tecla Mayús mientras modifica la selección con las teclas de flecha. Por defecto, los diferentes tipos de terminales utilizan diferentes modos de selección al copiar texto. Los terminales VT utilizan un modo de selección lineal, mientras que todos los demás utilizan la selección de modo de bloque. Para alternar entre los modos de selección en bloque y lineal, pulse y mantenga pulsada la tecla **Alt** cuando seleccione el texto.

- Copiar solo los campos de entrada -. Seleccione esta opción para copiar datos sólo de campos de entrada. Los datos de los campos protegidos son sustituidos por espacios en blanco cuando se llevan al portapapeles.
- Utilizar la pantalla completa cuando no haya selección - Esta opción aplica el comando Copiar a toda la pantalla del terminal cuando no hay nada seleccionado.

Opciones de pegado

Seleccione Pegar para pegar el contenido del portapapeles en la posición del cursor.

- **Omitir campos protegidos**: especifica cómo se asigna el texto pegado en la pantalla:
  - Si la opción no está seleccionada (valor por defecto), el texto se interpreta como una secuencia lineal que puede contener líneas y delimitadores nuevos y se pega según corresponda.
  - Si se selecciona esta opción, el texto se interpreta como un dato en la pantalla del host y se superpone en la pantalla activa desde la posición actual del cursor. Si la pantalla actual contiene un campo sin proteger, se pega el texto de origen; si la pantalla actual contiene un campo protegido, se omite el texto de origen.
- **Ajustar al campo siguiente en la línea actual**: seleccione esta opción para que los datos pegados desde el portapapeles rellenen la mayor parte posible del campo actual. Los datos restantes se pegarán en el siguiente campo de la misma fila hasta que se llegue al final de la fila o se hayan agotado los datos. Si también se selecciona **Ajustar a la siguiente línea**, los datos adicionales se pegarán en los campos posteriores de la fila siguiente y los datos se alinearán verticalmente con la posición inicial del cursor.
- **Ajustar a la siguiente línea**: si se selecciona, el comando Pegar rellena el primer campo con tantos datos del portapapeles como pueda contener el campo. Todo el texto restante se pegará en la línea justo debajo, siempre que permita su escritura (por ejemplo, un campo de entrada). De lo contrario, se trunca el texto restante. Las líneas de datos siguientes se pegan para alinearse verticalmente con la posición inicial del cursor.

  Por defecto, esta opción no está seleccionada y se trunca el texto que desborda el campo.
- **Restaurar la posición inicial del cursor después de pegar**: por defecto, el cursor del host se encuentra al final de los datos después de una operación de pegado. Seleccione esta opción para restablecer el cursor del host a su posición inicial después de haber completado la operación de pegado.

Opciones de corte

La operación Cortar está disponible para todos los terminales compatibles, excepto para los tipos de host VT. Seleccione el área que desea cortar y haga clic en el botón  de la barra de herramientas. Puede utilizar el menú contextual o la combinación de teclas para cortar los datos de la pantalla y guardarlos en el portapapeles. Los datos de los campos protegidos se copian en el portapapeles, pero no se eliminan de la pantalla.

Combinaciones de teclas

En HACloud, se admiten las combinaciones de teclas utilizadas habitualmente para las funciones de edición. Estas claves se transfieren a través del navegador, que genera las funciones de edición adecuadas.

Combinación de teclas	Tipo de host	Acción
Ctrl + C	3270, 5250, UTS, T27 y ALC	Copiar
Ctrl + V	3270, 5250, UTS, T27 y ALC	Pegar
Ctrl+X	3270, 5250, UTS, T27 y ALC	Cortar

Estas combinaciones de teclas se asignan en HACloud a varias acciones de edición de pantalla:

Combinación de teclas	Tipo de host	Acción
Ctrl + A	3270, 5250, UTS, T27 y ALC	Seleccionar todo el texto de la pantalla
Mayús + Tecla de flecha	Todas	Cambia la extensión de la selección actual
Ctrl + Mayús + A	VT	Seleccionar todo
Ctrl + Mayús + C	VT	Copiar
Ctrl + Mayús + V	VT	Pegar

Nota

En HACloud, puede utilizar el asignador de teclas para asignar acciones de edición a combinaciones de teclas. Puede acceder a las acciones de edición mediante un menú contextual en el terminal. Para ello, haga clic con el botón derecho en la pantalla. Las acciones de edición pueden estar restringidas por los permisos del navegador. Cuando una acción no está disponible para el usuario, los botones de la barra de herramientas y los elementos de menú contextual asociados no aparecerán.

Más información

Edición de la pantalla

5.6 Trabajar con sesiones

Todas las sesiones a las que usted tiene acceso están disponibles en la lista Sesiones Disponibles. El administrador del sistema crea y configura inicialmente las sesiones y se accede a ellas mediante una URL distribuida (por ejemplo, `https://<sessionserver>:7443`).

Para abrir una sesión

1. Seleccione la sesión y haga clic para abrirla.

2. Interactúe con su aplicación de host utilizando el panel Abrir sesión.

3. Puede crear múltiples instancias de una sesión configurada.

Puede tener múltiples sesiones abiertas simultáneamente y cambiar fácilmente entre ellas con ayuda de las fichas dispuestas en la parte superior de la pantalla. La sesión actual es siempre la ficha que se encuentra más a la izquierda y se identifica por un fondo blanco y texto en negrita. Cada sesión permanece activa durante 30 minutos.

Utilice la barra de herramientas para acceder a las distintas opciones disponibles para usted cuando interactúe con la sesión. Puede desconectarse de una sesión, cerrar la sesión, activar Teclas Rápidas y acceder a otras configuraciones. Es posible que algunas opciones estén sólo disponibles cuando su administrador le haya concedido permiso.

5.6.1 Utilizar Teclas Rápidas

El teclado del terminal de Teclas Rápidas ofrece una representación gráfica de las teclas en un teclado del host y le da acceso rápido a las teclas del terminal.

Haga clic en una tecla del terminal en el teclado de Teclas Rápidas para enviar la tecla al host. Las sugerencias de herramientas, que se visualizan pasando el cursor por una tecla, ofrecen una descripción de la asignación.

Las teclas rápidas están disponibles para cada tipo de host y se accede a ellas haciendo clic en el icono  de la barra de herramientas.

5.6.2 Edición de la pantalla

> **Nota**
>
> Cada navegador gestiona las funciones para copiar, pegar y cortar de un modo distinto y, en algunos casos, no se admitirá el uso de los botones de la barra de herramientas o el menú contextual. Se recomienda el uso de comandos de teclado para esas funciones. Aunque los comandos del teclado varían según el sistema operativo, en Windows son: CTRL+C para copiar, CTRL+V para pegar y CTRL+X para cortar.
>
> Es mucho más frecuente encontrar problemas con la función para pegar que con la función para cortar o copiar. Si no se muestra el botón Pegar de la barra de herramientas, es probable que la seguridad del navegador impida el acceso de lectura al portapapeles del sistema. Los diversos navegadores presentan un comportamiento diferente cuando se trata de proporcionar acceso al portapapeles. Sin embargo, la opción para pegar está casi siempre disponible mediante los comandos de teclado, (Control + V en Windows y Comando + V en Mac). En este caso, se presupone que no se han asignado de nuevo esas teclas. También puede utilizar el elemento de menú o el botón Pegar integrados del navegador.

Para copiar del terminal

1. Realce el área en la pantalla del terminal que desea copiar.
2. Haga clic en **Copiar** en la barra de herramientas o seleccione **Copiar** en el menú contextual disponible en la pantalla del terminal. También puede utilizar el comando de teclado, **CTRL + C**.

Para pegar en la pantalla del terminal

1. Posicione el cursor en el lugar en el que desea pegar el contenido.
2. Si el navegador admite la función para pegar, haga clic en **Pegar** en la barra de herramientas o seleccione **Pegar** en el menú contextual disponible en la pantalla del terminal. Si el navegador no admite esta función, estas opciones no estarán disponibles y deberá utilizar el comando de teclado, **CTRL + V**.

Para cortar áreas de la pantalla del terminal

> **Nota**
>
> Esta función está disponible para todos los tipos de terminales compatibles, excepto para los hosts VT.

1. Resalte el área en la pantalla del terminal que desea cortar.
2. Haga clic en **Cortar** en la barra de herramientas o seleccione **Cortar** en el menú contextual disponible en la pantalla del terminal. También puede utilizar el comando de teclado, **CTRL+X**.

Más información

- Especificar las opciones de edición

5.6.3 Salida de la sesión

En la esquina superior derecha de la pantalla, abra la lista desplegable asociada a su nombre de usuario y seleccione **Cerrar sesión** para dejar de trabajar con la aplicación del host.

5.7 Crear Macros

Una macro es una serie de acciones de teclado que usted graba y ejecuta después. Puede utilizar estos programas de macro JavaScript para automatizar las interacciones del usuario con el terminal. Puede acceder a macros y ejecutarlas desde todos los dispositivos compatibles.

Host Access for the Cloud graba y guarda macros avanzadas como JavaScript, lo que simplifica la edición y la mejora de las macros grabadas. Puede grabar macros para reproducirlas posteriormente, ejecutar macros al iniciar o cuando la sesión se conecta o desconecta del host. También puede escribir macros en el bloc de notas para realizar trabajos complejos que la grabadora no puede capturar.

Las macros se ponen a disposición de los usuarios de dos formas: creadas por un administrador o grabadas por los usuarios para su uso privado. Todas las macros están asociadas a una sesión y cumplen el mismo objetivo de automatizar la interacción con el host. La única diferencia entre ambas es sólo quién puede acceder a ellas y quién gestiona su creación y disponibilidad:

- **Macros creadas por administradores**

  Los administradores crean macros cuando crean la sesión. Son específicas de una sesión y están disponibles para todos los usuarios que tienen acceso a la sesión desde el icono Macro en la barra de herramientas. Los administradores pueden designar macros para ejecutarlas al iniciar o cuando la sesión se conecta o desconecta del host.

- **Macros creadas por usuarios**

  Los usuarios crean macros de usuarios finales para las sesiones para las que tienen autorización de acceso. El administrador concede permiso para crear macros configurando una Regla de Preferencias del Usuario. Los usuarios pueden acceder a la sesión utilizando sus propias credenciales o con función de Invitado. Las macros creadas por usuarios Invitados están disponibles para todos los usuarios Invitados. Los usuarios que han iniciado sesión utilizando sus propias credenciales pueden ver sólo las macros que han creado ellos.

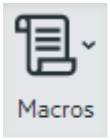
  Las macros avanzadas se listan en orden alfabético en la lista desplegable de la barra de herramientas. Las macros creadas por el usuario final se listan primero y van seguidas de un indicador de tres puntos grises en vertical que, cuando se ha seleccionado, muestra las opciones de Editar y Eliminar. Las macros creadas por el administrador se listan sin el indicador ya que esas macros no pueden ser modificadas por el usuario final.

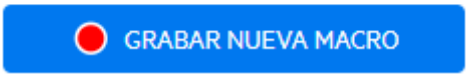
5.7.1 Trabajo con macros

Siga estos pasos para grabar, editar y ejecutar macros.

Grabar

1. Haga clic en el icono Macro de la barra de herramientas y haga clic en Grabar Nueva Macro.





2. Navegue por la aplicación del host para grabar las series de pasos que desea incluir en la macro.
3. Haga clic en  en la barra de herramientas para detener la grabación. El punto rojo parpadea para indicar que la grabación está en curso.
4. Cuando se le pida, escriba un nombre para la macro.

Editar

1. En la lista desplegable Macro, seleccione la macro que desea editar.

2. Haga clic en los tres puntos verticales para expandir el campo.
3. Haga clic en  para abrir el Editor de macros (en el panel izquierdo).
4. Utilice JavaScript para realizar los cambios que sean necesarios. Puede ejecutar y guardar la macro modificada utilizando los iconos de la barra de herramientas en el panel superior del editor.

Ejecute

Para ejecutar una macro, elija la macro en la lista desplegable y haga clic en  .

También puede asignar teclas que activarán automáticamente una macro ya grabada. En el cuadro de diálogo de configuración Asignar Tecla, seleccione **Ejecutar Macro** de la lista desplegable **Acción**. Seleccione una macro a asociar con la asignación de tecla de la lista **Valor**.

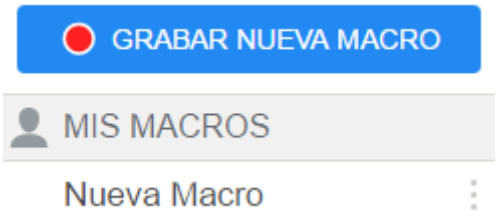
Detener

Puede detener una macro antes de que se complete desde el Editor de Macro o la barra de herramientas. Haga clic en  para detener la macro. Para volver a ejecutar la macro, navegue de vuelta a la pantalla de inicio de macro.

Suprimir

1. Seleccione en la lista desplegable Macro la macro que desea eliminar.

2. Expanda el campo haciendo clic en el icono de los tres puntos en vertical.



3. Haga clic en **Eliminar**.

Ver

La lista desplegable Macro está disponible desde la barra de herramientas para todos los usuarios que tienen permiso para grabar macros o acceden a una sesión en la que las macros han sido grabadas previamente por el administrador para que se utilicen en esa sesión.

Las macros se enumeran en **MIS MACROS** o **MACROS** en función de cómo se hayan grabado.

Todos los usuarios, tanto si han iniciado sesión con sus credenciales o como Invitado, pueden ver las macros asociadas a la sesión. Las macros enumeradas bajo el encabezado **MIS MACROS** aparecen en orden alfabético por su nombre y están visibles para los usuarios que las hayan grabado. Las macros grabadas por el administrador y asociadas a una sesión se muestran en orden alfabético en **MACROS**.

5.7.2 Depuración de macros

Como las macros están escritas en JavaScript y se ejecutan en el navegador, la mejor forma de depurarlas y de solucionar los problemas con ellas es utilizar las herramientas integradas en su navegador web. Los navegadores modernos vienen con un set de herramientas muy completo para depurar el código de JavaScript. Puede colocar puntos de interrupción, comprobar el código y obtener información de depuración.

> **Sugerencia**
>
> JavaScript distingue entre mayúsculas y minúsculas. Recuérdelo a la hora de editar el código de JavaScript.

Para depurar una macro:

1. Abra la macro que se va a editar. Consulte Trabajar con macros para obtener instrucciones.
2. Abra las herramientas de desarrollo del navegador.

Navegador	Abrir depurador
Mozilla Firefox 40.0.3	• Desde la barra de herramientas, abra el Menú y seleccione Desarrollador. • Desde el Menú Desarrollador Web, seleccione Depurador. El depurador se abre en un panel inferior.
Google Chrome 45.0	• Desde la barra de herramientas, abra el Menú y seleccione Más herramientas. • Seleccione Herramientas de Desarrollador para abrir el Depurador.
Microsoft Internet Explorer 11	• Desde la barra de herramientas, abra Configuración y seleccione F12 Herramientas de Desarrollador. • Abra la ficha Depurador.

3. Utilice una de las herramientas en el código de macro y ejecute el código.

   • debugger

   El enfoque más minucioso para depurar es utilizar la instrucción `"debugger"`. Cuando usted inserta estas instrucciones en su código de macro y lo ejecuta con las herramientas de desarrollo del navegador abiertas, la ejecución se detiene en esas líneas. Puede comprobar su macro, ver el valor de las variables locales y cualquier cosa que necesite comprobar.

   Le animamos a colocar múltiples instrucciones depurador; en su código para ayudarle a obtener la línea correcta. La naturaleza asíncrona de JavaScript puede hacer difícil la comprobación del código. Esto se puede compensar utilizando múltiples instrucciones depurador; colocadas cuidadosamente.

   Ejemplo 1: `debugger`

```
var hostCommand = menuSelection + '[enter]';
debugger;  // <– El depurador se detendrá aquí.
ps.sendKeys(hostCommand);
```

   • console.log(), alert()

   Estas dos opciones se suelen utilizar para depurar JavaScript. Aunque no son tan flexibles como la instrucción Depurador, ofrecen una vía rápida para obtener información de depuración. Estas funciones transmiten la información a la ficha “Consola” de JavaScript en las herramientas de desarrollador del navegador.

   Ejemplo 2: `console.log(), alert()`

```
var hostCommand = menuSelection + '[enter]';
console.log('Command:' + hostCommand);  // <– Proporcioionará la cadena a la pestaña "Console".
alert('Command:' + hostCommand); // Aparecerá una pequeña ventana que contiene los datos.
ps.sendKeys(hostCommand);
```

   • ui.message()

   La API de macros de Host Access for the Cloud proporciona una función de ui.message() que es muy similar a la función alert() de JavaScript. También puede utilizar la ui.message() para obtener información de depuración.

   Ejemplo 3: `ui.message()`

```
var hostCommand = menuSelection + '[enter]';
ui.message('Command:' + hostCommand); // <– Aparecerá una ventana de mensaje.
ps.sendKeys(hostCommand);
```

Tenga en cuenta lo siguiente:

- Comprobar y “yields”

  Mientras que las instrucciones yield en las macros las hacen más fáciles de entender, pueden hacer la comprobación del código con el depurador más difícil. Considere o bien utilizar múltiples instrucciones de depurador o instrucciones de depurador cuidadosamente colocadas de llamadas `console.log()` para obtener la información de depuración correcta.

- Internet Explorer

  La depuración en el Internet Explorer incluye el código transformado y puede ser más difícil que en otros navegadores.

5.7.3 Utilizar la API de macros

En Host Access for the Cloud, las macros se graban y escriben mediante JavaScript.

La API de macros consiste en un conjunto de objetos que puede utilizar para interactuar con el host, esperar estados de pantallas e interactuar con el usuario.

Acerca de promises y yields

Debido a que JavaScript se controla mediante un solo subproceso y utiliza "callback functions" y "promises" para ayudar a gestionar el flujo de ejecución del código, a veces puede ser difícil seguir el código. Host Access for the Cloud combina el concepto de "promises" con la clave "yield" para que el código de la macro se pueda organizar de forma más lineal.

- **Promises**

  Promises son patrones que ayudan a simplificar funciones que devuelven sus resultados de forma asíncrona en algún momento en el futuro. Todas las funciones "wait" y "ui" de la API de macros devuelven objetos "promise".

- **Yield**

  Las macros utilizan la palabra clave "yield" para bloquear la ejecución de la macro hasta que se resuelva o realice una "promise". Así, si se coloca yield enfrente de cualquier función ‘wait’ o ‘ui’, se detiene la ejecución hasta que esa función ha terminado de ejecutarse. Puede colocar la clave yield enfrente de cualquier función que devuelva una promise, también de sus propias funciones personalizadas.

> **Nota**
>
> La capacidad de bloquear la ejecución de la macro mediante la combinación de «yield» con «promises» está habilitada por la función `createMacro()`.

Errores

Los errores se pueden tratar en las macros utilizando una instrucción try / catch. Algunas funciones API pueden arrojar errores si, por ejemplo, no se cumplen las condiciones o si se sobrepasa el tiempo de espera. El error arrojado es 'atrapado' en la instrucción catch. Puede ajustar bloques de código más pequeños en una instrucción try / catch para tratar los errores a un nivel más granular.

Los desarrolladores de macro pueden generar también errores con `'throw new Error('Mensaje de error útil');`

Más información

- Objetos de Macro API
- Ejemplos de Macros

5.8 Objetos de Macro API

Puede crear macros utilizando la Macro API. De forma predeterminada para el uso en macros, se dispone de cuatro objetos primarios:

- **Session** - el punto de entrada principal para acceder al host. El objeto Session se utiliza para conectar, desconectar y proveer acceso al objeto PresentationSpace.
- **PresentationSpace** - representa la pantalla y proporciona muchas funciones comunes, como obtener y ajustar la ubicación del cursor, enviar datos al host y leer de la pantalla. Se obtiene llamando `session.getPresentationSpace()`.
- **Wait** - facilita una forma sencilla de esperar a que se produzcan varios estados del host antes de seguir enviando más datos o leer de la pantalla. Por ejemplo, puede esperar a que el cursor esté situado en una posición determinada, a que haya texto presente en una posición de la pantalla o simplemente esperar una cantidad de tiempo fija. Todas las llamadas de la función 'Wait' requieren la palabra clave yield, que se explica más adelante.
- **Interfaz de usuario:** - disponible automáticamente en la macro como la variable "ui". Provee capacidades básicas de interfaz de usuario. Puede utilizar este objeto para mostrar datos al usuario o para indicarlos a modo de información. Todas las llamadas de la función "UI" requieren la palabra clave "yield".

Todos los objetos disponibles

Consulte la lista de objetos disponibles en el panel de navegación derecho, "En esta página". (Es posible que deba expandir el navegador).

5.8.1 Attribute

Utilice el objeto Attribute, junto con el objeto AttributeSet, para descifrar la información de formato presente en la celda de datos.

Attribute	Indica...
PROTECTED	Una celda de datos protegida.
MODIFIED	Una celda de datos modificada.
NUMERIC_ONLY	El inicio de una celda de datos solo de caracteres numéricos.
ALPHA_NUMERIC	Una celda de datos alfanuméricos.
HIGH_INTENSITY	Si la celda de datos contiene texto de alta intensidad.
HIDDEN	Si la celda de datos contiene texto oculto.
PEN_DETECTABLE	Si la celda de datos es detectable por lápiz.
ALPHA_ONLY	Una celda solo de datos alfabéticos.
NUMERIC_SHIFT	El inicio de un campo numérico mayúscula.
NUMERIC_SPECIAL	Que la celda de datos marca el inicio de un campo numérico especial.
KATAKANA_SHIFT	Una sección de texto Katakana.
MAGNETIC_STRIPE	Que la celda de datos marca el inicio de un campo de banda magnética.
SIGNED_NUMERIC_ONLY	Que la celda de datos es un campo numérico firmado.
TRANSMIT_ONLY	Que la celda de datos es un campo solo de transmisión.
FIELD_END_MARKER	Que la celda de datos marca el final de un campo modificado.
FIELD_START_MARKER	Que la celda de datos marca el inicio de un campo modificado.
SPECIAL_EMPHASIS_PROTECTED	Un campo protegido de énfasis especial.
TAB_STOP	Que la celda de datos contiene una posición de tabulación.
REVERSE	Que la celda de datos se visualiza en modo de vídeo inverso.

Attribute	Indica...
BLINKING	Que la celda de datos contiene texto intermitente.
RIGHT_JUSTIFIED	Que la celda de datos marca el inicio de un campo justificado a la derecha.
LEFT_JUSTIFIED	Que la celda de datos marca el inicio de un campo justificado a la izquierda.
LOW_INTENSITY	Que la celda de datos contiene texto de baja intensidad.
UNDERLINE	Que la celda de datos contiene texto subrayado.
DOUBLE_BYTE	Que la celda de datos contiene texto de doble byte.
COLUMN_SEPARATOR	Que la celda de datos contiene un separador de columnas.
BOLD	Que la celda de datos contiene texto en negrita.
DOUBLE_WIDTH	Que la celda de datos marca un campo de anchura doble.
DOUBLE_HEIGHT_TOP	Una celda de datos superior de altura doble.
DOUBLE_HEIGHT_BOTTOM	Una celda de datos inferior de altura doble.
CONTROL_PAGE_DATA	Que la celda de datos contiene datos de página de control.
RIGHT_COLUMN_SEPARATOR	Que la celda de datos contiene un separador de columnas derecho.
LEFT_COLUMN_SEPARATOR	Que la celda de datos contiene un separador de columnas izquierdo.
UPPERSCORE	Que la celda de datos contiene sobrerrayado.
STRIKE_THROUGH	Que la celda de datos contiene texto tachado.

5.8.2 AttributeSet

El objeto AttributeSet permite al usuario descifrar los atributos presentes en la celda de datos. El objeto AttributeSet devuelve valores definidos en el objeto Attribute y cuando se utilizan juntos se puede obtener información de formato de la celda de datos.

Método	Descripción
`contains(attribute)`	Determina si el conjunto contiene el atributo especificado. **Parámetros** `{Number}` Atributo que se comprobará. **Devuelve** `{Boolean}` "True" (verdadero) si el atributo se encuentra en el conjunto.
`isEmpty()`	Determina si el conjunto de atributos está vacío. **Devuelve** `{Boolean}` "True" si el conjunto está vacío.
`size()`	Indica el número de atributos en un conjunto. **Devuelve** `{Number}` El número de atributos.
`toArray()`	Convierte el conjunto de atributos interno en una matriz. **Devuelve** `{Number[]}` Matriz de valores de atributos en el conjunto.
`toString()`	Convierte el conjunto de atributos interno en una cadena. **Devuelve** `{String} Nombres de atributos con espacio delimitado en el conjunto.`
`forEach(callback, thisArg)`	Función para iterar sobre cada elemento en el conjunto de atributos. **Parámetros** `{forEachCallback}` Devolución de llamada para realizar la operación específica. Se llama con el nombre de cada atributo en el conjunto. `{Object} thisArg` Puntero opcional a un objeto de contexto.
`forEachCallback(string, object)`	Un usuario ha provisto la función callback donde usted provee el comportamiento de ser utilizado como el parámetro callback para forEach. **Parámetros** `{String} Nombre de cadena de un atributo en el conjunto de atributos.`

	`{Object} thisArg` Puntero opcional a un objeto de contexto.

5.8.3 AutoSignOn

Método	Descripción
`getPassTicket()`	Obtiene un ticket de paso que se utiliza para iniciar sesión en una aplicación de mainframe. Se pueden solicitar múltiples tickets de paso utilizando distintos IDs de aplicación. **Parámetros** {String} El ID de aplicación indica al host la aplicación para la que es la entrada. **Devuelve** {Promise} Se cumple con la clave de ticket de paso o se rechaza si la operación falla. El ticket de paso obtenido del DCAS funciona sólo con la sesión de host actual y es válido durante diez minutos.
`sendUserName()`	Aplica el nombre de usuario incluido en el ticket de paso al campo en la posición actual del cursor en la pantalla de host actual. El nombre de usuario se debe enviar antes que la contraseña. Si se envía la contraseña primero, el ticket de paso quedará invalidado y usted tendrá que obtener otro. **Parámetros** {String} passTicketKey obtenida del getPassTicket. **Devuelve** {Promise} Se cumple si se envía correctamente el nombre de usuario. Rechazado si la operación falla.
`sendPassword()`	Aplica la contraseña incluida en el ticket de paso al campo en la posición actual del cursor en la pantalla de host actual. El nombre de usuario se debe enviar antes que la contraseña. Si se envía la contraseña primero, el ticket de paso quedará invalidado y usted tendrá que obtener otro. **Parámetros** {String} passTicketKey obtenida de getPassTicket. **Devuelve** {Promise} Se cumple si se envía correctamente la contraseña. Rechazado si la operación falla.

5.8.4 Color

Constantes de color a utilizar para los colores de primer plano y de fondo del objeto DataCell.

Color	Descripción	Valor Numérico
BLANK_UNSPECIFIED	Ningún color especificado	0
BLUE	Azul	1
GREEN	Verde	2
CYAN	Cian	3
RED	Rojo	4
MAGENTA	Magenta	5
YELLOW	Amarillo	6
WHITE_NORMAL_INTENSITY	Blanco de intensidad normal	7
GRAY	Gris	8
LIGHT_BLUE	Azul claro	9
LIGHT_GREEN	Verde claro	10
LIGHT_CYAN	Cian claro	11
LIGHT_RED	Rojo claro	12
LIGHT_MAGENTA	Magenta claro	13
BLACK	Negro	14
WHITE_HIGH_INTENSITY	Blanco de alta intensidad	15
BROWN	Marrón	16
PINK	Rosa	17
TURQUOISE	Turquesa	18

5.8.5 ControlKey

El objeto ControlKey define constantes para enviar teclas de control de cursor y comandos de host utilizando el método sendKeys. Las constantes están disponibles para estos tipos de host:

- IBM 3270
- IBM 5250
- VT
- UTS

IBM 3270

Palabra clave	Descripción
ALTVIEW	Alternar vista
ATTN	Atención
BACKSPACE	Retroceso
BACKTAB	TabAtrás
CLEAR	Borrar o Borrar pantalla
CURSOR_SELECT	Selección de cursor
DELETE_CHAR	Eliminar o Eliminar carácter
DELETE_WORD	Eliminar palabra
DEST_BACK	Borrar al utilizar Retroceso
DEV_CANCEL	Cancelar dispositivo
DOWN	Cursor abajo
DSPSOSI	Mostrar SO/SI
DUP	Campo duplicado
END_FILE	Final de campo
INTRO	Introduzca
ERASE_EOF	Eliminar final de campo
ERASE_FIELD	Eliminar campo
ERASE_INPUT	Eliminar entrada
FIELD_MARK	Marca de campo
HOME	Inicio de cursor
IDENT	Ident
INSERT	Insertar
LEFT_ARROW	Cursor izquierda
LEFT2	Dos posiciones a la izquierda
NEW_LINE	Nueva línea
PA1 - PA3	PA1 - PA3

Palabra clave	Descripción
PF1 - PF24	PF1 - PF24
PAGE_DOWN	Avance página
PAGE_UP	Retroceso página
RESET	Reset, reset terminal
RIGHT2	2 posiciones a la derecha
RIGHT_ARROW	Cursor derecha, derecha
SYSTEM_REQUEST	Solicitud de sistema
TAB	Tecla tabulación
UP	Cursor arriba

IBM 5250

Palabra clave	Descripción
ALTVIEW	Alternar vista
ATTN	Atención
AU1 - AU16	AU1 - AU16
BACKSPACE	Retroceso
BACKTAB	TabAtrás
BEGIN_FIELD	Principio de campo
CLEAR	Borrar o Borrar pantalla
DELETE_CHAR	Eliminar o Eliminar carácter
DEST_BACK	Borrar al utilizar Retroceso
DOWN	Cursor abajo
DSPSOSI	Mostrar SO/SI
DUP	Campo duplicado
END_FILE	Final de campo
INTRO	Introduzca
ERASE_EOF	Eliminar final de campo
ERASE_FIELD	Eliminar campo
ERASE_INPUT	Eliminar entrada
FIELD_EXT	Salir del campo
FIELD_MINUS	Campo resta
FIELD_PLUS	Campo suma
FIELD_MARK	Marca de campo
HELP	Solicitud de ayuda
HEXMODE	Modo Hex
HOME	Inicio de cursor
INSERT	Insertar
LEFT_ARROW	Cursor izquierda

Palabra clave	Descripción
NEW_LINE	Nueva línea
PA1 - PA3	PA1 - PA3
PF1 - PF24	PF1 - PF24
PAGE_DOWN	Avance página
PAGE_UP	Retroceso página
[imprimir]	Imprimir
RESET	Reset, reset terminal
RIGHT_ARROW	Cursor derecha, derecha
SYSTEM_REQUEST	Solicitud de sistema
TAB	Tecla tabulación
UP	Cursor arriba

VT

Palabra clave	Descripción
BACKSPACE	Retroceso
BREAK	Interrumpir
CLEAR	Borrar o Borrar pantalla
CURSOR_SELECT	Selección de cursor
DELETE_CHAR	Eliminar o Eliminar carácter
DOWN	Cursor abajo
EK_FIND	Editar buscar de teclado numérico
EK_INSERT	Editar insertar de teclado numérico
EK_NEXT	Editar siguiente de teclado numérico
EK_PREV	Editar anterior de teclado numérico
EK_REMOVE	Editar quitar de teclado numérico
EK_SELECT	Editar seleccionar de teclado numérico
END_FILE	Final de campo
INTRO	Introduzca
F1 - F24	F1 - F24
HOLD	Retención
HOME	Inicio
INSERT	Insertar
KEYPAD_COMMA	Teclado numérico Coma
KEYPAD_DOT	Teclado numérico decimal
KEYPAD_ENTER	Teclado numérico Intro
KEYPAD_MINUS	Teclado numérico -
KEYPAD0 - KEYPAD9	Teclado numérico 0 - Teclado numérico 9
LEFT_ARROW	Cursor izquierda
PF1 - PF20	PF1 - PF20
PAGE_DOWN	Avance página

Palabra clave	Descripción
PAGE_UP	Retroceso página
RESET	Reset, reset terminal
RETURN	Retorno, retorno de carro
RIGHT_ARROW	Cursor derecha, derecha
TAB	Tecla tabulación
UDK16 - UDK20	Tecla definida por el usuario 6 - Tecla definida por el usuario 20
UP	Cursor arriba

UTS

Palabra clave	Descripción
BACKSPACE	Retroceso
BACKTAB	TabAtrás
CHAR_ERASE	Borra el carácter en la posición del cursor y avanza el cursor.
CLEAR_DISPLAY	Borrar pantalla
CLEAR_EOD	Eliminar hasta final de pantalla
CLEAR_EOF	Eliminar hasta final de campo
CLEAR_EOL	Eliminar hasta final de línea
CLEAR_FCC	Borrar carácter de control de campo
CLEAR_HOME	Borrar pantalla y mover el cursor a la posición inicial
CONTROL_PAGE	Alternar la página de control
DELETE_LINE	Elimina la línea en la que se encuentra el cursor y sube las líneas restantes una fila arriba
DELIN_LINE	Borra el carácter que se encuentra debajo del cursor y mueve los caracteres restantes una línea hacia la izquierda.
DELIN_PAGE	Borra el carácter que se encuentra debajo del cursor y mueve los caracteres restantes una página hacia la izquierda.
DOWN	Mueve el cursor una línea hacia abajo. Se ajusta en la parte inferior.
DUP_LINE	Crea una copia de la línea actual y sobrescribe la línea siguiente con la duplicada.
END_FIELD	Mueve el cursor al final del campo actual.
END_PAGE	Mueve el cursor al final de la página actual.
EURO	Inserta el carácter del Euro
F1 - F22	Teclas de función F1-F22
HOME	Mueve el cursor al principio de la página actual (fila 1, col 1)
INSERT	Alterna el modo insertar/sobrescribir.
INSERT_IN_LINE	

Palabra clave	Descripción
	Inserta un espacio en la posición del cursor y mueve los caracteres restantes de la línea a la derecha. El carácter en la columna más a la derecha de la línea se descarta.
INSERT_IN_PAGE	Inserta un espacio en la posición del cursor y mueve los caracteres restantes de la página a la derecha. El carácter en la columna más a la derecha de cada línea se descarta.
INSERT_LINE	Inserta una nueva línea en la flecha del cursor y mueve las líneas restantes hacia abajo. La última fila de la página se descarta.
LEFT_ARROW	Mueve el cursor una posición hacia la izquierda ajustándolo de ser necesario.
LOCATE_FCC	Encuentra el carácter de control de campo siguiente en la pantalla.
MSG_WAIT	Recupera la cola de mensajes al terminal.
RETURN	Retorno de carro
RIGHT_ARROW	Mueve el cursor una posición hacia la derecha ajustándolo de ser necesario.
SOE	Inserta el carácter de Inicio de Entrada
START_OF_FIELD	Mueve el cursor al principio del campo.
START_OF_LINE	Mueve el cursor a la columna 1 de la línea actual.
TAB	Mueve el cursor a la posición de tabulación siguiente de la pantalla.
TOGGLE_COL_SEP	Alterna el atributo de separador de columna.
TOGGLE_STRIKE_THRU	Alterna el atributo de tachado en la celda de datos actual.
TOGGLE_UNDERLINE	Alterna el atributo de subrayado en la celda de datos actual.
TRANSMIT	Transmite datos de campo modificados al host.
UNLOCK	Envía la tecla UNLOCK al host.
UP	Mueve el cursor una fila hacia arriba, ajustándolo si es necesario.

5.8.6 DataCell

El objeto DataCell ofrece información sobre una posición particular en una pantalla del terminal.

Método	Descripción
`getPosition()`	Devuelve la posición de esta celda de datos en la pantalla. **Devuelve** `{Position}` La posición de la celda de datos en la pantalla.
`getChar()`	Obtiene el carácter asociado a la celda. **Devuelve** `{String}` El carácter asociado a la celda.
`getAttributes()`	Devuelve el conjunto de atributos especificado para esta instancia de celda de datos. Consulte AttributeSet. **Devuelve** `{AttributeSet}` El conjunto de atributos de esta instancia de celda de datos.
`getForegroundColor()`	Devuelve el color de primer plano, como está definido en el objeto Color, para esta celda de datos. **Devuelve** `{Number}` Color en primer plano de esta celda de datos. El color se define en el objeto Color.
`getBackgroundColor()`	Devuelve el color de fondo, como está definido en el objeto Color, para esta celda de datos. **Devuelve** `{Number}` Color de fondo de esta celda de datos. El color se define en el objeto Color.
`toString`	Convierte la celda de datos interna en una cadena. **Devuelve** `{String}` La representación en forma de cadena de una celda de datos.
`isFieldDelimiter()`	Comprueba si esta celda representa un delimitador de campo. **Devuelve** `{Boolean}` "True" (verdadero) si esta celda es un delimitador de campo; de lo contrario, "False" (falso).

5.8.7 Dimensión

Representa el tamaño de la pantalla o de la región de la pantalla.

Método	Descripción
`Dimension(rows,cols)`	Crea una nueva instancia Dimension **Parámetros** `{Number} filas` Dimensión de las filas de la pantalla. `{Number} columnas` Dimensión de las columnas de la pantalla.

5.8.8 Field

Utilice el objeto Field con FieldList para obtener la información presente en un campo de la pantalla.

Método	Descripción
`getAttributes()`	Devuelve el conjunto de atributos especificado para esta instancia de campo. Consulte AttributeSet. **Devuelve** `{AttributeSet}` El conjunto de atributos de este campo.
`getForegroundColor()`	Devuelve el color en primer plano para el campo. **Devuelve** `{Number}` Color en primer plano de este campo. Estos valores se definen en el objeto Color.
`getBackgroundColor()`	Devuelve el color de fondo para el campo. **Devuelve** `{Number}` Color de fondo de este campo. Estos valores se definen en el objeto Color.
`getStart()`	Devuelve la posición inicial del campo. La posición inicial es la posición del primer carácter del campo. Algunos tipos de host utilizan una posición de carácter para guardar los atributos de nivel de campo. En este caso, la posición del atributo no está considerada la posición inicial. **Devuelve** `{Position}` Posición inicial del campo. **Genera** `{RangeError}` Para campos de longitud cero.
`getEnd()`	Devuelve la posición final del campo. La posición final es la posición en el espacio de representación que contiene el último carácter del campo. **Devuelve** `{Position}` Posición final del campo. **Genera** `{RangeError}` Para campos de longitud cero.
`getLength()`	Devuelve la longitud del campo. Para los tipos de host que utilizan una posición de carácter para guardar los atributos de campo, la longitud del campo no incluye la posición del atributo de campo. **Devuelve** `{Number}` Longitud del campo.
`getDataCells()`	Obtiene las celdas de datos que comprende este campo. Consulte DataCell. **Devuelve**

	`{DataCell[]}` Las celdas de datos que comprenden este campo.
`getText()`	Obtiene el texto del campo. **Devuelve** `{String}` Campo de texto.
`setText()`	Establece el texto del campo. Para algunos tipos de host, como los VT, el texto se transmite al host de inmediato, pero en otros tipos de host el texto no se transmite al host hasta que se invoca una tecla de ayuda. Si el texto es más corto que el campo, el texto se coloca en el campo del host y el resto del campo se borra. Si el texto es más largo que el campo del host, se coloca tanto texto como quepa en el campo. **Parámetro** `{String}` Texto que se colocará en el campo. **Genera** `{Error}` Si el campo está protegido.
`clearField()`	Borra el campo actual de forma específica de la emulación. **Genera** `{Error}` Si el campo está protegido o no se admite el borrado.
`getPresentationSpace()`	Obtiene el objeto PresentationSpace que ha creado este campo. **Devuelve** `{PresentationSpace}` Elemento principal de esta instancia de campo.
`toString()`	Crea una descripción sencilla del campo. **Devuelve** `{String}` Una interpretación del campo legible por el usuario.

5.8.9 FieldList

Utilice el objeto FieldList junto con el objeto Field para obtener información de la lista de campos.

Método	Descripción
`getPresentationSpace()`	Obtiene el objeto PresentationSpace que ha creado este campo. **Devuelve** `{PresentationSpace}` Elemento principal de esta instancia de campo.
`findField(position, text, direction)`	Devuelve el campo que contiene el texto especificado. La búsqueda empieza desde la posición especificada y se realiza hacia delante o hacia detrás. Si la cadena contiene múltiples campos, se devuelve el campo que contiene la posición inicial. Cuando se busca hacia delante, la búsqueda no se ajusta a la parte superior de la pantalla. Cuando se busca hacia atrás, la búsqueda no se ajusta a la parte inferior de la pantalla. **Parámetros** `{Position}` Posición desde la que se debe iniciar la búsqueda. Consulte el objeto Position. `{String}` El texto a buscar (opcional). Si no se indica, devuelve el campo siguiente a la derecha o debajo de la posición especificada. `{Number}` Dirección de la búsqueda (opcional). Utilice PresentationSpace. Constantes SearchDirection para estos parámetros. Por ejemplo, PresentationSpace.SearchDirection.FORWARD o PresentationSpace.SearchDirection.BACKWARD. Si no se indica, se busca hacia delante. **Devuelve** `{Field}` Contiene la cadena o cero si no se encuentra un campo que cumpla los criterios especificados. **Genera** `{RangeError}` Si la posición está fuera del rango.
`get(index)`	Obtiene el campo en el índice dado. **Parámetros** `{Number}` Índice en la lista de campos. **Devuelve** `{Field}` Ubicado en el índice especificado. **Genera** `{RangeError}` Si el índice está fuera del rango.
`isEmpty()`	

	Determina si la lista de campos está vacía. **Devuelve** `{Boolean}` "True" (verdadero) si la lista está vacía.
`size()`	Indica el número de campos en la lista. **Devuelve** `{Number}` El número de campos.
`toString()`	Crea una descripción sencilla la lista de campos. **Devuelve** `{String}` Una interpretación de la lista de campos legible por el usuario.

5.8.10 FileTransfer

Utilice el objeto FileTransfer para listar y transferir archivos entre el sistema del host y el cliente.

La API de transferencia de archivos de Host Access for the Cloud abstrae las convenciones de ruta de archivos utilizadas por diferentes implementaciones de archivos del host. Siga los formatos de ruta de sistema de archivos URL o Linux a la hora de formatear las rutas de archivo utilizadas por la API. Por ejemplo, `/root/directory/file`.

Es importante observar todas las reglas específicas de los sistemas de host, como los caracteres permitidos o las longitudes de los nombres.

> **Nota**
>
> Los navegadores imponen importantes restricciones de seguridad sobre la capacidad de Javascript para interactuar con los sistemas de archivos de los clientes.

Método	Descripción
`getHostFileListing(remotePath)` `()`	Solicitar un listado de archivos de host. Si se omite `RemotePath`, se muestra un listado de archivos para el directorio de trabajo remoto actual. **Parámetros** `{String}` (opcional) Si se especifica, se obtiene un listado de archivos para la ruta remota especificada. Si no se especifica, se obtiene un listado de archivos para el directorio de trabajo remoto actual. **Devuelve** `{Promise}` Se resuelve en una matriz de objetos HostFile incluidos en remoteName. Se rechaza si la ruta remota no se puede leer.
`sendFile(localFile,` `remoteName)`	Envía el archivo especificado al host. **Parámetros** `{File}` Objeto de archivo de Javascript que señala al archivo local que se va a enviar. `{String}` (opcional) Nombre completo de archivo remoto tal y como lo permite el sistema remoto (Unix, Windows, MVS o VAX). **Devuelve** `{Promise}` Se cumple con un objeto `HostFile` que indica que el archivo se ha enviado correctamente. Se rechaza si se ha producido un error al enviar el archivo.
`getDownloadURL(remoteName)`	Construye un vínculo para descargar un archivo desde un sistema de host. **Parámetros** `{String}` Nombre completo de archivo remoto, tal y como lo permite el sistema remoto (Unix, Windows, MVS o VAX). **Devuelve** `{URL}` URL que se puede utilizar para recuperar el archivo desde el servidor de sesión de Host Access for the Cloud.
`setTransferOptions(options)`	Establece las opciones de transferencia para la sesión FileTransfer actual. Las opciones de transferencia se aplican a todas las transferencias futuras cuando o bien se cierra la sesión, o bien

	ésta se sobrescribe con otra llamada a `setTransferOptions`. **Parámetros** `{JSON}` Consulte FileTransferOptions para conocer los nombres y valores permitidos. **Devuelve** `{Promise}` Se cumple cuando finaliza la llamada. Se rechaza si se ha producido un error al configurar las opciones.
`cancelar()`	Cancela la transferencia actual en curso. **Parámetros** `{String}` Nombre completo de archivo remoto, tal y como lo permite el sistema remoto (Unix, Windows, MVS o VAX). **Devuelve** `{Promise}` Se cumple cuando finaliza la llamada. Se rechaza si se ha producido un error al cancelar la transferencia.

5.8.11 FileTransferFactory

Un objeto fileTransferFactory está disponible para todas las macros. Si se han configurado transferencias de archivos para la sesión, puede utilizarlas para obtener una referencia a un objeto FileTransfer.

Método	Descripción
`getIND$File()`	Devuelve un objeto FileTransfer para interactuar con el tipo Ind$File configurado para la sesión. **Devuelve** `{FileTransfer}` **Genera** `{Error}` Si la sesión no se ha configurado para permitir transferencias IND$File.

5.8.12 FileTransferOptions

Especificación del objeto de opción de transferencia de archivos. Ejemplo: `fileTransfer.setTransferOptions({ transferMethod : 'ascii' });```

Método	Descripción
`transferMethod`	`{String}` Valores permitidos: • 'ascii' • 'binario'

5.8.13 HostFile

Un objeto HostFile representa un archivo en el sistema de archivos del host.

Método	Descripción
`getName()`	Obtiene el nombre de archivo. **Devuelve** `{String}` El nombre de archivo.
`getParent()`	Obtiene el creador de este archivo del host. **Devuelve** `{String}` El elemento principal de este archivo del host. Esto significa cosas diferentes en tipos de host diferentes. Por ejemplo, en TSO éste es el nombre del catálogo en el que reside el archivo.
`getSize()`	El tamaño en bytes del archivo. **Devuelve** `{Number}` El tamaño del archivo en bytes.
`getType()`	El tipo de archivo representado. **Devuelve**

5.8.14 HostFileType

El objeto HostFileType define constantes para determinar el tipo de un objeto HostFile.

Valor	Descripción
FILE	Representa un archivo en el sistema de host.
DIR	Representa un directorio en el sistema de host.
DESCONOCIDO	Representa un archivo del host de origen desconocido.

5.8.15 OIA

Interfaz Operator Information Area (OIA). El objeto OIA devuelve valores que se han definido en el objeto OIAStatus.

Método	Descripción
`getStatus ()`	Devuelve el conjunto de indicadores de estado habilitado. Consulte StatusSet. **Devuelve** `{StatusSet}` Contiene la información de estado.
`getCommErrorCode()`	Devuelve el código de error de comunicación actual. **Devuelve** `{Number}` El código de error de comunicación actual. Si no existe, será 0.
`getProgErrorCode()`	Devuelve el código de error del programa actual.. **Devuelve** `{Number}` El código de error de programa actual. Si no existe, será 0.

5.8.16 OIAStatus

OIAStatus	Descripción
CONTROLLER_READY	Controlador listo
A_ONLINE	Online con una conexión no-SNA
MY_JOB	Conectada a una aplicación de host
OP_SYS	Conectada a SSCP (SNA)
UNOWNED	No conectada
TIME	Teclado inhibido
SYS_LOCK	Bloqueo del sistema tras tecla AID
COMM_CHECK	Prueba de comunicación
PROG_CHECK	Prueba de programa
ELSEWHERE	Pulsación de tecla no válido en la posición del cursor
FN_MINUS	Función no disponible
WHAT_KEY	Pulsación de tecla no válido
MORE_THAN	Demasiados caracteres ingresados en el campo
SYM_MINUS	Símbolo introducido no disponible
INPUT_ERROR	Error de entrada de operador (5250 sólo)
DO_NOT_ENTER	No introducir
INSERT	Cursor en modo insertar
GR_CURSOR	Cursor en modo gráfico
COMM_ERR_REM	Recordatorio de error de comunicación
MSG_WAITING	Indicador de mensaje en espera
ENCRYPT	La sesión está cifrada
NUM_FIELD	Carácter no válido en campo sólo numérico

5.8.17 Posición

Método	Descripción
`Position(row,col)`	Crea una nueva instancia Position **Parámetros** `{Number}` Coordenada de fila de la pantalla de filas. `{Number}` Coordenada de columna de la pantalla de columnas.

5.8.18 PresentationSpace

Utilice el objeto PresentationSpace para interactuar con la pantalla del terminal. Entre las interacciones disponibles están ajustar y obtener la posición del cursor y la lectura de texto.

Método	Descripción
`getCursorPosition()`	Devuelve una instancia de Position que representa la posición actual del cursor. Una sesión no conectada tiene una posición de cursor de 0,0. **Devuelve** `{Position}` Ubicación actual del cursor.
`setCursorPosition(position)`	Mueve el cursor del host a la posición de fila y columna especificado. En algunos hosts, como los VT, el host puede restringir los movimientos del cursor. **Parámetros** `{Position}` Position Nueva posición del cursor. **Devuelve** None **Genera** `{RangeError}` Si la posición no es válida en la pantalla actual.
`isCursorVisible()`	Comprueba que el cursor está actualmente visible en el espacio de presentación. El cursor se considera no visible si la sesión no está conectada. **Devuelve** `{Boolean}` "True" (verdadero) si el cursor está visible. False si el cursor no está visible.
`sendKeys(keys)`	Transmite una cadena de texto o ControlKey al host en la posición actual del cursor en el espacio de presentación. Si el cursor no se encuentra en la posición deseada, utilice primero la función `setCursorPosition`. La cadena de texto puede contener cualquier número de caracteres y objetos ControlKey. Por ejemplo: "myname" + `ControlKey.TAB` + "mypass" + `ControlKey.ENTER` transmitirá un ID de usuario, tabulará al campo siguiente, transmitirá una contraseña y, a continuación, transmitirá la tecla Intro. Si necesita transmitir un corchete, duplique los corchetes ([[o]]). **Parámetros** `{String}` Texto de teclas o teclas de control que se transmitirán.
`getText(start,length)`	Devuelve una cadena que representa un área lineal del espacio de presentación. Cuando se encuentran los

	límites de la fila, no se insertan caracteres de nueva línea. **Parámetros** `{Position}` Posición inicial desde la que se debe recuperar el texto. `{Number}` Longitud del número máximo de caracteres que se devolverán. Si el parámetro de longitud provoca que se supere la última posición del espacio de presentación, solo se devuelven los caracteres hasta la última posición. **Devuelve** `{String)` Representa un área lineal del espacio de presentación que puede estar vacía si la sesión no está conectada. **Genera** `{RangeError}` Si la posición o la longitud no son válidas en la pantalla actual.
`getSize()`	Obtiene las dimensiones de la pantalla como objeto Dimension. **Devuelve** `{Dimension}` Contiene el número de filas y columnas. El tamaño de la pantalla es [row:0, col:0] si la sesión no está conectada.
`getDataCells(start, length)`	Devuelve instancias de DataCell en las que el primer miembro será para la posición especificada por el parámetro de inicio. El número máximo de instancias DataCell en la lista viene especificado por el parámetro de longitud. **Parámetros** `{Position}` Inicio de la primera posición en la pantalla del host en la que se recuperan instancias de DataCell. Consulte Position. `{Number}` Longitud del número máximo de instancias de DataCell que se van a recuperar. Si no se especifica, devuelve DataCells de la posición inicial a la posición final de la pantalla. **Devuelve** `{DataCell[]}` Instancias que pueden estar vacías si no se ha conectado la sesión. Si la posición no está especificada, devuelve todas las DataCells. Si la longitud no se especifica, devuelve DataCells de la posición inicial a la posición final de la pantalla.

	Genera `{RangeError}` Si el inicio o la longitud están fuera del rango.
`getFields()`	Devuelve una lista de los campos en el espacio de presentación. Si el tipo de host no soporta campos o si la pantalla actual no está formateada el valor de retorno será siempre una lista vacía. Consulte FieldList. **Devuelve** `{FieldList}` Para los campos definidos del host en el espacio de presentación.

5.8.19 Session

El objeto Session es el punto de entrada principal para acceder al host. Contiene las funciones para conectar, desconectar y obtener el objeto PresentationSpace.

Método	Descripción
`connect()`	Conecta con el host configurado. Si es necesario, utilice `wait.forConnect()` para bloquear la ejecución de la macro hasta que la sesión esté conectada. **Devuelve** `None`.
`disconnect()`	Se desconecta del host configurado. Si es necesario, utilice `wait.forDisconnect()` para bloquear la ejecución de la macro hasta que la sesión esté conectada. **Devuelve** `None`.
`isConnected()`	Determina si la conexión con el host está establecida o no. **Devuelve** `{Boolean}` "True" (verdadero) si se ha establecido la conexión con el host; de lo contrario, "False" (falso).
`getPresentationSpace()`	Proporciona acceso a la instancia de PresentationSpace para esta sesión. **Devuelve** `{PresentationSpace}` Instancia asociada a esta sesión.
`getDeviceName()`	Devuelve el nombre del dispositivo para una sesión conectada o una cadena vacía si la sesión está desconectada o no tiene un nombre de dispositivo. **Devuelve** `{String}` El nombre del dispositivo conectado.
`getType()`	Devuelve el tipo de sesión de host. Véase SessionType. **Devuelve** `{String}` El tipo de sesión del host.
`setDeviceName()`	Aporta un medio para modificar el nombre de dispositivo en una instancia de sesión. **Parámetros** `{String}` name Nombre del dispositivo que se utilizará al conectarse a un host. **Genera** `{Error}` Si se intenta configurar el nombre de dispositivo mientras la sesión está conectada.
`getOIA()`	Proporciona acceso a la instancia de OIA para esta sesión. **Devuelve** `{OIA}` OIA asociada a este sesión.

5.8.20 SessionType

Constantes utilizadas para identificar el tipo de host al que se está realizando la conexión. Consulte el objeto Session.

Tipo de host	Descripción
IBM_3270	Indica una sesión de terminal IBM 3270
IBM_5250	Indica una sesión de terminal IBM 5250
VT	Indica una sesión VT

5.8.21 StatusSet

Puede utilizar el objeto StatusSet para descifrar el estado de OIA. El objeto StatusSet devuelve valores definidos en el objeto OIAStatus y, cuando se utilizan juntos, se puede obtener información de estado del OIA.

Método	Descripción
`contains(statusFlag)`	Determina si el conjunto contiene el indicador de estado especificado de constantes de OIAStatus. **Parámetros** `{Number}` Estado de statusFlag que se comprobará. **Devuelve** `{Boolean}` "True" (verdadero) si el indicador de estado está presente en el conjunto.
`isEmpty()`	Determina si el conjunto de estados está vacío. **Devuelve** `{Boolean}` "True" (verdadero) si el conjunto está vacío.
`size()`	Indica el número de indicadores de estado en el conjunto. **Devuelve** `{Number}` El número de estados.
`toArray()`	Convierte el conjunto de estados interno en una matriz. **Devuelve** `{Object []}` Matriz de indicadores de estado del conjunto.
`toString()`	Convierte el conjunto de estados interno en una cadena. **Devuelve** `{String}` Nombres delimitados por espacios de indicadores de estado en el conjunto.
`forEach(callback, thisArg)`	Función para iterar sobre cada elemento en el conjunto de estados. **Parámetros** `{forEachCallback}` Devolución de llamada para realizar la operación específica. Se llama con el nombre de cada estado en el conjunto.
`forEachCallback(string, thisArg)`	Una función de devolución de llamada suministrada por el usuario en la que se proporciona el comportamiento que se utilizará como parámetro de devolución de llamada a forEach. **Parámetros** `{String} String` El nombre de un estado en el conjunto de estado. `{Object}thisArg` Puntero opcional a un objeto de contexto.

5.8.22 Interfaz de usuario

El objeto de interfaz de usuario provee funciones para interactuar con el usuario, para preguntar por información básica y visualizarla. El objeto UI está disponible automáticamente en su macro como la variable “ui”.

> **Nota**
>
> **Importante:** Todas las funciones de UI requieren la palabra clave «yield» delante de ellas. Esto permite bloquear la ejecución de la macro hasta que se cumplan las condiciones para la función UI.
> `[parameter]` denota un parámetro opcional.

Método	Descripción
`prompt(message, [defaultAnswer], [mask])`	Se pregunta al usuario por información en la interfaz de usuario. **Parámetros** `{String} Título del mensaje que se mostrará al usuario` . Por defecto: cadena vacía. `{String} Respuesta por defecto que se utilizará si el usuario la deja en blanco` . Valor por defecto: cadena en blanco `{Boolean} La máscara indica si se debe ocultar la solicitud` (como con una contraseña). **Devuelve** `{Promise}` Se cumple si el usuario cierra la ventana del diálogo. Devuelve la entrada del usuario con “OK” o cero con “Cancel”.

`message([message])`	Muestra un mensaje en la interfaz de usuario.
	Parámetros
	`{String} Mensaje que se mostrará al usuario. Por defecto: cadena vacía.`
	Devuelve
	`{Promise} Se cumple cuando el usuario cierra la ventana del mensaje.`

5.8.23 Wait

Utilice el objeto wait para esperar una sesión particular o un estado de pantalla. Por ejemplo, puede esperar hasta que el cursor se encuentre en una posición particular o hasta que haya texto presente en una posición determinada antes de continuar con la ejecución de la macro.

Las funciones de espera se utilizan frecuentemente en combinación con funciones asíncronas como connect() y sendKeys().

Nota

Todas las funciones tienen tiempo límite como parámetro opcional y tienen un valor de tiempo límite por defecto de 10 segundos (10 000 ms).
Importante: Todas las funciones de espera requieren la clave 'yield' enfrente de ellas. Esto permite bloquear la ejecución de la macro hasta que se cumplan las condiciones para la función de espera.
`[parameter]` denota un parámetro opcional.

Método	Descripción
`setDefaultTimeout(timeout)`	Establece el valor de tiempo límite por defecto para todas las funciones. **Parámetros** `{Number}` Tiempo límite por defecto que se utilizará para todas las funciones de espera en milisegundos. **Devuelve** `{None}` **Genera** `{RangeError}` Si el tiempo límite especificado es inferior a cero.
`forConnect([timeout])`	Espera una solicitud de conexión para completar. **Parámetros** `{Number}` Tiempo en milisegundos. **Devuelve** `{Promise}` Se cumple si la sesión ya está conectada o cuando se realiza la conexión. Rechazada si expira el tiempo de espera.
`forDisconnect([timeout])`	Espera una solicitud de desconexión para completar. **Parámetros** `{Number}` Tiempo límite en milisegundos. **Devuelve** `{Promise}` Se cumple si la sesión ya está desconectada o cuando al fin se desconecta. Rechazada si expira el tiempo de espera.
`forFixedTime([timeout])`	Espera de forma incondicional un tiempo fijo. Tiempo en milisegundos (ms). **Parámetros** `{Number}` Tiempo límite en milisegundos. **Devuelve** `{Promise}` Se cumple una vez transcurrido el tiempo.
`forScreenChange([timeout])`	Espera a que cambie la pantalla de host. Esta función se devuelve cuando se detecta una actualización de pantalla. No ofrece garantías sobre el número de actualizaciones posteriores que pueden recibirse antes de que se complete la pantalla. Es aconsejable esperar repetidamente hasta que el contenido de la pantalla coincida con algunos criterios de detención conocidos.) **Parámetros**

	`{Number}` Tiempo límite en milisegundos. **Devuelve** `{Promise}` Se resuelve si la pantalla cambia. Rechazada si expira el tiempo de espera.
`forCursor(position, [timeout])`	Espera a que el cursor llegue a la posición especificada. **Parámetros** `{Position}` La posición que especifica la fila y la columna. **Devuelve** `{Promise}` Se cumple si el cursor ya se ha ubicado o si se ubica finalmente. Rechazada si expira el tiempo de espera.
`forText(text, position, [timeout])`	Espera a que el texto se encuentre en una posición específica de la pantalla. **Parámetros** `{String}` El texto previsto. `{Position}` La posición que especifica la fila y la columna. `{Number}` Tiempo límite en milisegundos. **Devuelve** `{Promise}` Se cumple si el texto ya se encuentra en la posición especificada o en cualquier otra ubicación. Rechazada si expira el tiempo de espera. **Genera** `{RangeError}` Si la posición no es válida.
`forHostPrompt(text, column, [timeout])`	Espera a que un símbolo de sistema esté colocado en una columna específica de la pantalla. **Parámetros** `{String}` Solicitud de texto prevista. `{Number}` Columna en la que se espera que se encuentre el cursor. `{Number}` Tiempo límite en milisegundos. **Devuelve** `{Promise}` Se cumple si ya se dan las condiciones o cuando al fin se dan. Rechazada si expira el tiempo de espera. **Genera** `{RangeError}` Si la columna está fuera del rango.
	NOTA: `wait.forHostSettle` solo debe utilizarse cuando otras funciones de espera adicionales

`forHostSettle([settleTime], [timeout])`	específicas son insuficientes. Supervisa los datos entrantes de la pantalla; resuelve settleTime ms tras la última actualización **y** cuando el teclado está desbloqueado. Esta función es útil cuando los datos llegan en varios paquetes y desea asegurarse de que se ha recibido toda la pantalla antes de continuar. **Parámetros** `{Number}` Tiempo que se esperará después de la última actualización para asegurarse de que no se reciban datos de forma inesperada. El valor por defecto es 200 milisegundos. `{Number}` tiempo de espera en milisegundos. **Devuelve** `{Promise}` Se cumple cuando ha transcurrido el tiempo de establecimiento tras la recepción de la última actualización de la pantalla y el teclado está desbloqueado.

5.9 Ejemplos de Macros

Para ayudarle a crear correctamente macros que se beneficien de todas las funciones del Editor de macros, dispone de estos ejemplos como punto de partida.

5.9.1 Interacción Básica con el Host

Este ejemplo muestra la interacción básica con el host, incluyendo:

- Enviar datos al host
- Esperar pantallas a mostrar
- Utilizar la palabra clave `yield` para esperar funciones asíncronas
- Leer texto de la pantalla
- Mostrar información básica al usuario
- Tratamiento de errores básicos

Todas las macros tienen disponibles los siguientes objetos de forma predeterminada:

1. **session**: punto de entrada principal para acceder al host. Puede conectar, desconectar y facilitar acceso al PresentationSpace.

   El objeto PresentationSpace obtenido de la sesión representa la pantalla y proporciona muchas funciones comunes, como obtener y establecer la ubicación del cursor, enviar datos al host y leer de la pantalla.

2. **wait**: facilita una forma sencilla de esperar a varios estados del host antes de seguir enviando más datos o leer de la pantalla.

3. **UI**: ofrece funciones básicas de interfaz de usuario. Muestra datos al usuario o le pide información.

```
// Función Crear una nueva macro
var macro = createMacro(function*(){
'use strict';

// Todas las macros tienen disponibles los siguientes objetos de forma predeterminada:
// 1. session - Punto de entrada principal para acceder al host. Puede conectar, desconectar y
facilitar acceso al PresentationSpace.
//    El objeto PresentationSpace obtenido de la sesión representa la pantalla y provee capacidades
muy comunes como obtener y ajustar la
//    posición del cursor, enviar datos al host y leer de la pantalla.
// 2. wait - Facilita una forma sencilla de esperar a varios estados del host antes de seguir
enviando más datos o leer de la pantalla.
// 3. uiI - Provee capacidades básicas de interfaz de usuario. Mostrar datos al usuario o pedirle
información.

// Declarar una variable para leer y visualizar algunos datos de pantalla.
// La mejor práctica es declarar todas las variables cerca de la parte superior de una función.
var numberOfAccounts = 0;

// Iniciar obteniendo el objeto PresentationSpace, que provee muchas operaciones de pantalla
comunes.
var ps = session.getPresentationSpace();

try {
    // Puede ajustar y obtener la posición del cursor
    ps.setCursorPosition(new Position(24, 2));

    // Utilizar la función sendKeys para enviar caracteres al host
    ps.sendKeys('cics');

    // SendKeys se utiliza también para enviar teclas de host como teclas PA y PF.
    // Véase "Control Keys" en la documentación para todas las opciones disponibles
    ps.sendKeys(ControlKey.ENTER);

    // Esperar a que el cursor se encuentre en la posición correcta.
    // El objeto wait provee varias funciones para esperar a que ocurran determinados estados
    // de modo que usted pueda proceder o bien a enviar más teclas, o bien a leer datos de la
pantalla.
    yield wait.forCursor(new Position(24, 2));

    // Puede mezclar caracteres y teclas de control en una llamada sendKeys.
    ps.sendKeys('data' + ControlKey.TAB + ControlKey.TAB + 'more data' + ControlKey.ENTER);

    // La palabra clave "yield" se debe utilizar enfrente de todas las llamadas de función "wait" y
"ui".
    // Le dice al navegador que detenga la ejecución de la macro hasta que la
    // función wait (asíncrona) vuelva. Consulte la documentación para saber qué funciones
    // requieren la palabra clave yield.
    yield wait.forCursor(new Position(10, 26));
    ps.sendKeys('accounts' + ControlKey.ENTER);

    // Puede esperar también a que aparezca un texto en ciertas áreas de la pantalla
    yield wait.forText('ACCOUNTS', new Position(3, 36)) ;
    ps.sendKeys('1' + ControlKey.ENTER);
```

```
    // Todas las funciones wait excederán el tiempo de espera si no se cumplen los criterios dentro
de un límite de tiempo.
    // Puede incrementar tiempos de espera con un parámetro opcional en las funciones wait (en
milisegundos)
    // Todos los tiempos de espera se especifican en milisegundos y el valor predeterminado es 10
segundos (10000 ms).
    yield wait.forCursor(new Position(1, 1), 15000);
    ps.sendKeys('A' + ControlKey.ENTER);

    // PS proporciona la función getText para leer texto de la pantalla
    numberOfAccounts = ps.getText(new Position(12, 3), 5);

    // Utilizar el objeto ui para visualizar algunos datos de la pantalla
    ui.message('Número de cuentas activas: ' + numberOfAccounts);

    // La try / catch permite capturar todos los errores y notificarlos a una ubicación central
} catch (error) {
    // De nuevo, utilizamos el objeto ui para visualizar un mensaje que indica que se ha producido
un error
    yield ui.message('Error: ' + error.message);
}
//Fin Macro Generada
});

// Ejecutar la macro y devolver los resultados al Ejecutor de macros
// La instrucción return es necesaria, ya que la aplicación aprovecha
// esto para saber si la macro se ha ejecutado correctamente y cuándo ha finalizado
return macro();
```

5.9.2 Interacción con el usuario

Este ejemplo ilustra cómo utilizar los métodos API provistos para pedirle entradas al usuario o para alertarle con un mensaje.

```
var macro = createMacro(function*(){
  'use strict';

  // El objeto "ui" ofrece funciones para preguntar información al usuario y para mostrar información

  // Declarar variables para uso posterior
  var username;
  var password;
  var flavor;
  var scoops;

  //Inicio Macro Generada
  var ps = session.getPresentationSpace();

  try {
    // Pedir al usuario que ingrese su nombre de usuario y guardarlo en una variable.
    // Recuerde que la palabra clave 'yield' es necesaria para bloquear la ejecución mientras se espera a la entrada del usuario.
    username = yield ui.prompt(‘Introduzca su nombre de usuario');

    // Pide al usuario ingresar un valor predeterminado que se le ha facilitado.
    flavor = yield ui.prompt('¿Cuál es su helado favorito?', 'Chocolate');

    // Pide al usuario ingresar información privada cuando se utiliza la opción 'mask' y el campo de entrada se enmascarará mientras escribe.
    // Si el parámetro no se utiliza, se puede utilizar 'cero' para especificar que no se desea utilizar.
    // Aquí lo ilustramos especificando que no necesitamos mostrar un valor predeterminado.
    password = yield ui.prompt('Introduzca su contraseña', null, true);

    // La función de preguntar devuelve cero si el usuario hace clic en el botón 'Cancelar' en lugar de en el botón 'Aceptar'.
    // Una forma de tratar este caso es ajustar la llamada a un bloque try/catch.
    scoops = yield ui.prompt('¿Cuántas cucharadas quiere?');
    if (scoops === null) {
      // Se sale de la macro.
      return;
      // Alternativamente podría arrojar un Error y capturarlo en el "catch" situado a continuación
     }
     // Utilizar los valores coleccionados para pedir nuestro ice cream
    ps.sendKeys(username + ControlKey.TAB + password + ControlKey.ENTER);
    yield wait.forCursor(new Position(5, 1));
    ps.sendKeys(flavor + ControlKey.TAB + scoops + ControlKey.ENTER);

     // Mostrar un mensaje al usuario. Utilizando la palabra clave 'yield' enfrente de la llamada bloquea
     // la ejecución de la macro hasta que el usuario hace clic en el botón 'Aceptar'.
    yield ui.message('Orden correcta. Enjoy your ' + scoops + ' scoops of ' + flavor + ' ice cream ' + username + '!');
    } catch (error) {
     // Aquí utilizamos el objeto ui para mostrar un mensaje de que ha ocurrido un error
    yield ui.message(error.message);
    }
```

```
    //Fin Macro Generada

});

return macro();
```

5.9.3 Navegar Por Datos

Este ejemplo explica cómo navegar por un número variable de pantallas y procesar los datos en cada pantalla.

```
 // Función Crear una nueva macro.
var macro = createMacro(function*(){
  'use strict';

  // Crear variable(s) para uso posterior
  var password;
  var accountNumber;
  'var transactionCount = 0;
  var row = 0;

  // Obtener una referencia para el objeto PresentationSpace.
  var ps = session.getPresentationSpace();

  try {
    // Introducir nombre de usuario y contraseña para iniciar sesión en la aplicación.
    yield wait.forCursor(new Position(19, 48));
    ps.sendKeys('bjones' + ControlKey.TAB);

    yield wait.forCursor(new Position(20, 48));
    password = yield ui.prompt('Contraseña:', null, true);
    ps.sendKeys(password);
    ps.sendKeys(ControlKey.ENTER);

    // Introducir un comando de aplicación.
    yield wait.forCursor(new Position(20, 38));
    ps.sendKeys('4');
    ps.sendKeys(ControlKey.ENTER);

    // Ir a la lista de transacciones para una lista.
    yield wait.forCursor(new Position(13, 25));
    ps.sendKeys('2');
    // Ingresar un número de cuenta. Codificación fija aquí para simplificar.
    yield wait.forCursor(new Position(15, 25));
    accountNumber = yield ui.prompt('Número de cuenta:', '167439459');
    ps.sendKeys(accountNumber);
    ps.sendKeys(ControlKey.ENTER);

    // Esperar hasta que esté en pantalla de perfil de cuenta
    yield wait.forText('ACCOUNT PROFILE', new Position(3, 33));

    // Buscar texto que indique que la última página de la grabación se ha alcanzado mientras
    while (ps.getText(new Position(22, 12), 9) !== 'LAST PAGE') {

      // Mientras que la página de la grabación no se haya alcanzado, ir a la siguiente página de grabaciones.
      ps.sendKeys(ControlKey.PF2);
      yield wait.forCursor(new Position(1, 1));

      // Si la posición del cursor no cambia entre las pantallas de grabación y no hay texto
      // en la pantalla, puede verificar si una pantalla se ha actualizado, puede esperar durante un
      // periodo de tiempo fijo después de que una tecla de ayuda haya sido enviada hasta el establecimiento de la pantalla.
      // Por ejemplo:
      // yield wait.forFixedTime(1000);

      // Para cada una de las pantallas, incremente la variable de recuento si contiene datos.
      for (row = 5; row <= 21; row++) {

        // Hay 2 columnas en la pantalla. Comprobar datos en columna 1.
        // En este ejemplo, sabemos que si hay un espacio en una posición
        // específica, se trata de una transacción.
        if (ps.getText(new Position(row, 8), 1) !== ' ') {
          transactionCount++;
        }
        // Comprobar datos en columna 2.
        if (ps.getText(new Position(row, 49), 1) !== ' ') {
          transactionCount++;
        }
      }
    }

    // Después de haber pasado por todas las páginas de grabación, mostrar el número de grabaciones en un cuadro de mensaje.
    yield ui.message('Encontradas ' + transactionCount + ' grabaciones para cuenta ' + accountNumber + '.');

    // Salir de la aplicación
    ps.sendKeys(ControlKey.PF13);
    ps.sendKeys(ControlKey.PF12);

    // La try / catch permite capturar todos los errores y notificarlos a una ubicación central
  } catch (error) {
    // Aquí utilizamos el objeto ui para visualizar un mensaje que indica que se ha producido un error
    yield ui.message(error.message);
  }
```

```
});

// Aquí ejecutamos la macro y devolvemos los resultados al Ejecutor de macros
// La instrucción return es necesaria, ya que la aplicación aprovecha
// esto para saber si la macro se ha ejecutado correctamente y cuándo ha finalizado
return macro();
```

5.9.4 Invocar un Servicio Web

Este ejemplo explica cómo realizar una llamada AJAX / REST desde una macro a un servicio web. Puede integrar datos desde su aplicación de host a la llamada del servicio web o desde el servicio web a su aplicación de host.

En este ejemplo llamamos el servicio Verastream Host Integrator (VHI) CICSAcctsDemo REST. En cualquier caso, puede adaptar fácilmente el código para llamar cualquier servicio web. No está limitado a VHI.

En el ejemplo, la llamada va a través de un proxy configurado en el servidor de sesión (mostrado más abajo) para evitar una complicación del tipo "Same Origin Policy" (Directiva del mismo origen). Si está utilizando un servicio web que soporte Cross-origin Resource Sharing (CORS) y está utilizando un navegador moderno, el proxy es innecesario.

Como la biblioteca jQuery está disponible en las macros, puede utilizar la función $.post() directamente para invocar servicios REST.

Este ejemplo explica también cómo ajustar una llamada jQuery REST en una nueva Promise. La promise devuelta por la función personalizada siguiente permite utilizar "yield" en el código de la macro principal. Esto permite que la ejecución de la macro espere hasta que la llamada de servicio se complete antes de continuar.

```
var macro = createMacro(function*() {
 'use strict';

 // Crear unas cuantas variables para usuario posterior
 var username;
 var password;
 var accountNumber;
 var accountDetails;

 // Crear una función que hará una llamada AJAX / REST a un servicio web VHI.
 // Se podría ajustar para llamar cualquier servicio web, no sólo VHI.
 // Si no se utiliza CORS, la solicitud tendría que pasar por un
 // proxy en el servidor de sesión. Véanse notas de ejemplo para más información.
 /**
  * Función de auxiliar de cifrado manual para encapsular parámetros AJAX / REST, invocar el servicio
  * REST y devolver los resultados dentro de una Promise.
  * @param {Number} acctNum para enviar a la consulta REST.
  * @param {String} nombre de usuario para acceder al servicio REST.
  * @param {String} contraseña para acceder al servicio REST.
  * @return {Promise} que contiene resultados $.post() compatibles con yield.
  */
 var getAccountDetails = function (acctNum, username, password) {
   var url = "proxy1/model/CICSAcctsDemo/GetAccountDetail";
   var args = {"filters": {"AcctNum": acctNum}, "envVars": {"Username": username, "Password": password}};

   // Ajustar una llamada jQuery AJAX / HTTP POST en una nueva Promise.
   // La promise que se devuelve aquí permite a la macro yield / esperar
   // hasta que se complete.
   return Promise.resolve($.post(url, JSON.stringify(args)))
     .catch(function (error) {
     // Se han producido errores de asignación en la llamada jQuery a nuestra Promise.
     throw new Error('REST API Error: ' + error.statusText);
   });
 };

 // Inicio Macro Generada
 var ps = session.getPresentationSpace();
 try {
   // Podría interactuar con el host aquí, iniciar sesión en app de host, etc...
   // Recuperar nombre de usuario y contraseña
   username = yield ui.prompt('Nombre de usuario:');
   password = yield ui.prompt('Contraseña:', null, true);
   accountNumber = yield ui.prompt('Número de cuenta:');
```

```
    if (!username || !password || !accountNumber) {
      throw new Error('Username or password not specified');
    }

    // Invocar servicio REST externo, y yields / esperar a que se complete la llamada.
    accountDetails = yield getAccountDetails(accountNumber, username, password);

    // Ahora tenemos los datos de nuestro servicio externo.
    // Puede integrar los datos en nuestra app de host local o simplemente mostrarlos al usuario.
    // En este ejemplo sólo mostramos los detalles de la cuenta resultantes.
    if (accountDetails.result && accountDetails.result.length > 0) {
      yield ui.message(accountDetails.result[0].FirstName + ' $' + accountDetails.result[0].AcctBalance);
    } else {
      yield ui.message('Ninguna grabación encontrada para cuenta: ‘ + accountNumber);
    }
  } catch (error) {
    // Si se ha producido un error durante la llamada AJAX / REST call
    // o la recuperación del nombre de usuario / contraseña terminaremos aquí.
    yield ui.message(error.message);
  }
});

// Ejecutar nuestra macro
return macro();
```

Cross Origin Scripting Proxy Support

Si tiene servicios web que no admiten CORS, las llamadas a AJAX/REST presentarán errores si intentan acceder a un servidor distinto a aquel en el que se originó la aplicación Host Access for the Cloud. Esta es una función de seguridad del navegador.

El servidor de Host Access for the Cloud proporciona un método explícito para establecer un proxy en servidores remotos de confianza.

- Abra `..\<directorio_de_instalación>\sessionserver\microservice\sessionserver\service.yml` para editarlo.
- En la sección `env`, agregue:

  ```
  nombre: zfe.proxy.mappings
  value: proxy-path=proxy-to-address
  ```

  Donde `proxy-path` hace referencia a la asignación de URL y `proxy-to-address` hace referencia a la URL en la que se redirigirá mediante proxy la llamada.
- En este ejemplo:

  ```
  nombre: zfe.proxy.mappings
  value: proxy1=http://remote-vhi-server:9680/vhi-rs/
  ```

  Las llamadas realizadas a `<servidor:puerto>/proxy1` se redirigirán mediante apoderado (proxy) a `http://remote-vhi-server:9680/vhi-rs/`.
- Se pueden especificar varias asignaciones de proxy utilizando una coma para separar las asignaciones de proxy individuales.
- Recuerde que incluso si un servidor REST soporta encabezados CORS, algunos navegadores antiguos pueden no soportarlos, por lo que este ejemplo sigue siendo relevante.

> **Sugerencia**
>
> Es posible que el archivo `service.yml` se sustituya cada vez que distribuya de nuevo Host Access for the Cloud. Haga siempre una copia de seguridad de sus archivos.

5.9.5 Trabajar con celdas de datos y atributos

Esta macro explica cómo usar DataCells y AttributeSet para inspeccionar una fila/columna en la pantalla para texto y atributos. En este ejemplo puede ver:

- Cómo obtener una colección de DataCells para una posición y longitud dadas.
- Cómo iterar por DataCells para formar una cadena de texto
- Para comparar, cómo puede hacer algo similar utilizando getText().
- Y finalmente, cómo trabajar con atributos, obtener un listado de cadenas o determinar si cadenas específicas están colocadas en una posición dada de la pantalla.

```
var macro = createMacro(function*() {
    'use strict';

    // Obtener PresentationSpace para interactuar con el host
    var ps = session.getPresentationSpace();

    // Declarar variables para uso posterior
    var cells;
    var text;
    var attrs;

    // Establecer el tiempo de espera predeterminado para las funciones "wait"
    wait.setDefaultTimeout(10000);

    // Macro de ejemplo para trabajar con DataCells y Attributes
    try {
        yield wait.forCursor(new Position(24, 2));

        // Obtener DataCells del espacio de presentación.
        // Fila 19, col 3 es la pregunta, 35 caracteres de longitud
        // "Seleccionar de los siguientes comandos:"
        cells = ps.getDataCells({row:19, col:3}, 35);
        text = '';

        // Puede visualizar texto utilizando getText
        yield ui.message("Screen text: " + ps.getText({row:19, col:3}, 35));

        // O puede ensamblar el texto de las DataCells en cada posición
        for(var index = 0; index < cells.length; index++) {
            text = text.concat(cells[index].getChar());
        }
        // Y visualizar el texto
        yield ui.message("Cells text: " + text);

        // Obtener los atributos de la primera DataCell (cell[0])
        attrs = cells[0].getAttributes();

        // Muestra si hay o no atributos en la celda de datos
        yield ui.message("Conjunto de atributos vacío: " + attrs.isEmpty());

        // Muestra cuántos atributos están configurados
        yield ui.message("Número de atributos: " + attrs.size());

        // Muestra qué atributos están configurados
        yield ui.message("Atributos: " + attrs.toString());

        // Mostrar ahora si el atributo de alta intensidad está configurado
        yield ui.message("Es de alta intensidad: " +
                         attrs.contains(Attribute.HIGH_INTENSITY));

        // Mostrar ahora si el atributo subrayado está configurado
        yield ui.message("Es subrayado: " +
                         attrs.contains(Attribute.UNDERLINE));

        // Mostrar ahora si los atributos alfanumérico, intensificado y detectable por lápiz están configurados
        yield ui.message("Es alfanumérico, intensificado y detectable por lápiz: " +
                         attrs.containsAll([Attribute.ALPHA_NUMERIC, Attribute.HIGH_INTENSITY, Attribute.PEN_DETECTABLE]));

        // Mostrar ahora si los atributos alfanumérico, intensificado y detectable por lápiz están configurados
        yield ui.message("Es alfanumérico, intensificado y detectable por lápiz: " +
```

```
                        attrs.containsAll([Attribute.UNDERLINE, Attribute.HIGH_INTENSITY, Attribute.PEN_DETECTABLE]));
    } catch (error) {
        yield ui.message(error);
    }
    //Fin Macro Generada
});

// Ejecutar la macro
return macro();
```

5.9.6 Utilizar Campos y Listas de Campos

Este ejemplo de macro explica cómo utilizar funciones comunes para interactuar con los campos de la Macro API. Por ejemplo, cómo obtener texto de campo, ver información de campo y utilizar field.setText como alternativa a sendKeys para interactuar con el host.

> **Nota**
>
> Debido a las consideraciones del navegador, `ui.message` contrae cadenas de espacios a un solo espacio. Los espacios se preservan en el JavaScript actual.

```
var macro = createMacro(function*() {
    'use strict';

    // Obtener PresentationSpace para interactuar con el host
    var ps = session.getPresentationSpace();

    // Declarar variables para uso posterior
    var fields;
    var field;
    var searchString = 'z/VM';

    // Establecer el tiempo de espera predeterminado para las funciones "wait"
    wait.setDefaultTimeout(10000);

    // Macro de ejemplo para trabajar con FieldList y Fields
    try {
    yield wait.forCursor(new Position(24, 2));

    // Obtener la lista de campos.
    fields = ps.getFields();

        // Ejecutar en toda la lista de campos y mostrar la información del campo.
        for(var index = 0; index < fields.size(); index++) {
            field = fields.get(index);

            yield ui.message("Field " + index + " info: " + field.toString());
        }

        yield ui.message("Ahora, encontrar un campo que contenga el texto '" + searchString + "'");
        field = fields.findField(new Position(1, 1), searchString);

        if(field !== null) {
            yield ui.message("Found field info: " + field.toString());
            yield ui.message("¿Encontrado primer plano de campo es verde? " + (Color.GREEN === field.getForegroundColor()));
            yield ui.message("¿Encontrado primer plano de campo es predeterminado? " + (Color.BLANK_UNSPECIFIED ===
field.getBackgroundColor()));
        }

        // Ahora, encontrar campo de comando y modificarlo.
        field = fields.findField(new Position(23, 80));
        if(field !== null) {
             field.setText("cics");
        }

        yield ui.message("Clic para enviar 'cics' al host.");
        ps.sendKeys(ControlKey.ENTER);

        // Esperar a nueva pantalla; obtener nuevos campos.
        yield wait.forCursor(new Position(10, 26));
        fields = ps.getFields();

        // Encontrar campo de usuario y configurarlo.
        field = fields.findField(new Position(10, 24));
        if(field !== null) {
            field.setText("myusername");
        }

        // Encontrar campo de contraseña y configurarlo.
        field = fields.findField(new Position(11, 24));
        if(field !== null) {
            field.setText("mypassword");
        }
```

```
        yield ui.message("Clic para enviar inicio de sesión al host.");
        ps.sendKeys(ControlKey.ENTER);

        // Esperar a nueva pantalla; obtener nuevos campos.
        yield wait.forCursor(new Position(1, 1));
        fields = ps.getFields();

        // Encontrar campo de comando y configurar comando logoff.
        field = fields.findField(new Position(24, 45));
        if(field !== null) {
            field.setText("cesf logoff");
        }

        yield ui.message("Clic para enviar logoff al host.");
        ps.sendKeys(ControlKey.ENTER);

    } catch (error) {
        yield ui.message(error);
    }
    //Fin Macro Generada
});

// Ejecutar la macro
return macro();
```

5.9.7 Macro Sign-On automático para Mainframes

En este ejemplo se utiliza el objeto AutoSignon para crear una macro que utiliza las credenciales asociadas a un usuario para obtener un ticket de paso del Digital Certificate Access Server (servidor de acceso a certificados digitales, DCAS).

```
var macro = createMacro(function*() {
    'use strict';

    // Obtener PresentationSpace para interactuar con el host
    var ps = session.getPresentationSpace();

    // Variable para ticket de paso de inicio de sesión
    var passTicket;

    // ID de inicio de sesión en aplicación
    var appId = 'CICSV41A';

    // Establecer el tiempo de espera predeterminado para las funciones "wait"
    wait.setDefaultTimeout(10000);

    // Inicio Macro Generada
    try {
        yield wait.forCursor(new Position(24, 2));

        // Obtener un ticket de paso de DCAS.
        passTicket = yield autoSignon.getPassTicket(appId);

        ps.sendKeys('cics');
        ps.sendKeys(ControlKey.ENTER);

        yield wait.forCursor(new Position(10, 26));

        // Sustituir nombre de usuario generado por sendUserName(passTicket) ...
        yield autoSignon.sendUserName(passTicket);

        // ps.sendKeys('bvtst01' + ControlKey.TAB + ControlKey.TAB);
        ps.sendKeys(ControlKey.TAB + ControlKey.TAB);

        yield wait.forCursor(new Position(11, 26));

        // Sustituir contraseña generada por sendPassword(passTicket) ...
        yield autoSignon.sendPassword(passTicket);

        // var userInput3 = yield ui.prompt('Contraseña:', '', true);
        // if (userInput3 === null) {
            // throw new Error('Password not provided');
        // }
        // ps.sendKeys(userInput3);
        ps.sendKeys(ControlKey.ENTER);

        yield wait.forCursor(new Position(1, 1));
        yield ui.message('Logged in. Log me off.');
        ps.sendKeys('cesf logoff');
        ps.sendKeys(ControlKey.ENTER);
    } catch (error) {
        yield ui.message(error);
    }
    //Fin Macro Generada
});

// Ejecutar la macro
return macro();
```

5.9.8 Utilizar Transferencia de Archivos (IND$File)

Esta serie de ejemplos de macros demuestra cómo utilizar la API de transferencia de archivos para recuperar una lista de archivos, descargar un archivo y cargar un archivo a un host 3270.

> **Nota**
>
> Debe haber iniciado sesión y tener una indicación de sistema abierta antes de ejecutar estas macros.

List archivos

Esta macro muestra cómo utilizar la API de transferencia de archivos para recuperar una lista de archivos de un host 3270 utilizando la transferencia IND$File. El objeto de transferencia IND$File se recupera de la transferencia de archivos de fábrica y se utiliza para obtener una matriz de objetos HostFile de TSO o de CMS.

```
var macro = createMacro(function*() {
    'use strict';

    try {
        var fileTransfer = fileTransferFactory.getInd$File();
        var hostFiles = yield fileTransfer.getHostFileListing();

        yield ui.message('Found ' + hostFiles.length + ' files');
        if (hostFiles.length > 0) {
            var firstFile = hostFiles[0];
            var msg1 = 'El nombre del catálogo es ' + firstFile.getParent() + '. ';
            var msg2 = 'The first file is ' + firstFile.getName();
            yield ui.message(msg1 + msg2);
        }
    } catch (error) {
        yield ui.message(error);
    }
});

// Run the macro
return macro();
```

Descargar archivo

Esta macro muestra cómo utilizar la API de transferencia de archivos para descargar un archivo de un host 3270 utilizando la transferencia IND$File. El objeto de transferencia IND$File se recupera de la transferencia de archivos de fábrica. En este ejemplo, el método de transferencia se ha definido en ASCII para mostrar el uso de la función setTransferOptions.

La macro de ejemplo descarga el primer archivo devuelto desde una llamada a getHostFileListing, lo que crea un URI de descarga con una llamada a la función getDownloadUrl. La macro se puede utilizar en un entorno CMS o TSO, pero la opción debe especificarse en la primera línea o el código debe modificarse ligeramente para el sistema previsto.

```
var hostEnvironment = 'CMS';  // 'TSO'
// Construct file path, ie catalog/file.name or catalog/partition/file
```

```
function getPath (fileNode) {
    var prefix = fileNode.getParent() ? fileNode.getParent() + '/' : '';
    return prefix + fileNode.getName();
}

var macro = createMacro(function*() {
    'use strict';

    try {
        var fileTransfer = fileTransferFactory.getInd$File();

        // Las opciones de transferMethod son 'binario' y 'ascii'
        fileTransfer.setTransferOptions({transferMethod: 'ascii'});

        // Esta demostración recupera el primer archivo devuelto en la lista
        var hostFiles = yield fileTransfer.getHostFileListing();
        var firstHostFile = hostFiles[0];

        if (hostEnvironment === 'CMS') {
           yield wait.forText('Ready', new Position(1,1), 5000);
        }

        // Download
        // Si ya conoce la ruta al archivo que desea, pásela a getDownloadURL()
        var downloadUrl = fileTransfer.getDownloadURL(getPath(firstHostFile));

        // Esto cambia la ubicación del navegador. Puede obtener resultados diferentes en navegadores diferentes
        window.location = downloadUrl;

        // Si desea leer el contenido del archivo en una variable en lugar de descargarlo,
        // puede utilizar jQuery
        // var fileContents = yield $.get(downloadUrl);

    } catch (error) {
        yield ui.message(error);
    }
});

// Run the macro
return macro();
```

Cargar archivo

Esta macro muestra cómo utilizar la API de transferencia de archivos para cargar un archivo a un host 3270 utilizando la transferencia IND$File. Esta macro de ejemplo pide al usuario seleccionar un archivo del sistema de archivos local activando el diálogo de selección de archivos del navegador. Éste recupera el catálogo actual en TSO o identificador de unidad en CMS llamando getHostFileListing. Por último, se llama a la función sendFile para entregar el archivo local seleccionado al host.

La macro se puede utilizar en un entorno CMS o TSO, pero la opción debe especificarse en la primera línea. En este ejemplo, el método de transferencia está ajustado a **ascii**; si lo desea, puede cambiarlo a **binario**.

```
var hostEnvironment = 'CMS';  // 'TSO'
// Abre la función programada de diálogo de selección de archivos del navegador
function promptForFileToUpload () {
    return new Promise(function (resolve, reject) {
        // No se nos notifica si el usuario camcela el ciálogo selector de archivos, por tanto se rechaza después de 30 segundos
        var timerId = setTimeout(reject.bind(null, 'Tiempo de espera agotado esperando la selección del archivo'), 30000);
        var fileSelector = document.createElement('input');
        fileSelector.setAttribute('type', 'file');
        fileSelector.onchange = function (evt) {
            var file = evt.target.files[0];
            clearTimeout(timerId);
            resolve(file);
        };
        fileSelector.click();
    });
}

var macro = createMacro(function*() {
    'use strict';

    try {
        var fileTransfer = fileTransferFactory.getInd$File();

        // Las opciones de transferMethod son 'binario' y 'ascii'
         fileTransfer.setTransferOptions({transferMethod: 'ascii'});

         var localFile = yield promptForFileToUpload();

         // Recuperar el catálogo actual y añadirle el nombre de archivo seleccionado
```

```
          var hostFiles = yield fileTransfer.getHostFileListing();
          var destination = hostFiles[0].getParent() + '/' + localFile.name;

          if (hostEnvironment === 'CMS') {
            yield wait.forText('Ready', new Position(1,1), 5000);
          }

          var result = yield fileTransfer.sendFile(localFile, destination);

      } catch (error) {
          yield ui.message(error);
      }
});

// Run the macro
return macro();
```

5.10 Ejecutar macro en evento

Utilice el panel Macro para seleccionar qué macros se deben ejecutar y para definir cuándo se deben ejecutar.

- Ejecutar macro al iniciar - Elija una macro para que se ejecute automáticamente cuando se abra la sesión.
- Ejecutar macro al conectar - Elija una macro para que se ejecute automáticamente cuando la sesión se conecte al host.
- Ejecutar macro al desconectar - Elija una macro para que se ejecute automáticamente cuando la sesión se desconecte al host.

Más información

- Crear Macros
- Utilizar la API de macros
- Ejemplos de Macros

5.11 Impresión

Existen varias opciones de impresión disponibles para los hosts 3270, 5250 y UTS. Puede realizar capturas de pantalla, imprimir una pantalla seleccionada y habilitar y configurar las funciones de impresión de host:

Los parámetros disponibles para usted para la configuración y la orientación de la página dependen de las opciones de su navegador.

5.11.1 Capturar una pantalla

Utilice la función de captura de pantalla para capturar múltiples pantallas y guardarlas como archivo para imprimirlas o compartirlas. Esta opción está disponible para todos los usuarios una vez que el administrador la selecciona utilizando **Preferencias del usuario**.

1. Vaya a la pantalla que desea capturar.
2. Haga clic en  para capturar la pantalla. El contador indica el número de capturas que ha hecho. Cada captura se imprimirá en una página aparte.
3. Haga clic en Guardar para navegar a la ubicación en la que desea guardar la captura. Su navegador determina cómo funciona la opción de guardar. Por ejemplo, en Chrome y dependiendo de los ajustes del navegador, el archivo se guarda en el archivo de descargas o usted ve un diálogo de Guardar como para seleccionar una ubicación para guardar el archivo de captura.
4. Para añadir las nuevas pantallas guardadas a un archivo de captura de pantalla existente, haga clic en **Añadir y guardar**. Al imprimir el archivo añadido, cada captura de pantalla se imprime en una página aparte.
5. Puede borrar las capturas en cualquier momento. Para ello, haga clic en **Borrar**.

5.11.2 Imprimir una pantalla

La opción de imprimir pantalla imprime el contenido de la pantalla del terminal. No imprime la barra de herramientas u otra información de pantalla.

1. Vaya a la pantalla que desea imprimir.
2. Haga clic en Imprimir Pantalla en la barra de herramientas.
3. Utilice el diálogo de impresión de su navegador para seleccionar la impresora y las opciones de configuración de página.

5.11.3 Impresión de host

Esta función está disponible para las sesiones de host 3270, 5250 y UTS. Puede crear una o más sesiones de impresora y asociarlas a la sesión de terminal actual. Cada sesión de impresora está enlazada a un ID de dispositivo en el sistema de host y cada trabajo de impresión posterior enviado a ese ID de dispositivo se enviará al cliente Web de Host Access for the Cloud.

La sesión de host genera un archivo PDF que contiene el archivo que se va a imprimir y lo envía al cliente Web. Después de recibir el archivo, el cliente Web lo descarga mediante las opciones de descarga configuradas en el navegador. Los diferentes navegadores ofrecen diferentes opciones para tratar los archivos descargados. Cuando se ha recibido el archivo PDF, puede enviarlo a cualquier impresora a la que usted tenga acceso.

> **Nota**
>
> Un administrador puede proporcionar a sus usuarios finales la capacidad de imprimir mediante la configuración de la opción de **Preferencias de Impresión de Host del Usuario**.

Para configurar la impresión de host

1. Desde una sesión de host, haga clic en **Configuración** en la barra de herramientas para abrir el panel de navegación izquierdo.
2. En el panel izquierdo haga clic en **Imprimir**.
3. Haga clic en **Agregar** para abrir el cuadro de diálogo de configuración. Personalice la sesión de impresora mediante la configuración de cada pestaña: Configuración de conexión, Configuración de página y Configuración avanzada.
4. Haga clic en **Guardar** para volver a su sesión. Los ajustes surten efecto cuando se vuelve a abrir la sesión.

Temas sobre impresión de host

- Configuración de conexión: 3270, 5250 y UTS
- Parámetros de Configuración de página
- Ajustes avanzados
- Para imprimir la sesión de impresora del host

Parámetros de conexión

De forma predeterminada, las sesiones de impresora están disponibles desde el icono de impresora de la barra de herramientas de la sesión de terminal. Si no desea que los usuarios finales tengan acceso a esta sesión de impresora, desactive **Habilitar esta sesión de impresora** en la ficha Conexión.

Estos parámetros varían en función del tipo de host.

- Parámetros de conexión 3270
- Parámetros de conexión 5250
- Parámetros de conexión UTS

PARÁMETROS DE CONEXIÓN 3270

Parámetro	Descripción
Nombre	Especifique un nombre para su sesión de impresora que sea fácil de identificar. Requerido.
Protocolo	Seleccione el protocolo que se utilizará. Las opciones son: • **TN3270E** - TN3270E o Telnet Extendido es para usuarios de software TCP/IP que se conectan a su mainframe IBM mediante un gateway Telnet que implementa RFC 1647. • **TN3287** - TN3287 es para usuarios de software TCP/IP que se conectan a su mainframe IBM mediante un gateway Telnet que implementa RFC 1646.
ID de dispositivo	Especifique si desea utilizar o solicitar un ID de dispositivo o, si ha seleccionado TN3270E, una Asociación TN, indique si desea vincular la sesión de terminal con la sesión de impresión. Requerido. Seleccione una de las siguientes opciones: • Especifique el ID de dispositivo: especifique el ID de dispositivo cuando la sesión de la impresora se conecte al host. • Utilizar Asociación TN - (TN3270E) Si decide utilizar una asociación TN, Host Access for the Cloud utiliza el nombre del dispositivo especificado en los parámetros de conexión para vincular las sesiones 3270 y 3287. La Asociación TN solo está disponible si selecciona TN3270E como protocolo. • Preguntar al usuario: cuando se conecta la sesión de la impresora, se le solicita al usuario que proporcione el ID de dispositivo de esa sesión.

PARÁMETROS DE CONEXIÓN 5250

Parámetro	Descripción
Nombre	Especifique un nombre para su sesión de impresora que sea fácil de identificar. Requerido.
ID de dispositivo	Especifique si desea utilizar un ID de dispositivo o una solicitud de un ID de dispositivo: • Especifique el ID de dispositivo: especifique el ID de dispositivo cuando la sesión de la impresora se conecte al host. • Preguntar al usuario: cuando se conecta la sesión de la impresora, se le solicita al usuario que proporcione el ID de dispositivo de esa sesión.

PARÁMETROS DE CONEXIÓN UTS

Parámetro	Descripción
Nombre	Especifique un nombre para su sesión de impresora que sea fácil de identificar. Requerido.
Protocolo	La selección de los protocolos DEMAND o MAPPER depende del tipo de sesión de UTS que se cree. Los tipos de sesión de UTS se determinan según los valores que se proporcionen para las opciones TSAP y Aplicación en el panel de conexión. Por ejemplo, si introduce valores que crean una sesión de MAPPER o DEMAND de UTS, debe seleccionar MAPPER o DEMAND como protocolo. Especifique el protocolo que se utilizará: • **MAPPER**: puede optar por especificar el ID de dispositivo que se utilizará cuando la sesión de la impresora se conecte al host o solicitar al usuario que proporcione el ID de dispositivo para la sesión de la impresora; a continuación, siga configurando la sesión. • **DEMAND**: después de proporcionar un nombre para la sesión, puede seguir configurando la sesión mediante las pestañas Configuración de página y Avanzado.

Parámetros de Configuración de página

La ficha Configuración de página contiene opciones de configuración para el tamaño y la orientación del papel, junto con las dimensiones, márgenes y valores de escala.

Parámetro	Descripción
Tamaño del papel	Seleccione el tamaño del papel utilizado por la impresora.
Orientación	Elija entre los tres modos: **Vertical**, **Horizontal** o **Auto**, que es el valor por defecto. Si se ha seleccionado Auto, la impresora evalúa el trabajo de impresión y utiliza el formato más apropiado.
Unidades de medidas	Seleccione la unidad de medida que desea utilizar para los márgenes y los tamaños de las páginas. Los valores son pulgadas o milímetros.
Dimensiones	Introduzca el número de filas y columnas a visualizar por página imprimida. El valor predeterminado para las filas es 60 y para las columnas, 80.
Márgenes	Ajusta los márgenes izquierdo, derecho, superior e inferior de la página.
Escala	Ajusta la escala horizontal y vertical para la salida de impresión. Aumente el porcentaje para aumentar el espacio horizontal o vertical utilizado en la salida de impresión.

Ajustes avanzados

Elija cuándo desea que se descargue el archivo PDF.

- **Automáticamente** - (predeterminada) El PDF se descarga automáticamente cuando el trabajo de impresión se ha completado. Cuando esta opción está seleccionada, el parámetro de tiempo de espera de inactividad no está disponible.
- **Manualmente** - Una vez que ha comenzado un trabajo de impresión, usted puede iniciar la descarga localizando el trabajo de impresión en la lista disponible desde del icono de impresión de la barra de herramientas y haciendo clic en Vaciar. El trabajo de impresión se agrega a un solo archivo PDF y se descarga.
- **Después de tiempo de espera de inactividad** - Con esta opción puede imprimir múltiples trabajos de impresión, agregarlos a un solo PDF y descargarlos automáticamente cuando usted especifique.

  Si se decide por un valor superior a 0 (por ejemplo, 5 segundos), cualquier trabajo de impresión asignado a una impresora que llegue en un tiempo de 5 segundos respecto a otro se agregará al mismo PDF. Después de 5 segundos sin trabajos de impresión restantes, el PDF se descarga.

  Si especifica 0 para el tiempo de espera de inactividad, cada trabajo de impresión se descarga inmediatamente después de completarse. Puede interrumpir un trabajo de impresión en cualquier momento haciendo clic en **Vaciar**.

Para imprimir la sesión de impresora del host

Cuando la sesión de terminal se abre, usted puede:

1. Seleccionar la sesión de impresora desee utilizar. Todas las sesiones de impresoras asociadas a la sesión de terminal abierta están disponibles para usted. Haga clic en  en la barra de herramientas para ver una lista.
2. La sesión de host recibe los datos de impresión del host y genera un archivo PDF para imprimir. Se envía un enlace a este archivo al cliente Web para indicar que se puede descargar.

   Puede supervisar los distintos trabajos de impresión utilizando el contador de páginas de la barra de herramientas o el contador asociado con impresoras separadas en la lista desplegable de impresión.

   El contador de páginas de la barra de herramientas refleja el número total de páginas que se están imprimiendo o completando activamente pero que están esperando a que el archivo se descargue del servidor. Puede iniciar una descarga seleccionando Vaciar de la lista de impresoras.

   El contador de páginas conectado a las impresoras en la lista desplegable de impresoras muestra el mismo valor pero por impresora. La suma de estos trabajos de impresión separados se refleja en el recuento de la barra de herramientas. El recuento se borra una vez descargados los trabajos de impresión.
3. Una vez que el archivo PDF está disponible, el archivo comienza a descargarse o espera a que usted inicie una descarga mediante la opción Vaciar, dependiendo de las opciones que haya configurado.

En caso necesario, debido a un trabajo de impresión de larga duración en curso o a otro problema, puede vaciar la tarea de impresión actual. La opción **Vaciar** está disponible en la lista de sesiones de impresora a la que se accede desde el icono de impresora de la barra de herramientas. Cuando usted vacía un trabajo de impresión, todo lo acumulado hasta entonces se imprime y el procesamiento de datos de impresión continúa.

6. Desarrollo

6.1 Desarrollo

Host Access for the Cloud incluye una colección de API y bibliotecas que le ayudan a desarrollar aplicaciones cliente/servidor y aplicaciones Web que integran los datos del host en diversos entornos de desarrollo.

También puede ampliar el cliente Web sin que esto afecte a los archivos instalados. Esta capacidad le proporciona una amplia gama de opciones para adaptar el cliente Web a sus propias necesidades.

- Con el SDK de Java, puede utilizar la API de Java suministrada para mejorar la presentación de datos de host mediante eventos del servidor.
- Con el Conector para Windows, puede interactuar con las sesiones de host en la aplicación .NET o en Visual Basic para aplicaciones mediante la API y los ejemplos proporcionados.
- Con la API de JavaScript, puede incrustar el cliente web en su propio sitio web.
- Al ampliar el cliente web, puede mejorar y aumentar el ámbito del cliente web mediante código personalizado como, por ejemplo, CSS o JavaScript.

Documentación de la API de HACloud

6.2 Uso del SDK de Java

Al trabajar con eventos del servidor y el SDK de Host Access for the Cloud puede proporcionar un código Java de procedimiento que puede ampliar y mejorar la presentación de los datos del host. Para ayudarle a crear eventos del servidor, Host Access for the Cloud incluye un SDK y ejemplos que pueden servirle como punto de partida.

Los Javadocs están disponibles en el directorio de instalación (`<directorio de instalación>\sessionserver\sdk\java\javadocs\index.html`), así como en línea aquí: Javadocs de HACloud.

1. Facilite el SDK de Host Access for the Cloud al entorno de desarrollo. El SDK está disponible en directorio-de-instalación\sessionserver\sdk.
2. Escriba el código Java necesario para realizar la tarea y compile el código en una clase de Java dentro de un archivo JAR (Java Archive).
3. Copie el archivo JAR en `<directorio-de-instalación>\sessionserver\microservices\sessionserver\extensions\server` y reinicie el servidor de sesión.

   Si tiene más de un servidor de sesión en el que desee ejecutar el evento, deberá copiar el archivo JAR a esta ubicación en cada servidor.
4. Agregue la sesión que desee asociar al evento en la Consola Administrativa.
5. Al configurar la sesión en el cliente web, abra el panel Personalización y escriba el nombre completo de clase para el evento.
6. Inicie la sesión y pruebe el evento.

6.2.1 Ejemplos y documentación

Para acceder a SDK para la visualización directa e importar a IDE:

1. Desplácese a `<directorio-de-instalación>\sessionserver\sdk\java`
2. En el directorio SDK, acceda a:

   - `\javadoc` : este directorio contiene archivos JavaDoc para visualizarlos directamente.
   - `\samples` - Este directorio contiene recursos de Java para visualización directa.
   - `\zfe-sdk.jar` - El archivo JAR contiene las clases de Java para importar a su IDE.
   - `\zfe-sdk-javadoc.jar` - El archivo JAR contiene archivos JavaDoc para importar a su IDE.

6.3 Uso del Conector para Windows

El Conector para Windows de Host Access for the Cloud es una instalación independiente que se puede encontrar en la página de descargas de Micro Focus. Con el Conector para Windows, puede interactuar con sesiones de host en su aplicación .NET o en Visual Basic para aplicaciones.

La documentación de la API está disponible en el directorio de instalación (`<dir_instalación>\sessionserver\sdk\csharp\apidocs\index.html`) y también en línea: Conector de HACloud para Windows.

Éstos son algunos puntos a recordar cuando prepare la instalación:

- Existen dos plataformas de instalación: una versión de 32 bits y una de 64 bits. En función de la que instale, la ruta de instalación básica por defecto será `C:\Archivos de programa (x86)\Micro Focus\HACloud\Connector for Windows` o `C:\Archivos de programa\Micro Focus\HACloud\Connector for Windows`
- La plataforma de instalación que seleccione determina también la plataforma de solución en la que puede desarrollar. Por ejemplo: si ha instalado la versión de 32 bits de Microsoft Office® y desea utilizar Visual Basic para aplicaciones con el conector, deberá instalar la versión de 32 bits del Conector para Windows de Host Access for the Cloud.
- La documentación de la API está disponible aquí: `<directorio de instalación>\sessionserver\sdk\csharp\apidocs\index.html`
- Se requiere .NET 4.5.2.
- El Conector para Windows admite dos métodos de autenticación: LDAP y Ninguno. La autenticación se configura en la Consola Administrativa de MSS.

6.3.1 Ejemplos y documentación del conector

La documentación está disponible como referencia desde su IDE. También hay ejemplos para ayudarle a beneficiarse del conector. Ambos se encuentran aquí:

1. Desplácese al directorio de instalación. En una instalación por defecto, `C:\Archivos de programa (x86)\Micro Focus\HACloud\Connector for Windows` o `C:\Archivos de programa\Micro Focus\HACloud\Connector for Windows` en función de su plataforma.
2. En el directorio Connector for Windows encontrará:
    - `MicroFocus.ZFE.Connector.dll` - un ensamblado .NET Framework para referenciar en su proyecto C# o .NET.
    - `MicroFocus.ZFE.Connector.tlb` - una biblioteca de tipos para utilizar en su proyecto COM o de Visual Basic para aplicaciones.
    - `\help` - este directorio contiene información que le ayudará a utilizar el conector.
    - `\samples` - este directorio contiene ejemplos de código que proveen un punto de partida para desarrollar sus propias aplicaciones.

6.3.2 Utilizar el conector con Microsoft Visual Studio

Si está utilizando Microsoft Visual Studio para desarrollar aplicaciones, recuerde los siguientes puntos:

- Si utiliza Microsoft Visual Studio con el Conector para Windows, asegúrese de que la plataforma de solución se ha establecido en x86 o x64 en función de su instalación. Por motivo de los componentes nativos que se utilizan en el Conector para Windows SDK, no se admite la plataforma Any CPU (Cualquier CPU). Utilice el Administrador de configuración de Solución Visual Studio para crear una plataforma para x86 o x64.
- Al añadir una referencia a la biblioteca del Conector para Windows, Visual Studio puede establecer la propiedad de la referencia Copia Local en True. Esta debe establecerse en False para que la biblioteca y sus dependencias se ejecuten desde el directorio de instalación del SDK.

6.4 Uso de la API de JavaScript

Mediante el uso de JavaScript en un navegador, puede incrustar el cliente Web en una página Web. Los usuarios finales, al acceder a una página Web habitual, pueden interactuar con el cliente Web y conectarse a la aplicación host, lo que les permite:

- Interactuar mediante programación con las sesiones de host.
- Ejecutarlo "sin cabeza", lo que significa que se puede acceder a todas sus funciones sin necesidad de disponer de una interfaz visible incrustada en la página Web.

Hay disponibles tutoriales de primeros pasos y de otros temas que puede utilizar. La documentación de API, junto con los tutoriales, está disponible en línea aquí: API de JavaScript de HACloud y `<directorio de instalación>\sessionserver\sdk\javascript`

> **Nota**
>
> El indicador SameSite debe ajustarse al utilizar la API de JavaScript. Consulte Definición del atributo SameSite.

6.5 Ampliación del cliente web

Puede actualizar, modificar y personalizar la presentación del cliente Web mediante su propio código HTML, CSS o JavaScript en el navegador.

Puede aprovechar las ventajas de las extensiones para realizar cambios visuales en el cliente Web y personalizar la aplicación. El cliente Web aloja el código HTML o CSS personalizado, lo que facilita la modificación y la asistencia.

Obtenga más información sobre:

- Adición de una extensión
- Ejemplo de extensión

6.5.1 Adición de una extensión

Antes de continuar, tenga en cuenta que, aunque Host Access for the Cloud permite planificar y utilizar código personalizado, el equipo que generó el propio código debe proporcionar asistencia al mismo.

> **Advertencia**
>
> Durante una actualización del producto, las extensiones están inhabilitadas. Esto significa que, después de una actualización, debe comprobar que el producto funcione en la forma prevista sin extensiones y, a continuación, debe habilitar de nuevo las extensiones mediante los pasos para añadir código personalizado.

Al añadir extensiones al cliente Web, las modificaciones están visibles para todos los usuarios y se aplican a todas las sesiones.

Para añadir una extensión

1. Abra `<directorio_de_instalación>/sessionserver/microservices/sessionserver/service.yml`.
2. Añada extensions_enabled al valor existente de la propiedad SPRING_PROFILES_ACTIVE. Utilice comas para separar los valores.

   Por ejemplo:

   ```
   env:
     - name: SPRING_PROFILES_ACTIVE
       value: tls,extensions_enabled
   ```

3. Reinicie el servidor de sesión.
4. Cree `<directorio_de_instalación>/sessionserver/microservices/sessionserver/extensions/client/index.html` para que actúe como punto de entrada. Esta es la ubicación en la que se añade el código HTML, CSS o JavaScript (incluidas las referencias a guiones externos).

Facilitar las extensiones sin la autenticación de cliente

Los archivos incluidos en el directorio `/client` están protegidos mediante el nivel de autenticación seleccionado en MSS.

Para compartir archivos sin necesidad de la autenticación:

Cree `<dir_instalación>/sessionserver/microservices/sessionserver/extensions/public/`. Coloque el código en ese directorio, llamándolo mediante la URL `/public/*`.

6.5.2 Ejemplo de extensión

En este ejemplo, una vez que las extensiones estén habilitadas (consulte el paso 2 mostrado anteriormente), puede añadir código CSS y JavaScript personalizado para cambiar el color de fuente de la etiqueta de menú e imprimir texto en la consola de JavaScript.

Creará tres archivos `custom.css`, `custom.js` y `index.html`.

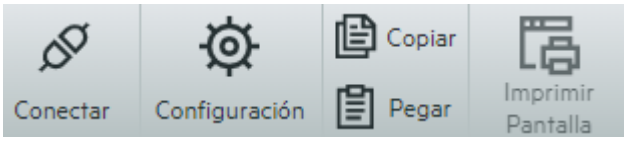
Paso 1

Localice el archivo `index.html`, que ha creado en el paso 4 mostrado anteriormente. Esta es la ubicación en la que incluirá los archivos de extensión, lo que creará un punto de entrada:

```
<!-- Define the link to the external style sheet -->
<link href="client/custom.css" rel="stylesheet">
<!-- Define the external JavaScript file -->
<script src="client/custom.js"></script>
```

Paso 2

Cambie las etiquetas de menú de color negro a naranja:



Cree el archivo custom.css para cambiar el color a naranja:

```
/* Change link text to Orange */
a span {
    color: #ff5d28;
}
```

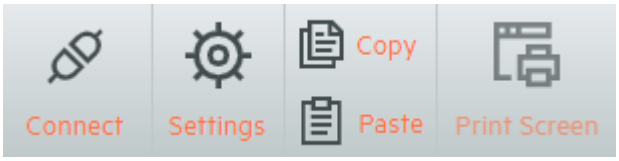
Paso 3

Cree el archivo custom.js para enviar texto a la consola de JavaScript:

```
//Print message to the JavaScript console
console.log('Hello World!');
```

Paso 4

Una vez insertados los archivos en su ubicación, `<directorio_de_instalación>/sessionserver/microservices/sessionserver/extensions/client/index.html`, los resultados deberían presentar un aspecto similar al siguiente:



Y el texto "Hello World" debería estar visible en la console de JavaScript:

Más información:

Documentación de la API de HACloud

7. Referencias técnicas

7.1 Referencias técnicas

En esta sección encontrará información sobre problemas específicos que se puede encontrar. En el Manual de Soporte Técnico de Micro Focus encontrará información sobre cómo obtener soporte técnico para su producto, acceder a nuestros recursos online y ponerse en contacto y trabajar con nuestra organización de servicio técnico mundial.

7.2 Supervisión de servidores de sesión mediante Prometheus y Grafana

Puede supervisar los servidores de sesión de Host Access for Cloud mediante Prometheus y Grafana. Ambas herramientas son gratuitas, de código abierto y se pueden ejecutar en contenedores de Docker, lo que facilita su distribución. Cada servidor de sesión proporciona un puesto final de Prometheus que muestra estadísticas sobre ese servidor. Prometheus se puede configurar para extraer datos de este puesto final y almacenar las estadísticas de forma continua, incluso desde varios servidores de sesión. A continuación, Grafana proporciona una consola para consultar y visualizar estos datos, con muy poca configuración.

Requisitos previos:

Debe tener instalados Docker y la herramienta de composición de Docker.

Pasos:

1. Cree un archivo de composición de Docker (.yml) que contenga imágenes de Grafana y Prometheus.
2. Vincule Prometheus al puesto final de Prometheus del servidor de sesión.
3. Configure el origen de datos de Grafana para comunicarse con Prometheus e importe las consolas preconfiguradas.
4. Configurar las consolas de Grafana.
5. Acceder a Grafana.

7.2.1 Paso 1. Crear un archivo de composición de Docker

Cree un archivo `docker-compose.yml` que contenga imágenes de Grafana y Prometheus.

```
version: "3.1"
services:
  grafana:
    build: grafana
    ports:
      - '3000:3000'
  prometheus:
    image: prom/prometheus:v2.6.1
    ports:
      - '9090:9090'
    volumes:
      - ./config/prometheus.yml:/etc/prometheus/prometheus.yml
      - ./prometheus:/prometheus
    networks:
      monitoring:
        aliases:
          - prometheus
networks:
  monitoring:
```

7.2.2 Paso 2. Vincular Prometheus al puesto final de Prometheus de HACloud

Para vincular Prometheus al puesto final, genere un archivo `prometheus.yml`.

- En el ejemplo, el archivo `prometheus.yml` se guarda en el directorio de configuración.
- Esta configuración de ejemplo le permite extraer el puesto final de Prometheus mediante HTTP o HTTPS (TLS).
- Si TLS está deshabilitado en el servidor de sesión, elimine tls_config y cambie el esquema a http en la configuración de ejemplo.
- Configure el parámetro session-server-hostname.

> **Nota**
>
> Debido a la conexión en red de Docker, este debe ser la dirección IP o el nombre de host reales del equipo host del servidor de sesión. Esta dirección IP se puede obtener normalmente mediante ifconfig/ipconfig.

- Ajuste los puertos si es necesario.

Ejemplo: config/prometheus.yml

```
scrape_configs:
  - job_name: ' HACloud Session Server with TLS'
    scrape_interval: 15s
    scheme: https
    tls_config:
      insecure_skip_verify: true
    metrics_path: actuator/prometheus
    static_configs:
      - targets: ['session-server-hostname:7443']
```

7.2.3 Paso 3. Configurar la comunicación entre Prometheus y el origen de datos

La comunicación se puede configurar dentro de la imagen de Docker de Grafana entre la instancia local de Prometheus y el origen de datos de Grafana. Las consolas precargadas también están disponibles durante el inicio.

Ejemplo: grafana/Dockerfile

```
FROM grafana/grafana:8.0.5
ADD ./provisioning /etc/grafana/provisioning
ADD ./config.ini /etc/grafana/config.ini
ADD ./dashboards /var/lib/grafana/dashboards
```

Ejemplo: grafana/config.ini

```
[paths]
provisioning = /etc/grafana/provisioning
```

Ejemplo: grafana/provisioning/datasources/all.yml

```
datasources:
- name: 'Prometheus'
  type: 'prometheus'
  access: 'browser'
  url: 'http://localhost:9090'
```

```
  is_default: true
  editable: false
```

Ejemplo: grafana/provisioning/dashboards/all.yml

```
- name: 'default'
  org_id: 1
  folder: ''
  type: 'file'
  options:
    folder: '/var/lib/grafana/dashboards'
```

7.2.4 Paso 4. Configurar las consolas de Grafana

Hay disponible un archivo JSON de ejemplo para ayudarle a empezar a configurar las consolas de Grafana.

Para que el contenedor de Docker cargue la consola durante el inicio:

- Busque `HACloudSessionservers.json` en el directorio `hacloud/utilities/grafana`.
- Copie `HACloudSessionservers.json` en el directorio `grafana/dashboards`.

7.2.5 Paso 5. Acceder a Grafana

- Inicie el contenedor de Docker con el comando docker-compose up -d.
- Compruebe que los destinos de Prometheus están extrayendo correctamente los servidores de sesión mediante `http://localhost:9090/targets`.
- Acceda a Grafana mediante `http://localhost:3000`.
- Tanto el nombre de usuario como la contraseña son *admin*. El nombre de usuario y la contraseña se pueden configurar mediante las variables de entorno de Docker.
- Utilice el comando docker-compose down para detener el contenedor de Docker.

7.3 Ejecución del servicio del servidor de sesión como usuario dedicado con privilegios reducidos

En aras de la seguridad, debería ejecutar el servicio del servidor de sesión como un usuario dedicado con privilegios reducidos.

> **Nota**
>
> Debe repetir estos pasos después de cualquier actualización del producto.

Para realizar este proceso en una plataforma Windows:

1. Después de instalar el producto por primera vez, cree un usuario estándar.
2. Asigne al usuario control total de los siguientes directorios:
   - `<directorio_de_instalación>\sessionserver\logs`
   - `<directorio_de_instalación>\sessionserver\tmp`
3. En el cuadro de diálogo Servicios de Windows, detenga el servicio del servidor de sesión de Micro Focus Host Access for the Cloud.
4. Abra las propiedades del servicio del servidor de sesión de Host Access for the Cloud.
5. Abra la pestaña Entrada y seleccione **Esta cuenta**.
6. Introduzca el nombre de usuario y la contraseña del usuario que va a ejecutar el servicio.
7. Inicie el servicio del servidor de sesión.

Para realizar esta acción en Unix/ Linux:

Siga los pasos anteriores, pero ajustándolos a su entorno y distribución específicos.

Más información

Running the Micro Focus MSS Server service as a dedicated user (Ejecución del servicio de servidor MSS de Micro Focus como un usuario dedicado)

7.4 Definición del atributo SameSite

Para ayudar a prevenir los ataques de falsificación de peticiones entre sitios, el atributo SameSite por defecto en la cookie del servidor de sesión se ha actualizado de **None** (menos restrictivo) a **Lax** (más restrictivo).

Con el atributo definido en "Lax", la cookie del servidor de sesión no se enviará en peticiones entre sitios, como suele ser el caso del SDK de JavaScript y la autenticación SAML.

Este cambio afecta a dos áreas de HACloud:

- El SDK de JavaScript y
- la autenticación SAML tras un equilibrador de carga

En estos casos, deberá ajustar el valor del atributo a **None**. Para ello, realice lo siguiente:

1. Abra `container.properties` en un editor de texto. La ubicación por defecto de este archivo es: `./sessionserver/conf/` .
2. Añada la siguiente línea a `container.properties` :

   `samesite.cookie.attribute=None`
3. Reinicie el servidor de sesión.

7.5 Modificación del límite de tamaño en las operaciones de carga de transferencia de archivos

Existe un límite de tamaño de archivo de 50 MB para las operaciones de carga de transferencia de archivos. Para modificar el límite de tamaño de archivo, defina `spring.servlet.multipart.maxfilesize` y `spring.servlet.multipart.maxrequestsize` en `HACloud/sessionserver/microservices/sessionserver/service.yml` y reinicie el servidor de sesión.

Por ejemplo:

```
- name: spring.servlet.multipart.maxfilesize
  value: "100MB"
- name: spring.servlet.multipart.maxrequestsize
  value: "100MB"
```

7.6 Configuración de la dirección de devolución de llamada de MSS

MSS proporciona una dirección de devolución de llamada al servidor de sesión cada vez que crea o edita una sesión.

Por defecto, se utiliza la dirección especificada en `management.server.url`.

Si el servidor de MSS está detrás de un apoderado (proxy) y el servidor de sesión no puede acceder a la dirección:

- Defina la propiedad `management.server.callback.address` en cada archivo container.properties de MSS en una dirección a la que pueda acceder el servidor de sesión para una instancia de MSS específica.
- Reinicie el servidor para que se apliquen los nuevos valores de propiedades.

7.7 Copiar sesiones entre los Servidores de Administración y Seguridad

Puede copiar y convertir sesiones de Reflection for the Web y facilitarlas a otro Servidor de Administración y Seguridad (MSS) y Host Access for the Cloud.

> **Nota**
>
> En el siguiente ejemplo, el Servidor de Administración y Seguridad del que copia las sesiones es el servidor de **origen**, y el Servidor de Administración y Seguridad en el que las está copiando es el servidor de **destino**.

Para copiar sesiones del servidor de origen al servidor de destino, siga los siguientes pasos:

1. Detenga el servidor MSS de destino.
2. En los servidores MSS de origen y de destino, abra SessionDS.xml, ubicado en:
   - En Windows: `C:\ProgramData\Micro Focus\MSS\MSSData`
   - En Linux: `/var/opt/microfocus/mss/mssdata`
3. En el archivo XML de origen, localice el elemento OBJECT_ARRAY.
4. Aún en el archivo XML de origen, en OBJECT_ARRAY, localice y copie los elementos Session hijo de Reflection for the Web.
5. Abra el archivo XML de destino y péguelo en el elemento OBJECT_ARRAY del archivo de destino.
6. Aún en el archivo de destino, localice el atributo de tamaño OBJECT_ARRAY que corresponda con el número de sesiones. Aumente ese valor con el número de elementos de sesión que haya agregado. Por ejemplo, si ha pegado seis elementos Session en el archivo de destino y el valor del atributo de tamaño existente de OBJECT_ARRAY es 4, aumente el valor en seis. El atributo de tamaño debe ser ahora diez. Y ahora debe tener 10 elementos Session listados bajo el elemento OBJECT_ARRAY.
7. Los nombres de las sesiones deben ser únicos. Compruebe si el archivo de destino contiene nombres de sesión duplicados. Puede encontrar nombres de sesión en el elemento Session hijo, SessionName.
8. Copie los archivos de configuración de cada sesión agregada a SessionDS.xml del servidor de origen al servidor de destino. Los nombres de los archivos de configuración se encuentran bajo el elemento Session en el elemento hijo, configuration. Los archivos propiamente dichos se encuentran en:
   - En Windows: `C:\ProgramData\Micro Focus\MSS\MSSData\deploy\dyncfgs`
   - En Linux: `/var/opt/microfocus/mss/mssdata/deploy/dyncfgs`
9. Reinicie el servidor MSS de destino. Abrir la Consola Administrativa. Debe ver todas la sesiones copiadas de Reflection for the Web en la lista Administrar sesiones.
10. El paso siguiente es convertir la sesión de Reflection for the Web en una sesión de Host Access for the Cloud. En Administrar sesiones, haga clic con el botón derecho en la sesión que desea convertir. Los tipos de sesión se identifican mediante un icono en la columna Tipo.
11. Consulte Convertir una sesión de Reflection for the Web para obtener información sobre cómo convertir sesiones de Reflection for the Web a sesiones de Host Access for the Cloud en la Consola Administrativa.

7.8 Cambio de puertos

Consulte Puertos para obtener una lista de los puertos por defecto utilizados por Host Access for the Cloud.

Para cambiar los puertos por defecto:

Componente	Instrucciones
Servidor de sesión de Host Access for the Cloud	Abra `sessionserver/microservices/sessionserver/service.yml` para modificar: `-name : SERVER_PORT` y `value: "7443"`
Servidor de Administración y Seguridad	El puerto SSL que utiliza el MSS para establecer una conexión HTTPS está ajustado a 443 de forma predeterminada. Si necesita cambiar el número de puerto, inicie el Servidor de Administración. Éste crea el archivo predeterminado PropertyDS.xml. Seguidamente, abra PropertyDS.xml en el directorio MssData. Cambie el valor de 443 al número de puerto apropiado en la sección siguiente y reinicie entonces el Servidor de Administración. `<CORE_PROPERTY NAME="sslport"> <STRING>443</STRING>`

7.9 Cómo iniciar y detener servicios automáticamente

Todos los componentes del servidor se instalan como servicios y se pueden configurar para iniciarse durante la instalación.

Si usted está trabajando con plataformas Linux, siga estos pasos para configurar el servidor de sesión para que se inicie automáticamente cuando su sistema arranque.

Cree un archivo con el nombre `sessionserver` que contenga lo siguiente y que utilice el directorio de instalación:

```
#!/bin/sh
#
#Este guión administra el servicio necesario para ejecutar el servidor de sesión
#chkconfig:235 19 08
#description: Administre el servidor de sesión de Host Access for the Cloud

###BEGIN INIT INFO
# Provides: sessionserver
# Required-Start: $all
# Required-Stop: $all
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Description: Inicie el servidor de sesión de Host Access for the Cloud
### END INIT INFO

INSTALL_DIR=<introducir directorio de instalación>
BIN_DIR=$INSTALL_DIR/sessionserver/bin
case "$1" in
start)
echo "Starting Host Access for the Cloud Session Server"
$BIN_DIR/server start

RETVAL=0
;;
stop)
echo "Stopping Host Access for the Cloud Session Server"
$BIN_DIR/server stop

RETVAL=0
;;
status) echo "Current Host Access for the Cloud Session Server status"
$BIN_DIR/server status

RETVAL=0
;;
restart) echo "Restart Host Access for the Cloud Session Server"
$BIN_DIR/server restart

RETVAL=0
;;
*)
echo "Usage: $0 (start|stop|status|restart)"

RETVAL=1
;;
esac
exit $RETVAL
```

Complete entonces los pasos relevantes.

En Linux:

1. Copie el archivo al directorio `/etc/init.d`.
2. Ajuste el permiso del archivo. Ejecute `chmod` utilizando el valor 755. Por ejemplo, `chmod 755 sessionserver`.
3. Ejecute `chkconfig` para añadir el guión de inicialización. Por ejemplo, `/sbin/chkconfig --add sessionserver`.

7.10 Ajuste de la vía de URL para el servidor de sesión

Puede ajustar la vía de URL utilizada para acceder al servidor de sesión.

Puede cambiar `https://myserver:7443/` a `https://myserver.com:7443/hacloud/`

1. Abra `<directorio_de_instalación>/sessionserver/microservices/sessionserver/service.yml`.
2. Añada la siguiente entrada (manteniendo el formato), donde *vía* se sustituye por el valor que desee utilizar.

```
- name: SERVER_SERVLET_CONTEXTPATH
  value:"/<vía>"
```

3. Reinicie el servidor de sesión.
4. Acceda al servidor de sesión en `https://<servidor de sesión>:7443/<vía especificada>/`

7.11 Configurar Nombres de usuario cuando se utiliza el Anonymous Access Control (Control de Acceso Anónimo)

Los usuarios necesitan acceso a sus macros, configuraciones de usuarios y otros parámetros personalizados tanto si se autentican mediante el Servidor de Administración y Seguridad como si no. Estos parámetros reciben de forma conjunta el nombre de Preferencias de usuario.

Si MSS se ha configurado para la autenticación, por ejemplo, mediante LDAP o SAML, se determina un nombre de usuario cuando un usuario entra a la sesión. Los valores de configuración del usuario se guardan de forma centralizada en MSS mediante ese nombre de usuario para todas las futuras entradas a la sesión.

Sin embargo, si el Método de autenticación de MSS se define en Ninguno, también conocido como modo anónimo, no hay ningún nombre de usuario exclusivo disponible para que el sistema identifique a ese usuario específico cuando regrese en el futuro. En esta configuración, todos los usuarios comparten los mismos parámetros. Si un usuario modifica un parámetro, este se cambiará para todos los demás usuarios.

Debido a que puede que no siempre sea el comportamiento deseado, Host Access for the Cloud admite varias formas en las que, como administrador, puede configurar un identificador exclusivo para cada usuario a fin de que sus configuraciones personalizadas se puedan almacenar y recuperar durante futuras entradas a la sesión.

> **Nota**
>
> Estas modificaciones en la configuración no alteran las consideraciones de seguridad al usar el Servidor de Administración y Seguridad en el modo anónimo.

7.11.1 Opciones de configuración

Hay cuatro opciones de configuración diferentes que puede elegir a la hora de configurar identificadores de nombres de usuario. Antes de que los cambios surtan efecto, debe reiniciar el servidor de sesión.

- Para utilizar un valor de cookie de solicitud HTTP como nombre de usuario

  Añada las siguientes líneas a `<session-server>/conf/container.properties`:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.CookieKeyAnonymousPrinci
  zfe.principal.name.identifier=<la-clave-de-cookie-que-se-va-a-utilizar>
  ```

- Para utilizar un valor de encabezado de solicitud HTTP como nombre de usuario

  Añada las siguientes líneas a: `<session-server>/conf/container.properties`:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.HeaderKeyAnonymousPrinci
  zfe.principal.name.identifier=<la-clave-de-encabezado-que-se-va-a-utilizar>
  ```

- Para utilizar un parámetro de URL de solicitud HTTP como nombre de usuario

  Añada las siguientes líneas a: `<session-server>/conf/container.properties`

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.UrlParameterAnonymousPri
  zfe.principal.name.identifier=<la clave-del-parámetro-url-que-se-va-a-utilizar>
  ```

- Para utilizar la dirección IP del cliente como nombre de usuario

  Añada la siguiente línea a: `<session-server>/conf/container.properties`

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.RemoteAddrAnonymousPrinc
  ```

7.11.2 Solución de problemas de configuración

Si alguno de los usuarios tiene problemas al conectarse a una aplicación Web de Host Access for the Cloud después de realizar cambios en la configuración, compruebe lo siguiente:

- Los usuarios reciben el mensaje *503 Servicio no disponible* al conectarse a una aplicación Web de Host Access for the Cloud. Compruebe primero el archivo de registro (`<servidor-de-sesión>/logs/sessionserver.log`) y, a continuación, realice lo siguiente:
  - Si el archivo de registro contiene este mensaje: *No es posible crear instancia AnonymousPrincipalNameProvider para clase...*, es posible que la propiedad `zfe.principal.name.provider` se haya escrito incorrectamente. Compruebe la ortografía y el uso de mayúsculas y minúsculas para solucionar este problema.
  - Si el archivo de registro contiene este mensaje, *zfe.principal.name.identifier no está definida*, falta la propiedad. Asegúrese de que la propiedad está definida para solucionar este problema.
- Los usuarios no se pueden autenticar correctamente.

  Los usuarios deben recibir un mensaje de error que indique que la petición HTTP inicial a la aplicación web de Host Access for the Cloud no incluía la información necesaria.

7.12 Acceso a Host Access for the Cloud mediante el Proxy inverso IIS

En esta nota, se describe cómo utilizar el Proxy Reverso IIS con Host Access for the Cloud. Para cumplir los requisitos de seguridad de Common Criteria, es necesario colocar Host Access for the Cloud detrás de un proxy del siguiente modo.

Requisitos previos

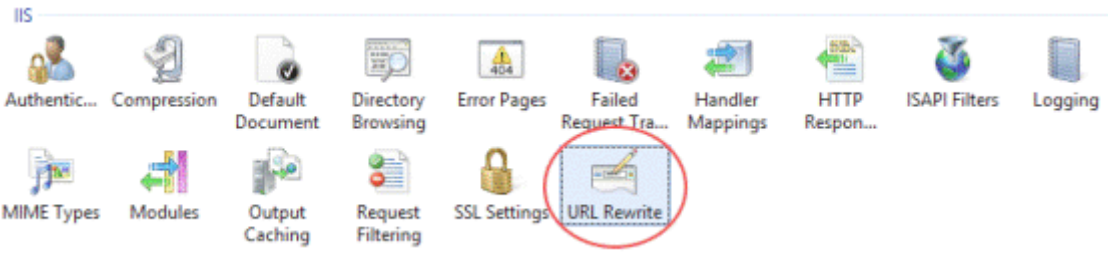
- Se necesita Internet Information Services (IIS) 8.0 o posterior.
- El protocolo WebSockets de IIS debe estar habilitado. Consulte IIS 8.0 WebSocket Protocol Support (Compatibilidad con el protocolo WebSocket IIS 8.0) para obtener información sobre cómo se habilita este protocolo.
- Se necesita Application Request Routing (ARR) 3.0 (Enrutamiento de solicitud de aplicaciones 3.0) de IIS o posterior.
- El módulo URL Rewrite (Reescribir URL) de IIS debe estar instalado.

7.12.1 Configurar el Proxy inverso IIS para HACloud

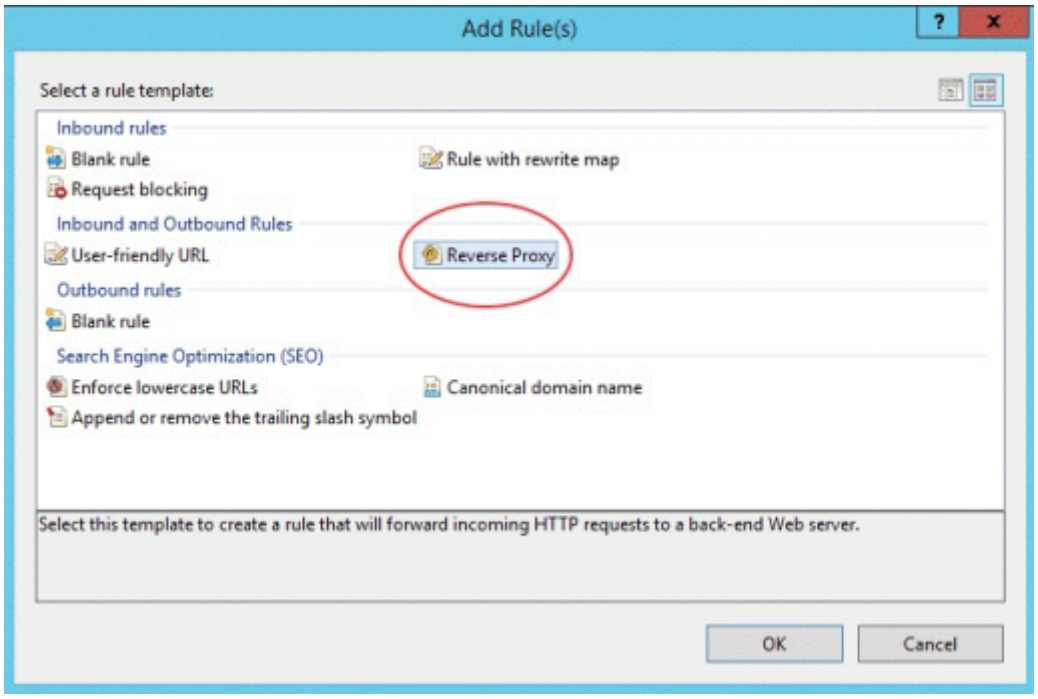
En este ejemplo, se muestra la configuración de un servidor IIS con la dirección IP 192.168.1.1 para establecer conexiones de proxy en el servidor de sesión de Host Access for the Cloud, en `http://10.10.10.1:7070`.

Configurar IIS

1. Inicie el Administrador de Internet Information Services (IIS), navegue hasta el sitio web que desee utilizar y abra el componente URL Rewrite (Reescribir URL).



1. Seleccione la acción Add Rule(s) (Agregar reglas) y añada una regla de Proxy inverso.



1. Para la regla de entrada, introduzca la dirección IP o el nombre de host y el puerto del servidor de Host Access for the Cloud. Por ejemplo, si el servidor de sesión se encuentra en el mismo equipo que IIS y está utilizando el puerto por defecto, introduzca `localhost:7443`.
2. Active la regla de salida "Rewrite the domain names..." (Reescribir nombres de dominio...) e introduzca el nombre de host o la dirección IP del servidor IIS en la casilla "To:" (A:).
3. Haga clic en OK para crear la nueva regla de Proxy inverso.

Configuración de HACloud

Para las conexiones proxy, el módulo URL Rewrite (Reescribir URL) de IIS debe inspeccionar y reescribir las páginas web y las conexiones WebSocket que pasan por el proxy. Para que la reescritura se realice correctamente, estos elementos se deben enviar de forma no comprimida. Recuerde que, de estar configurada, la compresión seguirá teniendo lugar del servidor IIS al

navegador del cliente. Por lo tanto, el servidor de sesión debe estar configurado para permitir conexiones WebSocket originadas desde el proxy.

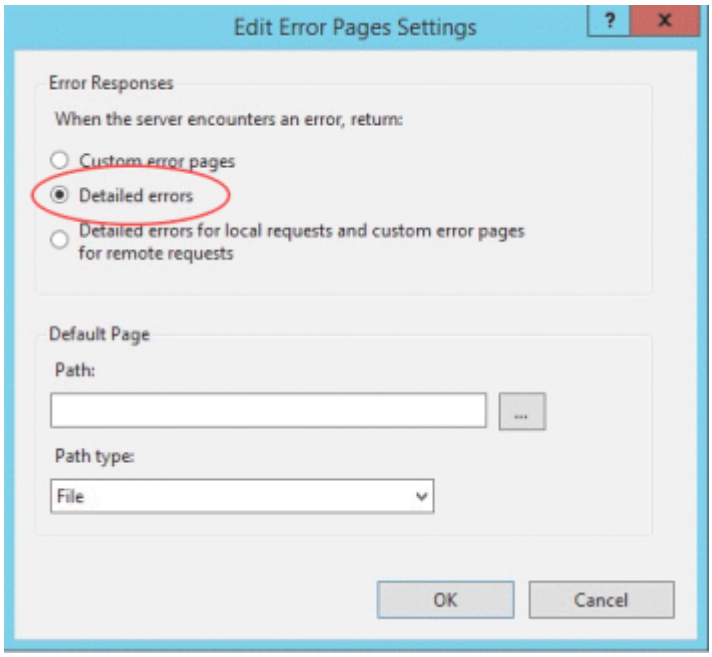
1. Abra container.properties en un editor de texto. La ubicación por defecto de este archivo es: /sessionserver/conf.
2. Añada las siguientes líneas a `container.properties`:

```
websocket.compression.enable=false
server.compression.enabled=false
websocket.allowed.origins=http://<nombre de servidor IIS o dirección IP>. Por ejemplo: 192.168.1.1.
```

   Guarde los cambios en el archivo. La propiedad Allowed Origins (Orígenes Permitidos) es una lista de URL delimitadas por comas. Si los clientes web se van a conectar a su sitio web utilizando una conexión HTTPS, ajuste la URL correspondientemente. Si se van a utilizar conexiones seguras y no seguras, utilice las dos URLs como valor: `websocket.allowed.origins=http://192.168.1.1,https://192.168.1.1`. Para evitar errores, asegúrese de que todos los formatos de dirección posibles estén incluidos en la lista Allowed Origins (Orígenes permitidos).
3. Reinicie el sitio Web y el servidor de sesión, y pruebe el proxy. Para ello, conéctese a: `http(s)://192.168.1.1`.

Solución de problemas

Si recibe errores de servidor web, habilitar los errores detallados puede ayudar a diagnosticar el problema. En el administrador de IIS, abra el componente Error Pages (Páginas de Error) y active Detailed errors (Errores detallados):



Normalmente, en el rango 5XX los errores vienen causados por problemas con la habilitación de la compresión o por errores en el valor Allowed Origins (Orígenes Permitidos).

Si el proxy IIS se va a conectar al servidor de sesión con HTTPS, el certificado utilizado con el servidor de sesión debe ser de confianza para el servidor IIS. Si el servidor de sesión está utilizando un certificado autofirmado, este certificado se debe añadir al almacén de certificados de confianza de Windows. Si el servidor de sesión está utilizando un certificado firmado, el firmante debe ser una CA de confianza.

7.13 Uso del Proxy inverso IIS con Host Access for the Cloud

Para cumplir los requisitos de seguridad de Common Criteria, es necesario colocar el servidor de sesión detrás de un proxy. Antes de realizar la configuración, lea "Acceso a Host Access for the Cloud mediante el Proxy inverso IIS" para obtener información sobre los requisitos previos y las instrucciones de configuración.

> **Nota**
>
> Para cumplir los requisitos de seguridad de criterios comunes, es posible que sea necesario colocar el servidor de sesión detrás de un proxy mediante las instrucciones de la sección Acceso a Host Access for the Cloud mediante el Proxy inverso IIS.

Para utilizar un proxy con Host Access for the Cloud mediante IIS, al utilizar la entrada única de IIS, deberá establecer una propiedad adicional en el mismo archivo container.properties:

```
servletengine.iis.url=<url>
```

El valor adopta la misma forma que la URL mostrada anteriormente, pero utiliza la dirección de Host Access for the Cloud. Por ejemplo: `http://server/` . No es necesario utilizar la forma abreviada del nombre del host en esta URL.

Una vez que haya concluido esta configuración, puede elegir esta opción de autenticación en Management and Security Server Administrative Console | Assign Access (Consola Administrativa del Servidor de Administración y Seguridad | Configuración de Control de Acceso). Consulte la ayuda en línea de la Consola Administrativa para obtener descripciones de las opciones de configuración.

Más información:

- Configuración del inicio de sesión único mediante IIS

7.14 Configuración del uso compartido de recursos entre orígenes (CORS)

Como medida de seguridad, los navegadores web modernos restringen los tipos de interacciones que se permiten entre distintos sitios web. Esto puede causar problemas al intentar la integración entre sitios, por ejemplo, al incrustar el cliente web HACloud en otro sitio web, como un portal. CORS es un mecanismo estándar que permite especificar que el navegador permita el acceso de un sitio a otro.

Puede configurar el servidor de sesión de HACloud para que incluya el encabezado HTTP CORS necesario cuando responda a las solicitudes web mediante la actualización del archivo `service.yml`.

1. Abra `<directorio de instalación>/sessionserver/microservices/sessionserver/service.yml`.
2. En el archivo, añada

```
    - name: CORS_ALLOWED_ORIGINS
      value: "https://integration-server1.com"
```

3. Reinicie el servidor de sesión.

Puede establecer este valor en una lista delimitada por comas de los orígenes permitidos o utilizar `*` para permitir el acceso desde todos los orígenes (permitir este tipo de acceso abierto puede suponer un riesgo para la seguridad). Si utiliza la opción comodín (*), tenga en cuenta que los navegadores web imponen restricciones adicionales, como el acceso limitado a las cookies. Para obtener más información, consulte Cross-Origin Resource Sharing (CORS) - HTTP/MDN (Uso compartido de recursos entre orígenes, CORS: HTTP/MDN).

7.15 Ajuste del tiempo límite de la sesión HTTP

El valor de tiempo de espera por defecto para una sesión de usuario inactiva es de 30 minutos. Esto significa que cuando un usuario cierra el navegador sin cerrar primero la sesión, su sesión de usuario y cualquier sesión de host abierta se eliminarán una vez transcurridos 30 minutos. El valor de tiempo límite mínimo permitido es de 600 segundos (10 minutos). Puede configurar este parámetro en el servidor.

1. Abra `<directorio de instalación>/sessionserver/microservices/sessionserver/service.yml`.
2. Ajuste el valor de tiempo límite en la sección `env` del archivo:

```
  - name: server.servlet.session.timeout
    value: <valor-deseado-en-segundos>
```

> **Nota**
>
> El formato de la sangría es importante.

3. Reinicie el servidor.

7.16 Habilitar el Nivel de Seguridad FIPS

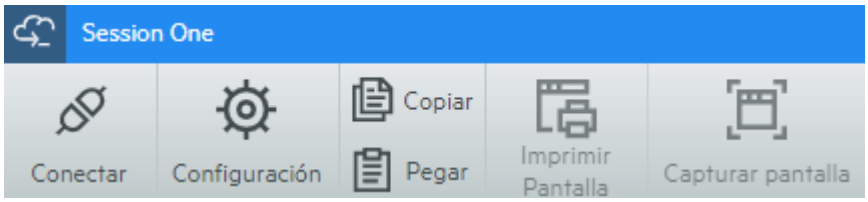
Los módulos criptográficos validados por el estándar de procesamiento de información federal (Federal Information Processing Standards, FIPS) 140-2 los utiliza el gobierno federal de EE. UU. como un estándar de normativa de seguridad. Host Access for the Cloud admite este estándar; puede habilitar fácilmente el modo FIPS mediante la edición de un archivo en el servidor de sesión.

- Abra `<directorio_de_instalación>\sessionserver\microservice\sessionserver\service.yml`.
- Añada el indicador `-Dcom.attachmate.integration.container.FIPS.enabled=true` al comando de Java - `start-command`.
- Reinicie el servidor.
- Para asegurarse de que el modo FIPS esté habilitado, abra `<directorio_de_instalación>\sessionserver\logs\sessionserver.log` y compruebe que el modo FIPS se haya definido en "true" (verdadero); `FIPS mode: true`.

7.17 Uso del modo de sesión única

Puede utilizar el modo de sesión única y proporcionar direcciones URL a sesiones específicas que se lanzan mediante el parámetro de nombre (por ejemplo, un enlace directo en una página del portal de la compañía). Para habilitar el inicio de una sesión única, utilice el parámetro de consulta singleSession. Puede utilizar este parámetro por sí solo para lanzar el cliente Web en modo de sesión única, por ejemplo, `http://<sessionserver>:7443//?singleSession`, o se puede utilizar en combinación con un parámetro de una sesión con nombre para iniciar una sesión con un nombre específico en el modo de sesión única: `http://<sessionserver>:7443/?singleSession&name=HumanResources`. El orden de los parámetros no tiene importancia.

Cuando los usuarios acceden a una sesión única, no pueden cambiar entre sesiones abiertas y no pueden abrir nuevas sesiones. No se abrirá una nueva sesión si la sesión especificada ya existe cuando el usuario abre el enlace.



Si desea que todas las sesiones del servidor de sesión se ejecuten en modo de sesión única:

- Abra `<directorio-de-instalación>/sessionserver/conf/container.properties`
- Añada `webclient.singleSession=true` al archivo.

7.18 Problemas conocidos

Estos problemas han sido identificados en versiones anteriores y ahora son problemas conocidos.

7.18.1 Problemas con el navegador

Las siguientes notas son específicas de navegadores web específicos.

Navegadores recomendados

Se recomienda expresamente que utilice Google Chrome o Mozilla Firefox. Aunque Host Access for the Cloud es compatible con Microsoft Internet Explorer (IE) 11, existen problemas de rendimiento conocidos con el motor de JavaScript de Internet Explorer que pueden afectar negativamente a la experiencia del usuario final con Host Access for the Cloud.

Se han identificado estos problemas y hay soluciones para ellos, aunque el método más sencillo es utilizar otro navegador.

- Internet Explorer no puede reproducir macros grabadas

  Cuando se utilizan determinadas versiones anteriores del navegador Web Microsoft Internet Explorer (IE) con Host Access for the Cloud, es posible que los intentos de reproducir macros presenten errores. El mensaje de error dice: *Error de macro: Error al transpilar el código de la macro: TypeError: desconocido: Referencia circular en argumento de valor no soportada*.

  Éste es un problema con esta versión de Internet Explorer y JavaScript. Puede ser posible evitar este error si borra la función createMacro() y la sustituye utilizando JavaScript Promises (por ejemplo, then()).

  Como este problema es específico de las versiones antiguas de Internet Explorer, la solución más sencilla para este problema es utilizar un navegador distinto (Chrome o Firefox) o una versión más reciente de Internet Explorer. Puede reproducir macros correctamente utilizando Internet Explorer versión 11.0.9600.18161, versión actualizada 11.0.27. Ejecute la actualización de Windows para actualizar el Internet Explorer.

- Conexiones HTTPS entre dispositivos móviles Apple iOS y el servidor de sesión

  Los usuarios de Host Access for the Cloud no se pueden conectar a un servidor de sesión mediante HTTPS desde su iPad de Apple al utilizar un certificado autofirmado. De ser factible, la solución más rápida es utilizar HTTP en lugar de HTTPS.

  Si se precisa HTTPS, dispone de las siguientes opciones:

  - Obtenga un certificado válido firmado por una CA de confianza e instálelo en el servidor de sesión.
  - Encuentre un navegador alternativo que acepte el certificado autofirmado. Consulte "Compatibilidad con el navegador y el sistema operativo" para obtener una lista de exploradores admitidos.
  - Crear una autoridad de certificación personalizada:
    - Cree una CA personalizada, un certificado de raíz de CA y un certificado del servidor firmado por ese certificado de raíz de la CA.
    - Instale el certificado del servidor en el servidor de sesión.
    - Instale el certificado de raíz de la CA personalizada en el iPad mediante un perfil. El iPad debe aceptar ahora el certificado del servidor ya que viene firmado por una “CA de confianza”.

  Para ver una lista de las CAs de confianza de Apple iOS, véase Listas de certificados de raíz de confianza en iOS.

- Internet Explorer Displays Blank Screens (Internet Explorer muestra pantallas vacías)

  Cuando se utiliza el navegador Web Microsoft Internet Explorer (IE) con Host Access for the Cloud (RZFE) o el Servidor de Administración y Seguridad (MSS), es posible que aparezca una pantalla en blanco en lugar de la sesión esperada.

Al utilizar Microsoft Internet Explorer para acceder a las sesiones de Host Access for the Cloud o al Servidor de Administración y Seguridad, puede experimentar problemas, como los siguientes:

Host Access for the Cloud se procesa correctamente para algunas URL, pero no para otras (se muestra una ventana en blanco). El comportamiento varía en función de si la sesión está utilizando una dirección IP, un nombre de host abreviado o un nombre completo.

En MSS, no puede crear o abrir una sesión de Host Access for the Cloud a menos que esta se encuentre en el mismo servidor que MSS. Usted ve una pantalla negra en el lugar donde espera ver la sesión.

Explicación

Este problema es específico de la forma en la que Internet Explorer cambia algunos ajustes dependiendo de su interpretación de la seguridad del sitio web. Los ajustes en cuestión son la Vista de Compatibilidad y las Cookies de terceros. Dependiendo de la “zona” que Internet Explorer determina para su sitio web, estos ajustes se deben habilitar o deshabilitar. Internet Explorer basa su determinación en la URL del sitio. Por ejemplo, si el nombre del servidor en la URL no contiene puntos (por ejemplo, `http://mycorporateserver/mss/AdminStart.html`), Internet Explorer presupone que la dirección pertenece a la zona Intranet local. Si es así, el sitio se asigna a la zona Internet.

Zona Internet Local

- Vista de Compatibilidad habilitada (no se desea)
- Cookies de terceros habilitadas (se desea)

Zona Internet

- Vista de Compatibilidad deshabilitada (se desea)
- Cookies de terceros deshabilitadas (no se desea)

Si bien es posible anular la Vista de Compatibilidad para un sitio Web especificando el Modo de documento con una etiqueta meta HTTP X-UA-Compatible, y Host Access for the Cloud utiliza ese modo específico, MSS no lo utiliza. Por lo tanto, si un servidor de Host Access for the Cloud y un Servidor de Administración y Seguridad se encuentran en la zona de Intranet local (con la Vista de Compatibilidad habilitada por defecto), es posible que Host Access for the Cloud siga funcionando correctamente, pero MSS no.

Solución

Para utilizar Internet Explorer 10 u 11 con los servidores de Host Access for the Cloud y MSS, necesita lo siguiente:

Usted debe determinar en qué zona se encuentra su sitio web y hacer los ajustes correspondientes en la configuración de Internet Explorer. Como Internet Explorer se puede configurar de tantas formas diferentes en función de su situación, es difícil ofrecer una

solución para utilizar correctamente Internet Explorer con Host Access for the Cloud y MSS. Hay algunas configuraciones posibles que se pueden seguir:

- Si tanto Host Access for the Cloud como MSS se encuentran en la zona de Internet, añada manualmente el servidor de Host Access for the Cloud a la zona de Intranet local o Sitios de confianza (Opciones de Internet > Seguridad > Intranet local > Sitios). Utilice nombres completos de host o direcciones IP completas.
- Si ambos servidores están en la zona Internet, cambie el comportamiento predeterminado para esa zona y habilite Cookies de terceros (Opciones > Privacidad > Avanzadas > Anular manejo automático de cookies).
- Si ambos servidores se encuentran en la zona Intranet Local, cambie el comportamiento predeterminado para esa zona y deshabilite la Vista de Compatibilidad (Herramientas > Ajustes de Vista de Compatibilidad).

Problemas de asignación de teclas con navegadeores distintos

Algunas teclas del teclado numérico y algunas teclas específicas del navegador no se pueden asignar. Por ejemplo, en Chrome no se pueden asignar Ctrl+n y Ctrl+w.

7.18.2 Problemas específicos del host

Los siguientes problemas son específicos de tipos de host diferentes.

Mostrar el carácter del Euro

Si el carácter de euro no se visualiza correctamente en la pantalla del terminal, póngase en contacto con el administrador del sistema para asegurarse de que el juego de caracteres de host de esta sesión se ha configurado correctamente. Por defecto, Host Access for the Cloud utiliza un conjunto de caracteres que no admite el carácter de euro (€). Para visualizar el carácter de euro, cambie el juego de caracteres por uno que admita este carácter.

Problemas encontrados con hosts VT

Tipo	Descripción
Problemas de desempeño	• Una salida de texto gruesa, como “Is-IR”, puede ralentizar el desempeño • Las zonas desplazables pueden aparecer lentas o entrecortadas • El movimiento del cursor puede ser lento o entrecortado • Internet Explorer es especialmente lento y su desempeño se degrada aún más cuando se utilizan filas y columnas.
Juegos de caracteres	• Los caracteres gráficos y algunos juegos de caracteres no se soportan. • Algunos caracteres no ingleses pueden hacer que la pantalla del terminal se congele.
Otros problemas de VT	• Insertar/eliminar columna (DECIC, DECDC) puede fallar. • VT400 no reconocerá DECSCL.

Contorno de campo en sesiones 3270

No se admiten totalmente los atributos de 3270 para contornos de campo. Host Access for the Cloud admite actualmente el subrayado y el suprarrayado. Sin embargo, aún no admite las líneas verticales derecha e izquierda ni combinaciones de los cuatro tipos de línea.

7.18.3 Problemas de instalación

Entre los temas de instalación y actualización, se incluye una sección de resolución de problemas que puede ayudar a diagnosticar y solucionar problemas específicos de instalación.

Definir un directorio temporal para el programa de instalación

El instalador requiere un directorio temporal que permita su escritura. Si el directorio temporal predeterminado no es adecuado, el instalador se puede ejecutar con un directorio temporal alternativo.

- Windows

  Si no se puede escribir en el directorio temporal predeterminado, defina temporalmente las variables de entorno TMP o TEMP en una ubicación alternativa al ejecutar el instalador. Restablezca las variables cuando haya finalizado la instalación.

- Linux/Unix

  La variable de entorno INSTALL4J_TEMP determina el directorio base que el instalador utilizará para la extracción automática. Cuando el programa de instalación extrae los archivos y lanza Java para llevar a cabo otras tareas, se utiliza la ubicación temporal de Java (/tmp).

  Para ejecutar los instaladores de Linux con un directorio temporal alternativo:

  - Defina la variable INSTALL4J_TEMP. Para ello, especifique el valor como la ubicación temporal deseada.
  - Cree el directorio temporal especificado para el instalador. El instalador requiere que ya exista el directorio.
  - Añada el conmutador de línea de comandos `-J-Djava.io.tmpdir={tempdir}` al lanzar el instalador. Por ejemplo:

```
abcd@linux:~$ INSTALL4J_TEMP=/home/abcd/i4jtemp
abcd@linux:~$ export INSTALL4J_TEMP
abcd@linux:~$ sudo ./hacloud-2.4.2.12345-linux-x64.sh -J-Djava.io.tmpdir=/home/abcd/i4jtemp
```

Instalaciones encadenadas de HACloud y MSS

- En Windows, una instalación encadenada de HACloud y MSS no necesitará otros ajustes si define temporalmente las variables de entorno TMP o TEMP descritas anteriormente.
- En Linux/Unix, no se puede ejecutar un instalador encadenado en esta plataforma; ejecútelos por separado, cada uno con los permisos administrativos, la variable INSTALL4J_TEMP definida y con el conmutador -J-Djava.io.tmpdir.

> **Nota**
>
> Si se está realizando una instalación «no encadenada» de MSS y HACloud, MSS debe instalarse primero y, a continuación, HACloud.

Definir un directorio temporal para el producto

HACloud utiliza un directorio temporal interno que debería ser adecuado en todos los casos. Sin embargo, este directorio puede modificarse si es necesario. Para ello, edite el archivo `container.conf`.

Esta ubicación se puede configurar:

1. Abra el archivo `<carpeta de instalación>/sessionserver/conf/container.conf` en el editor de texto.
2. Edite la propiedad wrapper.java.additional para especificar la nueva ubicación. Si la vía contiene espacios, escríbala entre comillas en Windows o utilice la sintaxis adecuada para las plataformas Linux/Unix. Por ejemplo, `wrapper.java.additional.9=-Djava.io.tmpdir=../tmp`
3. Si es necesario, puede definir una propiedad adicional para suprimir el directorio temporal cuando se cierre el servidor.
4. Reinicie el servidor.

8. Información legal