Configurar OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

Tabla de contenidos

Configurar OnCommand Workflow Automation

Después de completar la instalación de OnCommand Workflow Automation (WFA), debe completar varias opciones de configuración. Tiene que acceder a WFA, configurar usuarios, configurar orígenes de datos, configurar credenciales y configurar WFA.

Acceda a OnCommand Workflow Automation

Puede acceder a OnCommand Workflow Automation (WFA) a través de un navegador web desde cualquier sistema que tenga acceso al servidor WFA.

Debe haber instalado Adobe Flash Player para su explorador web.

Pasos

1. Abra un explorador Web e introduzca una de las siguientes opciones en la barra de direcciones:
   - `https://wfa_server_ip`

     wfa_Server_ip es la dirección IP (dirección IPv4 o IPv6) o el nombre de dominio completo (FQDN) del servidor WFA.

   - Si está accediendo a WFA en el servidor de WFA: `https://localhost/wfa`Si ha especificado un puerto no predeterminado para WFA, debe incluir el número de puerto de la siguiente forma:
   - `https://wfa_server_ip:port`
   - `https://localhost:port`Puerto es el número de puerto TCP que ha utilizado para el servidor WFA durante la instalación.
2. En la sección Iniciar sesión, introduzca las credenciales del usuario administrador que haya introducido durante la instalación.
3. En el menú **Configuración** > **Configuración**, configure las credenciales y un origen de datos.
4. Añada la GUI web de WFA para facilitar el acceso.

Orígenes de datos de OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) funciona con datos que se adquieren de orígenes de datos. Se proporcionan varias versiones de Active IQ Unified Manager y VMware vCenter Server como tipos de origen de datos de WFA predefinidos. Debe tener en cuenta los tipos de origen de datos predefinidos antes de configurar los orígenes de datos para la adquisición de datos.

Un origen de datos es una estructura de datos de sólo lectura que sirve como conexión al objeto de origen de datos de un tipo de origen de datos específico. Por ejemplo, un origen de datos puede ser una conexión a una base de datos Active IQ Unified Manager de un tipo de origen de datos Active IQ Unified Manager 6.3. Puede añadir un origen de datos personalizado a WFA tras definir el tipo de origen de datos necesario.

Para obtener más información sobre los tipos de origen de datos predefinidos, consulte matriz de interoperabilidad.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Configuración de un usuario de base de datos en DataFabric Manager

Debe crear un usuario de base de datos en DataFabric Manager 5.x para configurar el acceso de solo lectura de la base de datos de DataFabric Manager 5.x a OnCommand Workflow Automation.

Configure un usuario de base de datos ejecutando ocsetup en Windows

Puede ejecutar el archivo ocsetup en el servidor DataFabric Manager 5.x para configurar el acceso de solo lectura de la base de datos de DataFabric Manager 5.x a OnCommand Workflow Automation.

Pasos

1. Descargue el archivo wfa_ocsetup.exe en un directorio del servidor DataFabric Manager 5.x desde la siguiente ubicación:

   https://WFA_Server_IP/download/wfa_ocsetup.exe.

   WFA_Server_IP es la dirección IP (dirección IPv4 o IPv6) de su servidor WFA.

   Si ha especificado un puerto no predeterminado para WFA, debe incluir el número de puerto de la siguiente forma:

   https://wfa_server_ip:port/download/wfa_ocsetup.exe.

   Port es el número de puerto TCP que ha utilizado para el servidor WFA durante la instalación.

   Si especifica una dirección IPv6, debe escribirla entre corchetes.

2. Haga doble clic en el archivo wfa_ocsetup.exe.
3. Lea la información del asistente de configuración y haga clic en **Siguiente**.
4. Busque o escriba la ubicación de OpenJDK y haga clic en **Siguiente**.
5. Introduzca un nombre de usuario y una contraseña para anular las credenciales predeterminadas.

   Se crea una nueva cuenta de usuario de la base de datos con acceso a la base de datos DataFabric Manager 5.x.

   > Si no crea una cuenta de usuario, se utilizan las credenciales predeterminadas. Debe crear una cuenta de usuario con fines de seguridad.

6. Haga clic en **Siguiente** y revise los resultados.
7. Haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar** para completar el asistente.

Configurar un usuario de base de datos ejecutando ocsetup en Linux

Puede ejecutar el archivo ocsetup en el servidor DataFabric Manager 5.x para configurar el acceso de solo lectura de la base de datos de DataFabric Manager 5.x a OnCommand Workflow Automation.

Pasos

1. Descargue el archivo wfa_ocsetup.sh en el directorio inicial del servidor DataFabric Manager 5.x mediante el siguiente comando del terminal:

   ```
   wget https://WFA_Server_IP/download/wfa_ocsetup.sh
   ```

   WFA_Server_IP es la dirección IP (dirección IPv4 o IPv6) de su servidor WFA.

   Si ha especificado un puerto no predeterminado para WFA, debe incluir el número de puerto de la siguiente forma:

   ```
   wget https://wfa_server_ip:port/download/wfa_ocsetup.sh
   ```

   Port es el número de puerto TCP que ha utilizado para el servidor WFA durante la instalación.

   Si especifica una dirección IPv6, debe escribirla entre corchetes.

2. Utilice el siguiente comando de la terminal para cambiar el archivo wfa_ocsetup.sh a un ejecutable:

   ```
   chmod +x wfa_ocsetup.sh
   ```

3. Ejecute el script introduciendo lo siguiente en la terminal:

   ```
   ./wfa_ocsetup.sh OpenJDK_path
   ```

   OpenJDK_PATH es la ruta de OpenJDK.

   /Opt/NTAPdfm/java

   La siguiente salida se muestra en el terminal, lo que indica que la configuración se ha realizado correctamente:

   ```
   Verifying archive integrity... All good.
   Uncompressing WFA OnCommand Setup.....
   *** Welcome to OnCommand Setup Utility for Linux ***
       <Help information>
   *** Please override the default credentials below ***
   Override DB Username [wfa] :
   ```

4. Introduzca un nombre de usuario y una contraseña para anular las credenciales predeterminadas.

   Se crea una nueva cuenta de usuario de la base de datos con acceso a la base de datos DataFabric Manager 5.x.

   > Si no crea una cuenta de usuario, se utilizan las credenciales predeterminadas. Debe crear una cuenta de usuario con fines de seguridad.

   La siguiente salida se muestra en el terminal, lo que indica que la configuración se ha realizado correctamente:

```
***** Start of response from the database *****
>>> Connecting to database
<<< Connected
*** Dropped existing 'wfa' user
=== Created user 'username'
>>> Granting access
<<< Granted access
***** End of response from the database *****
***** End of Setup *****
```

Configurar un origen de datos

Debe configurar una conexión con un origen de datos en OnCommand Workflow Automation (WFA) para adquirir datos del origen de datos.

- Para Active IQ Unified Manager 6.0 y versiones posteriores, debe haber creado una cuenta de usuario de base de datos en el servidor de Unified Manager.

  Consulte la ayuda en línea de *OnCommand Unified Manager* para obtener más detalles.

- El puerto TCP para conexiones entrantes en el servidor de Unified Manager debe estar abierto.

  Consulte la documentación del firewall para obtener más detalles.

  A continuación, se muestran los números de puerto TCP predeterminados:

Número de puerto TCP	La versión del servidor de Unified Manager	Descripción
3306	6.x.	Servidor de bases de datos MySQL

- Para Performance Advisor, debe haber creado una cuenta de usuario de Active IQ Unified Manager con una función mínima de GlobalRead.

  Consulte la ayuda en línea de *OnCommand Unified Manager* para obtener más detalles.

- El puerto TCP para conexiones entrantes en VMware vCenter Server debe estar abierto.

  El número de puerto TCP predeterminado es 443. Consulte la documentación del firewall para obtener más detalles.

Puede añadir varias fuentes de datos del servidor de Unified Manager a WFA utilizando este procedimiento. Sin embargo, no debe utilizar este procedimiento si desea emparejar Unified Manager Server 6.3 y versiones posteriores con WFA y utilizar la funcionalidad de protección en el servidor de Unified Manager.

Para obtener más información sobre el emparejamiento de WFA con Unified Manager Server 6.x, consulte la ayuda en línea de *OnCommand Unified Manager*.

> Al configurar un origen de datos con WFA, debe tener en cuenta que los tipos de origen de datos Active IQ Unified Manager 6.0, 6.1 y 6.2 quedan obsoletos en la versión WFA 4.0, por lo que estos tipos de origen de datos no serán compatibles en futuras versiones.

Pasos

1. Acceda a WFA mediante un navegador web.
2. Haga clic en **Configuración** y en **Configuración** haga clic en **fuentes de datos**.
3. Elija la acción adecuada:

Para…	Realice lo siguiente…
Cree un nuevo origen de datos	Haga clic en en la barra de herramientas.
Edite un origen de datos restaurado si ha actualizado WFA	Seleccione la entrada de origen de datos existente y haga clic en en la barra de herramientas.

   Si ha añadido una fuente de datos del servidor de Unified Manager a WFA y, a continuación, actualizado la versión del servidor de Unified Manager, WFA no reconocerá la versión actualizada del servidor de Unified Manager. Debe eliminar la versión anterior del servidor de Unified Manager y, a continuación, añadir la versión actualizada del servidor de Unified Manager a WFA.

4. En el cuadro de diálogo Nuevo origen de datos, seleccione el tipo de origen de datos necesario y escriba un nombre para el origen de datos y el nombre de host.

   Según el tipo de origen de datos seleccionado, los campos de puerto, nombre de usuario, contraseña y tiempo de espera pueden completarse automáticamente con los datos predeterminados, si están disponibles. Puede editar estas entradas según sea necesario.

5. Elija una acción adecuada:

Durante…	Realice lo siguiente…
Active IQ Unified Manager 6.3 y posteriores	Introduzca las credenciales de la cuenta de usuario de la base de datos que creó en el servidor de Unified Manager. Consulte *Ayuda en línea de Unified Manager de OnCommand* para obtener información detallada sobre la creación de una cuenta de usuario de base de datos. No debe proporcionar las credenciales de una cuenta de usuario de base de datos de Active IQ Unified Manager que se creó mediante la interfaz de línea de comandos o la herramienta ocsetup.

6. Haga clic en **Guardar**.
7. En la tabla orígenes de datos, seleccione el origen de datos y haga clic en en la barra de herramientas.
8. Compruebe el estado del proceso de adquisición de datos.

Añada un servidor de Unified Manager actualizado como origen de datos

Si el servidor de Unified Manager (5.x o 6.x) se añade como origen de datos a WFA y, a continuación, se actualiza el servidor de Unified Manager, Debe añadir el servidor actualizado de Unified Manager como origen de datos porque los datos asociados con la versión actualizada no se rellenan en WFA, a menos que se añadan manualmente como un origen de datos.

Pasos

1. Inicie sesión en la GUI web de WFA como administrador.
2. Haga clic en **Configuración** y en **Configuración**, haga clic en **fuentes de datos**.
3. Haga clic en en la barra de herramientas.
4. En el cuadro de diálogo Nuevo origen de datos, seleccione el tipo de origen de datos necesario y, a continuación, escriba un nombre para el origen de datos y el nombre de host.

   Según el tipo de origen de datos seleccionado, los campos de puerto, nombre de usuario, contraseña y tiempo de espera pueden completarse automáticamente con los datos predeterminados, si están disponibles. Puede editar estas entradas según sea necesario.
5. Haga clic en **Guardar**.
6. Seleccione la versión anterior del servidor de Unified Manager y haga clic en en la barra de herramientas.
7. En el cuadro de diálogo de confirmación Eliminar tipo de origen de datos, haga clic en **Sí**.
8. En la tabla orígenes de datos, seleccione el origen de datos y, a continuación, haga clic en en la barra de herramientas.
9. Compruebe el estado de la adquisición de datos en la tabla Historial.

Crear usuarios locales

OnCommand Workflow Automation (WFA) le permite crear y gestionar usuarios WFA locales con permisos específicos para distintos roles, como invitado, operador, aprobador, arquitecto administrador y backup.

Debe haber instalado WFA y haber iniciado sesión como administrador.

WFA permite crear usuarios para los siguientes roles:

- **Invitado**

  Este usuario puede ver el portal y el estado de una ejecución de flujo de trabajo, y se le puede notificar de un cambio en el estado de una ejecución de flujo de trabajo.

- **Operador**

  Este usuario puede obtener una vista previa y ejecutar flujos de trabajo para los que tiene acceso el usuario.

- **Approver**

Este usuario puede obtener una vista previa de los flujos de trabajo, ejecutarlos, aprobarlos y rechazarlos para los que el usuario tiene acceso.

> Se recomienda proporcionar el ID de correo electrónico del aprobador. Si hay varios autorizadores, puede proporcionar un ID de correo electrónico de grupo en el campo **correo electrónico**.

- **Arquitecto**

  Este usuario tiene acceso completo para crear flujos de trabajo, pero está restringido a la modificación de la configuración global del servidor WFA.

- **Admin**

  Este usuario tiene acceso completo al servidor WFA.

- **Backup**

  Este es el único usuario que puede generar copias de seguridad del servidor WFA de forma remota. Sin embargo, el usuario está restringido de todos los demás accesos.

Pasos

1. Haga clic en **Configuración** y en **Administración** haga clic en **usuarios**.
2. Para crear un nuevo usuario, haga clic en en la barra de herramientas.
3. Introduzca la información necesaria en el cuadro de diálogo Nuevo usuario.
4. Haga clic en **Guardar**.

Configure las credenciales de un sistema de destino

Puede configurar las credenciales de un sistema de destino en OnCommand Workflow Automation (WFA) y utilizar las credenciales para conectarse a ese sistema específico y ejecutar comandos.

Después de la adquisición de datos inicial, es necesario configurar las credenciales de las cabinas donde se ejecutan los comandos. La conexión de la controladora WFA de PowerShell funciona en dos modos:

- Con credenciales

  WFA intenta establecer una conexión mediante HTTPS primero y, a continuación, intenta utilizar HTTP. También puede utilizar la autenticación LDAP de Microsoft Active Directory para conectarse a cabinas sin definir credenciales en WFA. Para utilizar LDAP de Active Directory, debe configurar la matriz para realizar la autenticación con el mismo servidor LDAP de Active Directory.

- Sin credenciales (para sistemas de almacenamiento que funcionan en 7-Mode)

  WFA intenta establecer una conexión mediante autenticación de dominio. Este modo utiliza el protocolo de llamada a procedimiento remoto, que se asegura mediante el protocolo NTLM.

- WFA comprueba el certificado de capa de sockets seguros (SSL) para los sistemas ONTAP. Es posible que se pida a los usuarios que revisen y acepten/denieguen la conexión a sistemas ONTAP si el certificado SSL no es de confianza.

- Debe volver a introducir las credenciales de ONTAP, Active IQ de NetApp y LDAP después de restaurar un backup o completar una actualización sin movimiento.

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Haga clic en **Configuración** y en **Configuración** haga clic en **credenciales**.
3. Haga clic en en la barra de herramientas.
4. En el cuadro de diálogo nuevas credenciales, seleccione una de las siguientes opciones de la lista **coincidencia**:

   - **Exact**

     Credenciales para una dirección IP o un nombre de host específicos

   - **Patrón**

     Credenciales para toda la subred o el intervalo IP

     Esta opción no admite el uso de sintaxis de expresiones regulares.

5. Seleccione el tipo de sistema remoto en la lista **Tipo**.
6. Introduzca el nombre de host o la dirección IPv4 o IPv6 del recurso, el nombre de usuario y la contraseña.

   WFA 5.1 verifica los certificados SSL de todos los recursos que se han añadido a WFA. Como verificación de certificado puede solicitar la aceptación de los certificados, no se admite el uso de caracteres comodín en las credenciales. Si tiene varios clústeres utilizando las mismas credenciales, no puede añadirlos de una vez.

7. Realice la acción siguiente para probar la conectividad:

Si ha seleccionado el siguiente tipo de coincidencia…	Realice lo siguiente…
Exact	Haga clic en **Prueba**.
Patrón	Guarde las credenciales y elija una de las siguientes opciones: • Seleccione la credencial y haga clic en en la barra de herramientas. • Haga clic con el botón derecho del ratón y seleccione **probar conectividad**.

8. Haga clic en **Guardar**.

Configurando OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) le permite configurar diversos ajustes, por ejemplo, AutoSupport y notificaciones.

Al configurar WFA, puede configurar una o varias de las siguientes opciones, según sea necesario:

- AutoSupport para enviar mensajes de AutoSupport al soporte técnico
- Servidor de Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) para la autenticación y autorización de LDAP para usuarios de WFA
- Envíe por correo electrónico notificaciones sobre operaciones de flujo de trabajo y mensajes de AutoSupport
- Protocolo simple de gestión de red (SNMP) para recibir notificaciones sobre operaciones de flujos de trabajo
- Syslog para registro remoto de datos

Configure AutoSupport

Puede configurar varias opciones de AutoSupport, como la programación, el contenido de los mensajes de AutoSupport y el servidor proxy. AutoSupport envía registros semanales del contenido seleccionado al soporte técnico para archivado y análisis de problemas.

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Haga clic en **Configuración** y en **Configuración** haga clic en **AutoSupport**.
3. Asegúrese de que la casilla **Activar AutoSupport** está seleccionada.
4. Especifique la información obligatoria.
5. Seleccione una de las siguientes opciones en la lista **Contenido**:

Si desea incluir…	Elija esta opción…
Solo detalles de configuración como usuarios, flujos de trabajo y comandos de la instalación de WFA	enviar sólo datos de configuración
Detalles de configuración DE WFA y datos en tablas de caché de WFA como el esquema	envío de datos de configuración y caché (predeterminado)
Detalles de configuración DE WFA, datos en tablas de caché de WFA y datos en el directorio de instalación	envío de datos ampliados de configuración y caché

La contraseña de cualquier usuario de WFA se *no* incluye en los datos de AutoSupport.

6. Compruebe que puede descargar un mensaje de AutoSupport:
   a. Haga clic en **Descargar**.
   b. En el cuadro de diálogo que se abre, seleccione la ubicación para guardar el archivo .7z.
7. Pruebe el envío de un mensaje AutoSupport al destino especificado haciendo clic en **Enviar ahora**.
8. Haga clic en **Guardar**.

Configure las opciones de autenticación

Puede configurar OnCommand Workflow Automation (WFA) para que utilice un servidor de protocolo ligero de acceso a directorios (LDAP) de Microsoft Active Directory (AD) para autenticación y autorización.

Debe haber configurado un servidor LDAP de Microsoft AD en el entorno.

Solo se admite la autenticación de Microsoft AD LDAP para WFA. No puede utilizar ningún otro método de autenticación LDAP, incluidos Microsoft AD Lightweight Directory Services (AD LDS) o el catálogo global de Microsoft.

> Durante la comunicación, LDAP envía el nombre de usuario y la contraseña en texto sin formato. Sin embargo, la comunicación LDAPS (LDAP Secure) es cifrada y segura.

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Agregue una lista de nombres de grupos de Active Directory a las funciones necesarias.

   > Puede agregar una lista de nombres de grupos de AD a los roles requeridos en la ventana grupos de Active Directory.

   Grupos de Active Directory

3. Haga clic en **Administración** > **Configuración de WFA**.
4. En el cuadro de diálogo Configuración de WFA, haga clic en la ficha **autenticación** y, a continuación, active la casilla de verificación **Activar Active Directory**.
5. Introduzca la información obligatoria en los campos:
   a. Si desea utilizar el formato user@domain para usuarios de dominio, reemplace sAMAccountName por userPrincipalName en el campo **Nombre de usuario**.
   b. Si se requieren valores únicos para el entorno, edite los campos obligatorios.
6. Haga clic en **Agregar** para agregar Active Directory en la tabla servidores de Active Directory con un formato URI: `ldap://active_directory_server_address\[:port\]`

   ldap://NB-T01.example.com[:389]

   Si ha habilitado LDAP sobre SSL, puede usar el siguiente formato URI: `ldaps://active_directory_server_address\[:port\]`

7. Proporcione las credenciales para enlazar el servidor LDAP y el DN base.
8. Pruebe la autenticación del usuario dado:
   a. Introduzca el nombre de usuario y la contraseña.
   b. Haga clic en **probar autenticación**.

   > Debe haber agregado el grupo de Active Directory para probar la autenticación del usuario especificado en WFA.

9. Haga clic en **Guardar**.

Agregar grupos de Active Directory

Puede agregar grupos de Active Directory en OnCommand Workflow Automation (WFA).

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Haga clic en **Configuración** y en **Administración**, haga clic en **grupos de Active Directory**.
3. En la ventana grupos de Active Directory, haga clic en el icono **Nuevo**.
4. En el cuadro de diálogo New Active Directory Group, introduzca la información necesaria.

   Si selecciona **Approver** en la lista desplegable **rol**, se recomienda proporcionar el ID de correo electrónico del aprobador. Si hay varios autorizadores, puede proporcionar un ID de correo electrónico de grupo en el campo **correo electrónico**. Seleccione los diferentes eventos del flujo de trabajo para el que se enviará la notificación al grupo de Active Directory concreto.

5. Haga clic en **Guardar**.

Configure las notificaciones por correo electrónico

Puede configurar OnCommand Workflow Automation (WFA) para que le envíe notificaciones por correo electrónico acerca de las operaciones del flujo de trabajo, por ejemplo, el flujo de trabajo iniciado o el flujo de trabajo con errores.

Debe haber configurado un host de correo en el entorno.

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Haga clic en **Configuración** y en **Configuración** haga clic en **correo**.
3. Introduzca la información obligatoria en los campos.
4. Pruebe la configuración de correo realizando los siguientes pasos:
   a. Haga clic en **Enviar correo de prueba**.
   b. En el cuadro de diálogo probar conexión, introduzca la dirección de correo electrónico a la que desea enviar el correo electrónico.
   c. Haga clic en **Prueba**.
5. Haga clic en **Guardar**.

Configure SNMP

Puede configurar OnCommand Workflow Automation (WFA) para que envíe capturas de protocolo simple de gestión de redes (SNMP) acerca del estado de las operaciones del flujo de trabajo.

WFA ahora admite los protocolos SNMP v1 y SNMP v3. SNMP v3 ofrece funciones de seguridad adicionales.

El archivo WFA .mib proporciona información sobre las capturas que envía el servidor WFA. El archivo .mib se encuentra en el directorio <WFA_install_location>\wfa\bin\wfa.mib del servidor WFA.

El servidor WFA envía todas las notificaciones de captura con un identificador de objeto genérico (1.3.6.1.4.1.789.1.1.12.0).

No se pueden usar cadenas de la comunidad SNMP como Community_String@SNMP_host para la configuración de SNMP.

Configurar syslog

Puede configurar OnCommand Workflow Automation (WFA) para que envíe datos del registro a un servidor de syslog específico con fines como el registro de eventos y el análisis de información de registros.

Debe haber configurado el servidor de syslog para aceptar datos del servidor de WFA.

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Haga clic en **Configuración** y en **Mantenimiento** haga clic en **Syslog**.
3. Active la casilla de verificación **Activar Syslog**.
4. Introduzca el nombre de host de syslog y seleccione el nivel de registro de syslog.
5. Haga clic en **Guardar**.

Configurar protocolos para conectarse a sistemas remotos

Puede configurar el protocolo utilizado por OnCommand Workflow Automation (WFA) para conectarse a sistemas remotos. Puede configurar el protocolo en función de los requisitos de seguridad de su organización y del protocolo que admite el sistema remoto.

Pasos

1. Inicie sesión en WFA a través de un navegador web como administrador.
2. Haga clic en **Diseño de origen de datos** > **tipos de sistema remoto**.
3. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Configurar un protocolo para un nuevo sistema remoto	a. Haga clic en . b. En el cuadro de diálogo Nuevo tipo de sistema remoto, especifique los detalles como el nombre, la descripción y la versión.
Modifique la configuración del protocolo de un sistema remoto existente	a. Seleccione y haga doble clic en el sistema remoto que desee modificar. b. Haga clic en .

4. En la lista Protocolo de conexión, seleccione una de las siguientes opciones:
   - HTTPS con conmutación al HTTP (predeterminada)

- Solo HTTPS
- Solo HTTP
- Personalizado

5. Especifique los detalles para el protocolo, el puerto predeterminado y el tiempo de espera predeterminado.
6. Haga clic en **Guardar**.

Desactive la directiva de contraseñas predeterminada

OnCommand Workflow Automation (WFA) está configurado para implementar una política de contraseñas para los usuarios locales. Si no desea usar la política de contraseñas, puede deshabilitarla.

Debe haber iniciado sesión en el sistema host de WFA como usuario raíz.

La ruta de instalación predeterminada de WFA se utiliza en este procedimiento. Si ha cambiado la ubicación predeterminada durante la instalación, debe utilizar la ruta de instalación de WFA cambiada.

Pasos

1. En la confirmación del shell, desplácese hasta el siguiente directorio del servidor de WFA: WFA_install_location/wfa/bin/
2. Introduzca el siguiente comando:

```
./wfa --password-policy=none --restart=WFA
```

Modifique la política de contraseñas predeterminada

OnCommand Workflow Automation (WFA) está configurado para implementar una política de contraseñas para los usuarios locales. Puede modificar la política de contraseñas predeterminada.

Debe haber iniciado sesión en el sistema host de WFA como usuario raíz.

- La ruta de instalación predeterminada de WFA se utiliza en este procedimiento.

  Si ha cambiado la ubicación predeterminada durante la instalación, debe utilizar la ruta de instalación de WFA cambiada.

- El comando para la directiva de contraseñas predeterminada es ./wfa --password-policy=default.

  El valor predeterminado es "minLength=true,8;specialChar=true,1;digitalChar=true,1;lowercaseChar=true,1;uppercaseChar=true,1;espaceChar=false" . Esto indica que la política de contraseña predeterminada debe tener una longitud mínima de ocho caracteres, debe contener al menos 1 carácter especial, 1 dígito, 1 carácter en minúscula, 1 carácter en mayúscula y sin espacios.

Pasos

1. En la confirmación del shell, desplácese hasta el siguiente directorio del servidor de WFA: WFA_install_location/wfa/bin/

2. Modifique la política de contraseña predeterminada introduciendo el comando siguiente:

```
./wfa --password-policy=PasswordPolicyString --restart=WFA
```

Habilite o deshabilite el acceso remoto a la base de datos de OnCommand Workflow Automation

De forma predeterminada, solo los clientes que se ejecutan en el sistema host de WFA pueden acceder a la base de datos OnCommand Workflow Automation (WFA). Puede cambiar la configuración predeterminada si desea habilitar el acceso a la base de datos de WFA desde un sistema remoto.

- Debe haber iniciado sesión en el sistema host de WFA como usuario raíz.
- Si hay un firewall instalado en el sistema host de WFA, debe haber configurado la configuración del firewall para permitir el acceso al puerto MySQL (3306) desde el sistema remoto.

La ruta de instalación predeterminada de WFA se utiliza en este procedimiento. Si ha cambiado la ubicación predeterminada durante la instalación, debe utilizar la ruta de instalación de WFA cambiada.

Pasos

1. Desplácese hasta el siguiente directorio del servidor WFA: WFA_install_location/wfa/bin/.
2. Ejecute una de las siguientes acciones:

Para…	Introduzca el siguiente comando…
Habilite el acceso remoto	`./wfa --db-access=public --restart`
Desactivar el acceso remoto	`./wfa --db-access=default --restart`

Modifique la configuración de tiempo de espera de transacción de OnCommand Workflow Automation

De forma predeterminada, la transacción de la base de datos OnCommand Workflow Automation (WFA) se agota en 300 segundos. Puede aumentar la duración del tiempo de espera predeterminado al restaurar una base de datos WFA de gran tamaño desde un backup para evitar un posible fallo de la restauración de la base de datos.

Debe haber iniciado sesión en el sistema host de WFA como usuario raíz.

La ruta de instalación predeterminada de WFA se utiliza en este procedimiento. Si ha cambiado la ubicación predeterminada durante la instalación, debe utilizar la ruta de instalación de WFA cambiada.

Pasos

1. En la confirmación del shell, desplácese hasta el siguiente directorio del servidor de WFA: WFA_install_location/wfa/bin/
2. Introduzca el siguiente comando:

```
./wfa --txn-timeout[=TIMEOUT] --restart=WFA

./wfa --txn-timeout=1000 --restart=WFA
```

Configure el valor del tiempo de espera para Workflow Automation

Puede configurar el valor de tiempo de espera para la interfaz gráfica de usuario web de Workflow Automation (WFA), en lugar de utilizar el valor de tiempo de espera predeterminado de 180 segundos.

El valor de tiempo de espera que se establece es un tiempo de espera absoluto en lugar de un tiempo de espera relacionado con la inactividad. Por ejemplo, si establece este valor en 30 minutos, se cerrará la sesión después de 30 minutos, incluso si está activo al final de este tiempo. No puede configurar el valor de tiempo de espera desde la interfaz gráfica de usuario web de WFA.

Pasos

1. Inicie sesión como usuario raíz en el equipo host de WFA.
2. Establezca el valor del tiempo de espera:

```
installdir bin/wfa -S=timeout value in minutes
```

Habilitar cifrados y añadir nuevos cifrados

OnCommand Workflow Automation 5.1 admite una serie de cifrados listas para usar. También puede añadir cifrados adicionales según sea necesario.

Se pueden habilitar los siguientes cifrados de la caja:

```
enabled-cipher-suites=
"TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,T
LS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA38
4,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384"
```

Puede agregar cifrados adicionales a esta configuración en la `standalone-full.xml` archivo. Este archivo está ubicado en el directorio: `<installdir>/jboss/standalone/configuration/standalone-full.xml`.

El archivo se puede modificar para admitir códigos adicionales de la siguiente manera:

```
<https-listener name="https" socket-binding="https" max-post-
size="1073741824" security-realm="SSLRealm"
enabled-cipher-suites="**< --- add additional ciphers here ---\>**
enabled-protocols="TLSv1.1,TLSv1.2"/>
```