



Configure OnCommand Workflow Automation

OnCommand Workflow Automation 5.0

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/es-es/workflow-automation-50/rhel-install/task-access-oncommand-workflow-automation.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Configure OnCommand Workflow Automation. 1
 - Acceda a OnCommand Workflow Automation 1
 - Orígenes de datos de OnCommand Workflow Automation 1
 - Crear usuarios locales 7
 - Configure las credenciales de un sistema de destino 8
 - Configurando OnCommand Workflow Automation 9
 - Desactive la directiva de contraseñas predeterminada 14
 - Modifique la política de contraseñas predeterminada 14
 - Habilite o deshabilite el acceso remoto a la base de datos de OnCommand Workflow Automation. 15
 - Modifique la configuración de tiempo de espera de transacción de OnCommand Workflow Automation. . . 15
 - Configure el valor del tiempo de espera para Workflow Automation 16

Configure 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.

Lo que necesitará

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+ Port` 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. **Opcional:** en el menú **Ajustes > Configuración**, configure las credenciales y un origen de datos.
4. **Opcional:** Añada un marcador a 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. Varias versiones de Data Center Manager de Active IQ y VMware vCenter Server se proporcionan 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 del Administrador de centros de datos Active IQ de un tipo de origen de datos de Active IQ Data Center 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.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Configuración de un usuario de base de datos en el Administrador del centro de datos de Active IQ

Debe crear un usuario de base de datos en versiones anteriores a 6.0 de Active IQ para configurar el acceso de sólo lectura de la base de datos del Administrador de centros de datos de Active IQ a OnCommand Workflow Automation.

Configure un usuario de base de datos ejecutando ocsetup en Windows

Puede ejecutar el `ocsetup` Archivo en el servidor del Administrador de centros de datos de Active IQ para configurar el acceso de sólo lectura de la base de datos del Administrador de centros de datos de Active IQ a OnCommand Workflow Automation.

Pasos

1. Descargue el `wfa_ocsetup.exe` Archivo a un directorio del servidor del Administrador de centros de datos de Active IQ 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 del JRE 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 del Administrador de centros de datos de Active IQ.



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 `ocsetup` Archivo en el servidor del Administrador de centros de datos de Active IQ para configurar el acceso de sólo lectura de la base de datos del

Administrador de centros de datos de Active IQ a OnCommand Workflow Automation.

Pasos

1. Descargue el `wfa_ocsetup.sh` Archivo en el directorio inicial del servidor Active IQ Data Center Manager mediante el siguiente comando de la 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 en la terminal para cambiar el `wfa_ocsetup.sh` archivo a un ejecutable:

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

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

```
./wfa_ocsetup.sh JRE_path
```

JRE_PATH es la ruta de acceso al JRE.

ejemplo

```
/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 del Administrador de centros de datos de Active IQ.



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.

Lo que necesitará

- Para versiones de Active IQ Data Center Manager anteriores a la 6.0, debe haber ejecutado la última versión de la herramienta de configuración en el servidor de Data Center Manager para habilitar y configurar el acceso remoto de sólo lectura a la base de datos.
- Para Active IQ Data Center Manager 6.0 y posterior, debe haber creado una cuenta de usuario de base de datos en el servidor Data Center Manager.

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

- El puerto TCP para las conexiones entrantes en el servidor de Data Center 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 | Versión del servidor de Data Center Manager | Descripción |
|----------------------|---|---|
| 2638 | 5.x. | Servidor de bases de datos SQL Anywhere de Sybase |
| 3306 | 6.x. | Servidor de bases de datos MySQL |

- Para Performance Advisor, debe haber creado una cuenta de usuario del Administrador de centros de datos de Active IQ 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.

Acerca de esta tarea

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



Para obtener más información acerca del emparejamiento de WFA con el servidor de Data Center Manager 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 Data Center 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 agregado una fuente de datos del servidor de Data Center Manager a WFA y, a continuación, actualizado la versión del servidor de Data Center Manager, WFA no reconocerá la versión actualizada del servidor Data Center Manager. Debe eliminar la versión anterior del servidor de Data Center Manager y, a continuación, agregar la versión actualizada del servidor de Data Center Manager a WFA.


4. En el cuadro de diálogo **Nuevo origen de datos**, seleccione el tipo de origen de datos necesario e introduzca 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... |
|--|--|
| Versiones de Data Center Manager de Active IQ anteriores a 6.0 | Introduzca el nombre de usuario y la contraseña que utilizó para reemplazar las credenciales predeterminadas mientras ejecuta la herramienta de configuración. |


| Durante... | Realice lo siguiente... |
|--|---|
| Active IQ Data Center Manager 6.3 y versiones posteriores | Introduzca las credenciales de la cuenta de usuario de base de datos que creó en el servidor de Data Center Manager. Consulte <i>Ayuda en línea de Unified Manager de OnCommand</i> para obtener información detallada sobre la creación de una cuenta de usuario de base de datos. |
| Performance Advisor para (versiones de Active IQ Data Center Manager anteriores a 6.0) | <p>Introduzca las credenciales de un usuario del Administrador de centros de datos de Active IQ con el rol mínimo de GlobalRead.</p> <div>  <p>No debe proporcionar las credenciales de una cuenta de usuario de base de datos de Active IQ Data Center Manager que se haya creado mediante la interfaz de línea de comandos o la herramienta de configuración.</p> </div> |

- Haga clic en **Guardar**.
- Opcional:** en la tabla orígenes de datos, seleccione el origen de datos y haga clic en  en la barra de herramientas.
- Compruebe el estado del proceso de adquisición de datos.


Agregar un servidor actualizado de Data Center Manager como origen de datos


Si el servidor de Data Center Manager (5.x o 6.x) se añade como origen de datos a WFA y, a continuación, se actualiza el servidor de Data Center Manager. Debe agregar el servidor actualizado de Data Center Manager como un 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

- Inicie sesión en la GUI web de WFA como administrador.
- Haga clic en **Configuración** y en **Configuración**, haga clic en **fuentes de datos**.
- Haga clic en  en la barra de herramientas.
- 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.

- Haga clic en **Guardar**.
- Seleccione la versión anterior del servidor de Data Center 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. **Opcional:** 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.

Lo que necesitará

Debe haber instalado WFA y haber iniciado sesión como administrador.

Acerca de esta tarea

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.

Acerca de esta tarea

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.

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 **credenciales nuevas**, 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

Puede utilizar la sintaxis de expresiones regulares para esta opción.
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.
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 | <p>Guarde las credenciales y elija una de las siguientes opciones:</p> <ul style="list-style-type: none"> • 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 (ASUP) para enviar mensajes de ASUP 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 un correo electrónico para notificaciones por correo electrónico sobre operaciones de flujo de trabajo y envío de mensajes de ASUP
- 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. **Opcional:** Compruebe que puede descargar un mensaje de AutoSupport:

- Haga clic en **Descargar**.
- En el cuadro de diálogo que se abre, seleccione la ubicación en la que desea guardar .7z archivo.

7. **Opcional:** 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.

Lo que necesitará

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

Acerca de esta tarea

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. Haga clic en **Configuración** y en **Configuración** haga clic en **autenticación**.
3. Active la casilla de verificación **Activar Active Directory**.
4. Introduzca la información obligatoria en los campos:
 - a. **Opcional:** Si desea utilizar el formato *USER@Domain* para usuarios de dominio, reemplace sAMAccountName con userPrincipalName En el campo **atributo de nombre de usuario**.

b. **Opcional:** Si se requieren valores únicos para su entorno, edite los campos necesarios.

c. Introduzca el URI del servidor AD de la siguiente manera: +

`ldap://active_directory_server_address[:port]+ ejemplo`

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

Si ha habilitado LDAP sobre SSL, puede usar el siguiente formato URI:

`ldaps://active_directory_server_address[:port]`

a. Añadir una lista de nombres de grupos de AD con los roles requeridos.



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

5. 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 **Nuevo grupo de Active Directory**, 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.

Lo que necesitará

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. **Opcional:** Pruebe los ajustes 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.

Acerca de esta tarea

La WFA .mib El archivo proporciona información acerca de las capturas que envía el servidor de WFA. La .mib el archivo se encuentra en la <WFA_install_location>\wfa\bin\wfa.mib directorio en el servidor de 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 comunidad SNMP como *Community_String@SNMP_host* para la configuración de SNMP.

Pasos

1. Inicie sesión en WFA a través de un navegador web como usuario administrador y acceda al servidor de WFA.
2. Haga clic en **Configuración** y en **Configuración** haga clic en **SNMP**.
3. Active la casilla de verificación **Activar SNMP**.
4. Introduzca una dirección IPv4 o IPv6 o el nombre de host y el número de puerto del host de gestión.

WFA envía capturas SNMP al número de puerto especificado. El número de puerto predeterminado es 162.

5. En la sección **notificar**, seleccione una o varias de las siguientes casillas de verificación:
 - Se inició la ejecución del flujo de trabajo
 - La ejecución del flujo de trabajo se ha realizado correctamente
 - La ejecución del flujo de trabajo ha fallado o se ha realizado correctamente
 - Ejecución del flujo de trabajo en espera de aprobación
 - Error de adquisición
6. Haga clic en **Enviar notificación de prueba** para comprobar la configuración.
7. Haga clic en **Guardar**.

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.

Lo que necesitará

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 **Diseñador > tipos de sistema remoto**.
3. Ejecute una de las siguientes acciones:

| Si desea... | Realice lo siguiente... |
|---|---|
| Configurar un protocolo para un nuevo sistema remoto | <ol style="list-style-type: none">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 | <ol style="list-style-type: none">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.

Lo que necesitará

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

Acerca de esta tarea

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 el símbolo del sistema del shell, desplácese hasta el siguiente directorio en el 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.

Lo que necesitará

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

Acerca de esta tarea

- 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 de la política de contraseñas predeterminada es `./wfa --password-policy=default`.

El valor predeterminado es

"minLength=true,6;specialChar=true,1;digitalChar=true,1;lowercaseChar=true,1;uppercaseChar=true,1;spaceChar=false".

Esto indica que la política de contraseña predeterminada debe tener una longitud mínima de 6 caracteres, debe contener al menos 1 carácter especial, 1 dígito, 1 carácter en minúscula, 1 carácter en mayúscula y sin espacios.

Pasos

1. En el símbolo del sistema del shell, desplácese hasta el siguiente directorio en el 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.

Lo que necesitará

- 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.

Acerca de esta tarea

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 | <code>./wfa --db-access=public --restart</code> |
| Desactivar el acceso remoto | <code>./wfa --db-access=default --restart</code> |

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.

Lo que necesitará

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

Acerca de esta tarea

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 el símbolo del sistema del shell, desplácese hasta el siguiente directorio en el servidor de WFA:

```
WFA_install_location/wfa/bin/
```

2. Introduzca el siguiente comando:

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

ejemplo

```
./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.

Acerca de esta tarea

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:

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

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.