



Configurando OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

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

Tabla de contenidos

- Configurando OnCommand Workflow Automation. 1
 - Configure AutoSupport. 1
 - Configure las opciones de autenticación 2
 - Agregar grupos de Active Directory 3
 - Configure las notificaciones por correo electrónico 3
 - Configure SNMP 3
 - Configurar syslog 5
 - Configurar protocolos para conectarse a sistemas remotos 6

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	send only configuration data
Detalles de configuración DE WFA y datos en tablas de caché de WFA como el esquema	send configuration and cache data (predeterminado)
Detalles de configuración DE WFA, datos en tablas de caché de WFA y datos en el directorio de instalación	send configuration and cache extended data



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. 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. 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.
 - c. Introduzca el URI del servidor AD de la siguiente forma:
`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\]`

- 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**.
6. Si es necesario tener conectividad LDAP con una cabina, configure el servicio WFA para que inicie sesión como usuario de dominio necesario:
 - a. Abra la consola de servicios de Windows mediante Services.msc.

- b. Haga doble clic en el servicio * WFA Server* de NetApp.
- c. En el cuadro de diálogo Propiedades del servidor WFA de NetApp, haga clic en la ficha **Iniciar sesión** y, a continuación, seleccione **esta cuenta**.
- d. Introduzca el nombre de usuario y la contraseña del dominio y, a continuación, haga clic en **Aceptar**.

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 la versión 1 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. En la lista desplegable **Versión**, seleccione **Versión 1**.
5. 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.

6. En la sección notificar, seleccione una o más 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
7. Haga clic en **Enviar notificación de prueba** para comprobar la configuración.
8. Haga clic en **Guardar**.

Configurar SNMP versión 3

También puede configurar OnCommand Workflow Automation (WFA) para que envíe capturas de protocolo simple de gestión de redes (SNMP) versión 3 acerca del estado de las operaciones del flujo de trabajo.

La versión 3 ofrece dos opciones de seguridad adicionales:

- Versión 3 con autenticación

Los retos se envían sin cifrar a través de la red. Las aplicaciones de gestión SNMP, que se configuran con los mismos parámetros de autenticación que los mensajes de captura SNMP, pueden recibir capturas.

- Versión 3 con autenticación y cifrado

Las capturas se envían cifradas a través de la red. Para recibir y descifrar estas capturas, debe configurar aplicaciones de administración SNMP con los mismos parámetros de autenticación y clave de cifrado que las capturas 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. En la lista desplegable **Versión**, seleccione una de las siguientes opciones:
 - Versión 3
 - Versión 3 con autenticación
 - Versión 3 con autenticación y cifrado
5. Seleccione las opciones de configuración de SNMP que correspondan a la opción específica de la versión 3 de SNMP que seleccionó en el paso 4.
6. 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.
7. En la sección notificar, seleccione una o más de las siguientes casillas de verificación:
 - La planificación del flujo de trabajo se ha iniciado, ha fallado o ha finalizado
 - 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/ se ha realizado parcialmente correctamente
 - Ejecución del flujo de trabajo en espera de aprobación
 - Error de adquisición
8. Haga clic en **Enviar notificación de prueba** para comprobar la configuración.
9. 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.

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	<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**.

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.