



Configuración de las relaciones de protección en Unified Manager

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

This PDF was generated from <https://docs.netapp.com/es-es/oncommand-unified-manager-95/health-checker/task-configuring-a-connection-between-workflow-automation-and-unified-manager.html> on December 20, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Configuración de las relaciones de protección en Unified Manager 1
 - Antes de empezar 1
 - Pasos 1
 - Configuración de una conexión entre Workflow Automation y Unified Manager 1
 - Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation 2
 - Crear una relación de protección de SnapMirror desde la página de detalles Health/Volume 3
 - Crear una relación de protección SnapVault desde la página de detalles Health/Volume 4
 - Creación de una política de SnapVault para maximizar la eficiencia de transferencia 5
 - Creación de una política de SnapMirror para maximizar la eficiencia de transferencia 6
 - Crear programaciones de SnapMirror y SnapVault 6

Configuración de las relaciones de protección en Unified Manager

Hay varios pasos que debe realizar para usar Unified Manager y OnCommand Workflow Automation a fin de configurar las relaciones de SnapMirror y SnapVault para proteger sus datos.

Antes de empezar

- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.
- Debe haber establecido relaciones entre iguales entre dos clústeres o dos máquinas virtuales de almacenamiento (SVM).
- OnCommand Workflow Automation debe integrarse con Unified Manager:
 - [Configure OnCommand Workflow Automation](#)
 - [Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation](#)

Pasos

1. Según el tipo de relación de protección que desee crear, realice una de las siguientes acciones:
 - [Cree una relación de protección de SnapMirror.](#)
 - [Cree una relación de protección SnapVault.](#)
2. Si desea crear una directiva para la relación, en función del tipo de relación que esté creando, realice una de las siguientes acciones:
 - [Cree una política de SnapVault.](#)
 - [Cree una política de SnapMirror.](#)
3. [Cree una programación de SnapMirror o SnapVault.](#)

Configuración de una conexión entre Workflow Automation y Unified Manager

Puede configurar una conexión segura entre OnCommand Workflow Automation (WFA) y Unified Manager. La conexión a Workflow Automation le permite usar funciones de protección como flujos de trabajo de configuración de SnapMirror y SnapVault, así como comandos para gestionar las relaciones de SnapMirror.

Antes de empezar

- La versión instalada de Workflow Automation debe ser 4.2 o superior.
- Debe haber instalado «paquete WFA para gestionar Clustered Data ONTAP», versión 9.5.0 o superior en el servidor WFA. Puede descargar el paquete requerido en el almacén de automatización del almacenamiento de NetApp.


"PAQUETE WFA para gestionar ONTAP"

- Debe tener el nombre del usuario de la base de datos que ha creado en Unified Manager para admitir conexiones de WFA y Unified Manager.

Este usuario de la base de datos debe haber sido asignado el rol de usuario del Esquema de integración.

- Debe tener asignado la función de administrador o de arquitecto en Workflow Automation.
- Debe tener la dirección de host, el número de puerto 443, el nombre de usuario y la contraseña para la configuración de Workflow Automation.
- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.

Pasos

1. En la barra de herramientas, haga clic en  Y, a continuación, haga clic en **Workflow Automation** en el menú de configuración de la izquierda.
2. En el área **Usuario** de base de datos de OnCommand Unified Manager de la página **Configuración/Automatización de flujo de trabajo**, seleccione el nombre e introduzca la contraseña del usuario de base de datos que creó para admitir conexiones de Unified Manager y Workflow Automation.
3. En el área **credenciales de OnCommand Workflow Automation** de la página **Configuración/Automatización de flujo de trabajo**, introduzca el nombre de host o la dirección IP (IPv4 o IPv6) y el nombre de usuario y la contraseña para la configuración de Workflow Automation.

Debe utilizar el puerto del servidor de Unified Manager (puerto 443).

4. Haga clic en **Guardar**.
5. Si utiliza un certificado autofirmado, haga clic en **Sí** para autorizar el certificado de seguridad.

Aparece la página Setup/Workflow Automation.

6. Haga clic en **Sí** para volver a cargar la interfaz de usuario web y agregar las funciones de Workflow Automation.

Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation

Puede determinar si el almacenamiento en caché de origen de datos de Unified Manager funciona correctamente comprobando si la adquisición del origen de datos se ha realizado correctamente en Workflow Automation. Puede hacerlo cuando se integre Workflow Automation con Unified Manager para garantizar que la funcionalidad Workflow Automation esté disponible después de la integración.

Antes de empezar

Para realizar esta tarea, debe tener asignado la función Administrador o la función Arquitecto de Workflow Automation.

Pasos

1. En la interfaz de usuario de Workflow Automation, seleccione **ejecución > orígenes de datos**.
2. Haga clic con el botón derecho del ratón en el nombre del origen de datos de Unified Manager y, a continuación, seleccione **adquirir ahora**.
3. Compruebe que la adquisición se realiza correctamente sin errores.

Para que la integración de Workflow Automation en Unified Manager se tenga éxito, es necesario resolver los errores de adquisición.

Crear una relación de protección de SnapMirror desde la página de detalles Health/Volume

Puede usar la página de detalles Health/Volume para crear una relación de SnapMirror de modo que la replicación de datos esté habilitada para fines de protección. La replicación de SnapMirror permite restaurar datos del volumen de destino en caso de que se pierdan datos en el origen.

Antes de empezar

- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Acerca de esta tarea

El menú **Protect** no aparece en los siguientes casos:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Si el volumen es un volumen de FlexGroup
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

Se pueden ejecutar hasta 10 tareas de protección simultáneamente sin que el rendimiento se vea afectado. Es posible que experimente algún impacto en el rendimiento cuando se ejecutan entre 11 y 30 trabajos al mismo tiempo. No se recomienda ejecutar más de 30 trabajos simultáneamente.

Pasos

1. En la ficha **Protección** de la página de detalles **Estado/volumen**, haga clic con el botón derecho del ratón en la vista de topología el nombre de un volumen que desea proteger.
2. Seleccione **proteger > SnapMirror** en el menú.

Se muestra el cuadro de diálogo Configurar protección.

3. Haga clic en **SnapMirror** para ver la ficha **SnapMirror** y configurar la información de destino.
4. Haga clic en **Avanzado** para establecer la garantía de espacio según sea necesario y, a continuación, haga clic en **aplicar**.
5. Complete el área **Información de destino** y el área **Configuración de relación** del cuadro de diálogo

Configurar protección.

6. Haga clic en **aplicar**.

Volverá a la página de detalles Health/Volume.

7. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la página de detalles **Estado/volumen**.

Las tareas y los detalles del trabajo se muestran en la página de detalles Protection/Job.

8. En la página de detalles **Protection/Job**, haga clic en **Refresh** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y determinar cuándo se ha completado el trabajo.
9. Una vez completadas las tareas de trabajo, haga clic en **Atrás** en el explorador para volver a la página de detalles **Estado/volumen**.

La nueva relación se muestra en la vista de topología de la página de detalles Health/Volume.

Resultados

En función de la SVM de destino especificada durante la configuración o de las opciones habilitadas en su configuración avanzada, la relación de SnapMirror resultante puede ser una de varias variaciones posibles:

- Si especificó una SVM de destino que se ejecuta con la misma versión o una posterior de ONTAP en comparación con la del volumen de origen, el resultado predeterminado será una relación de SnapMirror basada en replicación de bloques.
- Si especificó una SVM de destino que se ejecuta con una misma versión o una posterior de ONTAP (versión 8.3 o posterior) en comparación con el volumen de origen, pero habilitó la replicación de versión flexible en la configuración avanzada, se obtiene un resultado de una relación de SnapMirror con la replicación de versión flexible.
- Si especificó una SVM de destino que se ejecuta en una versión anterior de ONTAP 8.3 o una versión superior a la del volumen de origen y la versión anterior admite la replicación de versión flexible, el resultado es una relación de SnapMirror con la replicación de versión flexible.

Crear una relación de protección SnapVault desde la página de detalles Health/Volume

Puede crear una relación de SnapVault mediante la página de detalles Health/Volume para que los backups de datos se habilitaron para fines de protección en los volúmenes.

Antes de empezar

- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation para que lleve a cabo esta tarea.

Acerca de esta tarea

El menú **Protect** no aparece en los siguientes casos:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador

- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

Pasos

1. En la ficha **Protección** de la página de detalles **Estado/volumen**, haga clic con el botón derecho del ratón en un volumen de la vista de topología que desee proteger.
2. Seleccione **proteger** > **SnapVault** en el menú.

Se abre el cuadro de diálogo Configure Protection.

3. Haga clic en **SnapVault** para ver la ficha **SnapVault** y configurar la información del recurso secundario.
4. Haga clic en **Avanzado** para establecer la deduplicación, compresión, crecimiento automático y garantía de espacio según sea necesario y, a continuación, haga clic en **aplicar**.
5. Complete el área **Información de destino** y el área **Configuración de relación** del cuadro de diálogo **Configurar protección**.
6. Haga clic en **aplicar**.

Volverá a la página de detalles Health/Volume.

7. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la página de detalles **Estado/volumen**.

Se muestra la página de detalles Protection/Job.

8. Haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.

Cuando se completan las tareas de trabajos, las nuevas relaciones se muestran en la vista de topología de la página de detalles Health/Volume.

Creación de una política de SnapVault para maximizar la eficiencia de transferencia

Puede crear una nueva política de SnapVault para configurar la prioridad para una transferencia de SnapVault. Las políticas se usan para maximizar la eficiencia de las transferencias del almacenamiento primario al secundario en una relación de protección.

Antes de empezar

- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- Ya debe haber completado el área Destination Information en el cuadro de diálogo Configure Protection.

Pasos

1. En la ficha **SnapVault** del cuadro de diálogo **Configurar protección**, haga clic en el enlace **Crear directiva** del área **Configuración de relación**.

Aparece la pestaña SnapVault.

2. En el campo **Nombre de directiva**, escriba el nombre que desea asignar a la directiva.
3. En el campo **prioridad de transferencia**, seleccione la prioridad de transferencia que desea asignar a la directiva.
4. En el campo **Comentario**, introduzca un comentario para la directiva.
5. En el área **etiqueta de replicación**, agregue o edite una etiqueta de replicación, según sea necesario.
6. Haga clic en **Crear**.

La nueva directiva se muestra en la lista desplegable Crear directiva.

Creación de una política de SnapMirror para maximizar la eficiencia de transferencia

Puede crear una política de SnapMirror para especificar la prioridad de transferencia de SnapMirror para las relaciones de protección. Las políticas de SnapMirror permiten maximizar la eficiencia de transferencia del origen al destino asignando las prioridades para que las transferencias de menor prioridad se programen después de las transferencias de prioridad normal.

Antes de empezar

- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- En esta tarea se supone que ya ha completado el área Información de destino del cuadro de diálogo Configurar protección.

Pasos

1. En la ficha **SnapMirror** del cuadro de diálogo **Configurar protección**, haga clic en el enlace **Crear directiva** del área **Configuración de relación**.

Se mostrará el cuadro de diálogo Create SnapMirror Policy.

2. En el campo **Nombre de directiva**, escriba el nombre que desea asignar a la directiva.
3. En el campo **prioridad de transferencia**, seleccione la prioridad de transferencia que desea asignar a la directiva.
4. En el campo **Comentario**, introduzca un comentario opcional para la directiva.
5. Haga clic en **Crear**.

La nueva política se muestra en la lista desplegable SnapMirror Policy.

Crear programaciones de SnapMirror y SnapVault

Puede crear programaciones básicas o avanzadas de SnapMirror y SnapVault para habilitar las transferencias automáticas de protección de datos en un volumen primario o

de origen, de modo que las transferencias se realicen con mayor frecuencia o menos frecuencia, según la frecuencia de los cambios de datos en los volúmenes.

Antes de empezar

- Debe tener el rol de administrador de OnCommand o de administrador del almacenamiento.
- Ya debe completar el área Destination Information en el cuadro de diálogo Configure Protection.
- Debe haber configurado Workflow Automation para que lleve a cabo esta tarea.

Pasos

1. En la ficha **SnapMirror** o en la ficha **SnapVault** del cuadro de diálogo **Configurar protección**, haga clic en el vínculo **Crear programación** del área **Configuración de relación**.

Se mostrará el cuadro de diálogo Crear programación.

2. En el campo **Nombre de horario**, escriba el nombre que desea asignar a la programación.
3. Seleccione una de las siguientes opciones:

- **Básico**

Seleccione si desea crear una programación básica de tipo intervalo.

- **Avanzado**

Seleccione si desea crear una programación de tareas con Cron.

4. Haga clic en **Crear**.

La nueva programación se muestra en la lista desplegable SnapMirror Schedule o SnapVault Schedule.

Información de copyright

Copyright © 2023 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.