Configuración y habilitación de la protección de datos condicionada por políticas

SnapManager Oracle

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/es-es/snapmanager-oracle/unix-administration/task_configuring_snapdrive_when_rbac_is_enabled.html on October 04, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configuración y habilitación de la protección de datos condicionada por políticas 1
Configuración de DataFabric Manager Server y SnapDrive cuando el control de acceso basado en roles está habilitado 1
La configuración de SnapDrive cuando RBAC no está habilitado 2
Comprender la habilitación o deshabilitación de la protección de datos en el perfil 2

Configuración y habilitación de la protección de datos condicionada por políticas

Debe configurar SnapDrive y DataFabric Manager Server para permitir la protección de datos en el perfil a fin de proteger backups en sistemas de almacenamiento secundario. Puede seleccionar las políticas de protección en la consola de Protection Manager para especificar cómo se protegerán los backups de la base de datos.

> Debe asegurarse de que Unified Manager de OnCommand se encuentre instalado en un servidor aparte para habilitar la protección de datos.

Configuración de DataFabric Manager Server y SnapDrive cuando el control de acceso basado en roles está habilitado

Cuando se habilita el control de acceso basado en roles (RBAC), debe configurar DataFabric Manager Server para que incluya las funcionalidades de RBAC. También debe registrar al usuario de SnapDrive creado en DataFabric Manager Server y al usuario raíz del sistema de almacenamiento en SnapDrive.

1. Configure DataFabric Manager Server.
   a. Para actualizar DataFabric Manager Server para actualizar los cambios realizados directamente en el sistema de almacenamiento por la base de datos de destino, introduzca el siguiente comando:dfm host Discover Storage_System
   b. Cree un usuario nuevo en DataFabric Manager Server y defina la contraseña.
   c. Para añadir el usuario del sistema operativo a la lista de administración del servidor DataFabric Manager, introduzca el siguiente comando: dfm user add sd-admin
   d. Para crear una nueva función en DataFabric Manager Server, introduzca el siguiente comando:dfm role create sd-admin-role
   e. Para agregar la funcionalidad DFM.Core.AccessCheck Global a la función, introduzca el siguiente comando:rol dfm add sd-admin-role DFM.Core.AccessCheck Global
   f. Para agregar sd-admin-role al usuario del sistema operativo, introduzca el siguiente comando:dfm user role set sd-adminsd-admin-role
   g. Para crear otra función en DataFabric Manager Server para el usuario raíz de SnapDrive, introduzca el siguiente comando:dfm role create sd-Protect
   h. Para agregar funciones de RBAC a la función creada para el usuario raíz de SnapDrive o el administrador, escriba los siguientes comandos:rol dfm add sd-Protect SD.Config.Read Globaldfm role add sd-Protect SD.Config.Write Globaldfm role add sd-Protect SD.Config.GlobalDelete dfm rol add sd-Protect SD.Storage.Read Globaldfm función add.sd-Protect
   i. Para añadir el usuario de oracle de la base de datos de destino a la lista de administradores del servidor DataFabric Manager y asignar la función sd-Protect, escriba el siguiente comando:dfm user add -r sd-protecttardb_host1\oracle
   j. Para añadir el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, introduzca el siguiente comando:dfm host set Storage_System hostLogin=oracle hostPassword=password

k. Para crear una nueva función en el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, introduzca el siguiente comando:dfm host role create -h Storage_System-c "api-**, login-**" Storage-rbac

l. Para crear un nuevo grupo en el sistema de almacenamiento y asignar el nuevo rol creado en DataFabric Manager Server, introduzca el siguiente comando:dfm host usergroup create -h Storage_System-r Storage-rbac-roleStorage-rbac-group

m. Para crear un nuevo usuario en el sistema de almacenamiento y asignar la nueva función y el grupo creado en DataFabric Manager Server, introduzca el siguiente comando:dfm host user create -h Storage_system-r Storage-rbac-role -p password -g Storage-rbac-groupptardb_host1

2. Configure SnapDrive.

   a. Para registrar las credenciales del usuario sd-admin en SnapDrive, introduzca el siguiente comando:snapdrive config set -dfm sd-admindfm_host

   b. Para registrar el usuario raíz o el administrador del sistema de almacenamiento con SnapDrive, introduzca el siguiente comando:snapdrive config set tardb_host 11erorage_system

La configuración de SnapDrive cuando RBAC no está habilitado

Para habilitar la protección de datos, debe registrar en SnapDrive al usuario raíz o al administrador de DataFabric Manager Server y al usuario raíz del sistema de almacenamiento.

1. Para actualizar DataFabric Manager Server para actualizar los cambios realizados directamente en el sistema de almacenamiento mediante la base de datos de destino, introduzca el siguiente comando:

   host dfm detecte storage_system

2. Para registrar el usuario raíz o el administrador de DataFabric Manager Server en SnapDrive, introduzca el siguiente comando:

   SnapDrive config set -dfm Administratordfm_host

3. Para registrar el usuario raíz o el administrador del sistema de almacenamiento con SnapDrive, escriba el siguiente comando:

   configuración de SnapDrive establezca root storage_system

Comprender la habilitación o deshabilitación de la protección de datos en el perfil

Puede habilitar o deshabilitar la protección de datos al crear o actualizar un perfil de base de datos.

Para crear un backup protegido de una base de datos en los recursos de almacenamiento secundario, los administradores de bases de datos y los administradores de almacenamiento realizan las siguientes acciones.

Si desea…	Realice lo siguiente…
Cree o edite un perfil	Para crear o editar un perfil, realice lo siguiente: • Habilite la protección de backup en el almacenamiento secundario. • Si utiliza Data ONTAP en 7-Mode y tiene instalado Protection Manager, puede seleccionar las políticas creadas por el administrador de almacenamiento o backup en Protection Manager. Si utiliza Data ONTAP en 7-Mode y la protección está habilitada, SnapManager crea un conjunto de datos para la base de datos. Un conjunto de datos consta de una colección de conjuntos de almacenamiento junto con la información de configuración asociada con sus datos. Los conjuntos de almacenamiento asociados a un conjunto de datos incluyen un conjunto de almacenamiento principal utilizado para exportar datos a clientes y el conjunto de réplicas y archivos que existen en otros conjuntos de almacenamiento. Los conjuntos de datos representan datos de usuario exportables. Si el administrador deshabilita la protección de una base de datos, SnapManager elimina el conjunto de datos. • Si utiliza ONTAP, debe seleccionar la política *SnapManager_CDOT_Mirror* o *SnapManager_CDOT_Vault_* en función de la relación de SnapMirror o SnapVault creada. Al deshabilitar la protección de copia de seguridad, se muestra un mensaje de advertencia que indica que el conjunto de datos se eliminará y no será posible restaurar o clonar copias de seguridad para este perfil.
Ver el perfil	Dado que el administrador de almacenamiento aún no ha asignado recursos de almacenamiento para implementar la normativa de protección, el perfil se muestra como no conforme tanto en la interfaz gráfica de usuario de SnapManager como en el resultado del comando profile show.

Si desea…	Realice lo siguiente…
Asigne recursos de almacenamiento en la consola de gestión de Protection Manager	En Protection Manager Management Console, el administrador de almacenamiento ve el conjunto de datos no protegido y asigna un pool de recursos a cada nodo del conjunto de datos que está asociado con el perfil. A continuación, el administrador de almacenamiento garantiza que los volúmenes secundarios estén aprovisionados y que se inicialicen las relaciones de protección.
Ver el perfil conforme en SnapManager	En SnapManager, el administrador de la base de datos ve que el perfil ha cambiado al estado conforme tanto en la interfaz gráfica de usuario como en la salida del comando profile show, lo que indica que se han asignado recursos.
Cree el backup	• Seleccione Full backup. • Además, seleccione si el backup debe estar protegido y seleccione la clase de retención primaria (por ejemplo, por hora o por día). • Si utiliza Data ONTAP operando en 7-Mode y desea proteger el backup inmediatamente en un almacenamiento secundario, lo que anula la programación de protección de Protection Manager, especifique la opción -protectnow. • Si utiliza ONTAP y desea proteger el backup inmediatamente en el almacenamiento secundario, especifique la opción Protect. La opción protectnow no se puede aplicar en Clustered Data ONTAP.
Vea el backup	El nuevo backup se muestra como programado para la protección, pero no está protegido (en la interfaz SnapManager y en el resultado del comando backup show). El estado de protección se muestra como «"no protegido"».
Consulte la lista de copias de seguridad	Una vez que el administrador de almacenamiento haya verificado que el backup se ha copiado a un sistema de almacenamiento secundario, SnapManager cambia el estado «sin protección» a «protegido».

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.