Configuración y habilitación de la protección de datos condicionada por políticas

SnapManager for SAP

NetApp
April 19, 2024

Tabla de contenidos

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.

Configure 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.

Pasos

1. Configure DataFabric Manager Server.

   a. 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:

      dfm host discover *storage_system*

   b. Cree un usuario nuevo en DataFabric Manager Server y defina la contraseña.

   c. Para añadir un usuario del sistema operativo a la lista de administración del servidor de DataFabric Manager, escriba el siguiente comando:

      dfm user add *sd-admin*

   d. Para crear una función nueva 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, escriba el siguiente comando:

      dfm role add *sd-admin-role* DFM.Core.AccessCheck Global

   f. Para añadir `sd-admin-role` para el 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, escriba el siguiente comando:

dfm role create *sd-protect*

h. Para añadir funcionalidades de RBAC al rol creado para el usuario raíz de SnapDrive o el administrador, escriba los siguientes comandos:

dfm role add *sd-protect* SD.Config.Read Global

dfm role add *sd-protect* SD.Config.Write Global

dfm role add *sd-protect* SD.Config.Delete Global

dfm role add *sd-protect* SD.Storage.Read Global

dfm role add *sd-protect* DFM.Database.Write Global

dfm role add *sd-protect* GlobalDataProtection

a. Para añadir el usuario de oracle de la base de datos de destino a la lista de administradores del servidor DataFabric Manager y asignar el rol sd-Protect, introduzca el siguiente comando:

dfm user add -r *sd-protecttardb_host1*\oracle

b. Para añadir el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, escriba el siguiente comando:

dfm host set *storage_system* hostLogin=oracle hostPassword=*password*

c. Para crear una función nueva 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-role*

d. Para crear un grupo nuevo 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*

e. 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-grouptardb_host1*

2. Configure SnapDrive.

a. Para registrar las credenciales de *sd-admin* Usuario con SnapDrive, introduzca el comando siguiente:

snapdrive config set -dfm *sd-admindfm_host*

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

```
snapdrive config set tardb_host1storage_system
```

Configure SnapDrive cuando el control de acceso basado en roles no esté 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.

Pasos

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:

   ejemplo

   ```
   dfm host discover storage_system
   ```

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

   ejemplo

   ```
   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:

   ejemplo

   ```
   snapdrive config set 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 la `profile show` resultado del comando.
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 `profile show` resultado del comando, que indica que se han asignado recursos.

Si desea…	Realice lo siguiente…
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 al almacenamiento secundario, anule la programación de protección de Protection Manager, especifique el `-protectnow` opción. • Si utiliza ONTAP y desea proteger el backup inmediatamente en el almacenamiento secundario, especifique el `protect` opción. La `protectnow` La opción no es aplicable 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 la `backup show` resultado del comando). 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

Información de la marca comercial