Introduction to data protection in SnapManager

SnapManager Oracle

NetApp
January 29, 2021

Table of Contents

Introduction to data protection in SnapManager

SnapManager supports data protection to protect the backups on the secondary or tertiary storage systems. You must set up SnapMirror and SnapVault relationships between the source and the destination volumes.

If you are using Data ONTAP operating in 7-Mode, SnapManager provides policy-driven data protection by integrating with Protection Manager (OnCommand Unified Manager). This automates replicating SnapManager backups on a primary storage system to a secondary storage system or even to a tertiary storage system by using SnapVault or SnapMirror policies created by the storage or backup administrator in Protection Manager. Retention on primary storage is controlled by SnapManager based on the retention defined during profile creation and the retention class tagged during the backup creation. Secondary storage backup retention is controlled by the policy defined in Protection Manager.

If you are using clustered Data ONTAP, SnapManager 3.4 provides *SnapManager_cDOT_Mirror* and *SnapManager_cDOT_Vault* policies for data protection. While creating a profile, you can select these policies depending on the SnapMirror or SnapVault relationship that was established using clustered Data ONTAP CLI or System Manager. When you create a backup selecting the profile for which you enabled protection, the backups are protected to a secondary storage system.

If you were using SnapManager 3.3.1 with clustered Data ONTAP, the backups were protected using post-scripts which were selected while creating profiles. If you want to use those profiles, after upgrading to SnapManager 3.4 you must perform the following operations.

- You must update the profiles to select either *SnapManager_cDOT_Mirror* or *SnapManager_cDOT_Vault* policy and delete the post-script that was used for data protection.
- After updating profile to use *SnapManager_cDOT_Vault* policy, you must delete existing backup schedules and create new schedules to specify the SnapVault label for the backups.
- If the profiles were created in SnapManager 3.3.1 without selecting the post-scripts, you must update the profiles to select either *SnapManager_cDOT_Mirror* or *SnapManager_cDOT_Vault* policy to enable data protection.

If you have backups in the secondary storage system that were mirrored or vaulted using SnapManager 3.3.1 post-scripts, you cannot use those backups for restore or cloning using SnapManager 3.4.

If you are using clustered Data ONTAP, SnapManager 3.4.2 supports multiple protection relationships (SnapMirror and SnapVault) on source volumes. Only one SnapMirror and one SnapVault relationship per volume is supported. You must create separate profiles, each with the SnapManager_cDOT_Mirror and the SnapManager_cDOT_Vault policy selected.

Snapdrive for Unix 5.3.2 and later is required to use multiple protection policies.