Data Protector

Virtual Machine Image Backups in an Internal Workflow

A virtual machine (VM) environment inclusive of its proprietary information is saved and stored as an image copy. The image copies for multiple VMs within this network file storage system require protection from tampering or theft and also carry individual retention policies that must be upheld. Additionally, in the event that an environment needs to be restored or a new one created, these images need to be available in their original formats. The workflow for this is managed from a central location where a backup server is also present.

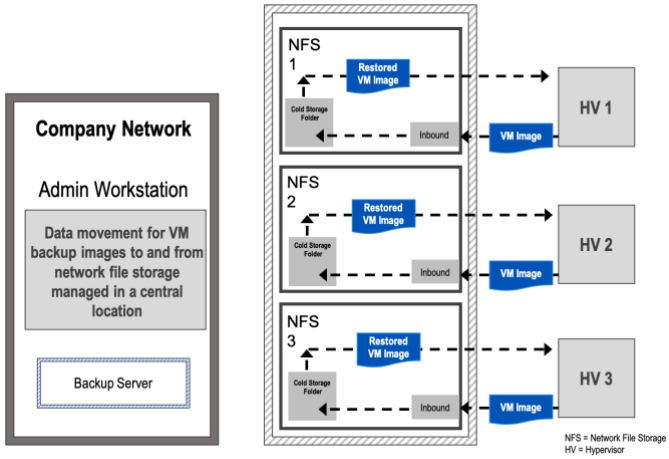

Figure 1. Use case for virtual image backups in an internal workflow

This is a very creative approach for using the Data Protector in an internal workflow. The Data Protector is implemented on a single location with a backup Data Protector configuration identical to the original in play. Tasks are managed in a single location for all network file storage locations (NFS). Each NFS location is associated with a single hypervisor (HV). From the central location, the Data Protector is watching the inbound folders within each NFS for activity. The backup VM image for each HV is protected and stored within its given NFS. When necessary from the central location, the protected image can be unprotected and restored to its respective HV.

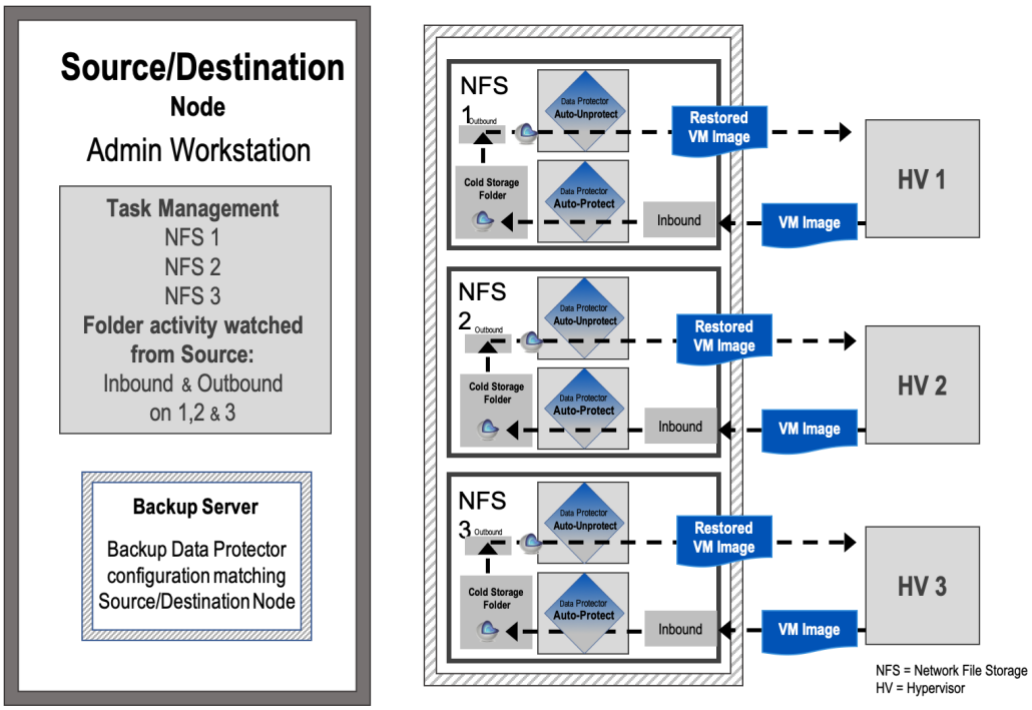

Figure 2. Data Protector workflow for virtual backups in an internal workflow

IMPLEMENTATION REQUIREMENTS

- This is an internal workflow that is securing backup images.
- A single location for Source and Destination is owned and managed by the Sertainty Customer.
- Archive or cold storage location(s) is managed by the Sertainty Customer.
- Folders are created at the storage location for each HV VM image set which is the backup for each HV. In the initial diagram, pre-exsting folders are shown. These can be associated with Data Protector Tasks if desired, but additional folders can be created for management ease. In the second diagram, an outbound folder is added to demonstrate the protected file in UXP Object format moving from cold storage to a folder watched by the Data Protector.
- The transfer to-and-from NFS locations for all VM image backups is managed by the Sertainy Customer.
- The movement of protected VM image backups from cold storage folder to Data Protector watched folder is managed by the Sertainty Customer.
- All Task management occurs in centralized location. Folders watched from this location.
- The UXP Identity is generated for the Source/Destination.

DATA PROTECTOR SOLUTION

- Backup VM images are generated for each of the current HV environments.
- The images for each HV are moved to the corresponding inbound folder within its respective NFS.
- The Data Protector facilitates the Auto-Protect process using the Source/Destination machine UXP Identity.
- The protected images in UXP Object format are moved to a cold storage folder within the NFS.
- These UXP Objects are held based on an internal retention policy and sit dormant until needed.
- If the protected backup in UXP Object format needs to be restored, the UXP Object is moved to the outbound folder where the Data Protector facilitates the Auto-Unprotect process and authenticates against the Source/Destination UXP Identiity embedded in the UXP Object.
- The VM image is extracted and placed in its expected location available for use.

Email us today:
tech-support@sertainty.com