PoINT Storage Manager

PoINT NetApp FPolicy Server for Cluster Mode

PoINT Software & Systems GmbH

A publication of:
PoINT Software & Systems GmbH
Eiserfelder Str. 316
57080 Siegen, Germany

Phone: +49 (0) 271 / 3841 - 0
Mail: info@point.de
Web: www.point.de

Document Version: 24.2.2021/DG
Program Version: 6.6

Attention
A functioning storage workflow requires a well configured system environment with devices working free of faults and, if applicable, flawless storage media. Therefore it is of the essence that the user does backup all data by functions offered by PoINT software and/or (if required) by supplementary software products at adequate intervals (i.e. in accordance with the scope and frequency of changes), and thereby to facilitate the reinstatement of these data even in exceptional situations (i.e. in case of hardware malfunction).

Trademarks
The PoINT logo is a registered trademark of PoINT Software & Systems GmbH. All other trademarks belong to their respective owners.

Contents

1 Overview

This document describes functionality, requirements and restrictions of the PoINT NetApp FPolicy Server for Cluster Mode which is an optional component of PoINT Storage Manager. It is available as a separate installation package which has to be installed after installing PoINT Storage Manager.

It is intended for administrators who are responsible to configure and administer PoINT Storage Manager. This document must be used in combination with the PoINT Storage Manager manual and the documentation for the PoINT NetApp FAS Agent. Please also refer to the related documentation of your NetApp storage system.

In combination with PoINT Storage Manager the PoINT NetApp FPolicy Server for Cluster Mode provides transparent “stub”-based read access to archived files for NetApp FAS systems. The archiving functionality is provided by the module PoINT NetApp FAS Agent.

2 Requirements

The following requirements must be fulfilled for operating the PoINT NetApp FPolicy Server for Cluster Mode of PoINT Storage Manager:

- PoINT Storage Manager Version must have been installed and licensed. The license key must enable the PoINT NetApp FPolicy Server for Cluster Mode and one PoINT NetApp FAS Agent license per addressed Storage Virtual Machine.
- NetApp ONTAP Version 8.3 or later running in Cluster Mode. Versions 8.3 and 9.0 through 9.8 have been tested.
- File system access via CIFS to the Data Source on the NetApp FAS is required, even if clients are only using NFS.
- The PoINT Storage Agent Service (PntStorageAgent.exe) must be allowed to accept TCP connections on port 8632. You may either create a firewall exception for this process or for the port number. The default port number can be changed using the following registry value on the PoINT Storage Manager server:
  HKEY_LOCAL_MACHINE\SOFTWARE\PoINT\PoINT Storage Manager\ArchiveAgent
  Value Name: FPolicyLocalPort
  Value Type: DWORD
  Content: <Port Number> (default: 8632)
  If Storage Vaults have already been created, it is also necessary, to adjust the existing FPolicy configuration as described in chapter 3.5, Change the FPolicy Configuration.
- The PoINT Storage Agent Service (PntStorageAgent.exe) uses the SSL port (443) to communicate with the NetApp Storage Virtual Machine. This communication must be allowed in the local firewall and on the network route.
- The PoINT NetApp FPolicy Server requires management access to the Storage Virtual Machine using either a dedicated LIF or the Data LIFs. Additionally, it is recommended to configure one Data LIF for each NetApp cluster node which may host the Storage Virtual Machine. Refer to chapter Management Access below for further information.
- If multiple LIFs are present on a Storage Virtual Machine then all LIFs should have CIFS protocol enabled. If either LIF does not have CIFS enabled then all LIFs with CIFS must be accessible using the same DNS name and this DNS name must be specified as Data Source for the Storage Vault.
- SSL must be enabled and configured on the Storage Virtual Machine, i.e. a valid certificate must have been created.
- The Storage Agent Account requires administrative privileges on the system where PoINT Storage Manager is installed and it must be a member of the group Backup Operators (BUILTIN\backup operators) on the NetApp Storage Virtual Machine. This account must be a domain account.
- The maximum number of inodes for NetApp FAS volumes containing PoINT Storage Manager Storage Vaults must be increased to at least three times the maximal number of files which will be stored on that volume. The maximal and current number of inodes can be viewed using the ONTAP command “volume show -fields files, files-used”. The command “volume modify -files” can be used to increase the maximal number of inodes. No more files can be stored on

the volume and PoINT Storage Manager job cycles will fail with an error indicating insufficient disc space if the maximal number of inodes has been reached.

– The SMB3 feature “Copy Offload” (ODX) does not correctly work with purged files. Therefore it is strongly recommended to disable this function for all addressed Storage Virtual Machines.

3 Functionality

PoINT NetApp FPolicy Server for Cluster Mode utilizes the NetApp FPolicy feature of Data ONTAP to allow transparent read access to files which have been archived to the configured archive devices. Whenever an archived file is read the NetApp FAS requests the data from the PoINT NetApp FPolicy Server for Cluster Mode which then reads the data from the archive device.

When configuring a Storage Vault for a NetApp FAS system, the PoINT NetApp FPolicy Server for Cluster Mode automatically creates appropriate "FPolicy policies" on the NetApp FAS and registers itself as an FPolicy Server.

3.1 Management Access

In order to configure FPolicy on the NetApp, the PoINT NetApp FPolicy Server requires management access to the Storage Virtual Machine which hosts the CIFS Server. This can be achieved by allowing “Management Access” for all Data LIFs belonging to the Storage Virtual Machine. To enable “Management Access” for a Data LIF it is necessary to assign an appropriate Firewall Policy and to include “management-https” in the Service Policy which is assigned to the LIF. In this case the field “Management I/F” in the Storage Vault configuration dialog can remain empty.

Alternatively, it is possible to configure a dedicated LIF which allows management access, only. In this case, the address or DNS name of this LIF must be specified as “Management I/F” in PoINT Storage Manager. It is also possible to use the Cluster Management LIF for this purpose.

3.2 Management Login

During configuration of a new Storage Vault you will be prompted for a Management Login which will be used by the PoINT NetApp FPolicy Server to connect to the Storage Virtual Machine. This login must be created on the Cluster or on the Storage Virtual Machine, depending on how management access is configured. When using the Data LIF for management access, the login must exist on the Storage Virtual Machine. When using a dedicated Management LIF, the login must be created on the Cluster or the SVM, depending on where the Management LIF belongs to.

The login can be created using a NetApp command shell or the NetApp OnCommand System Manager. It is not necessary to create a related Windows or domain account, but it is possible to use one. Please note that logins on the NetApp are case sensitive. Therefore the capitalization must be identical in the configuration on the NetApp and in PoINT Storage Manager.

This login must be allowed to log in using ONTAPI with password authentication or domain authentication if a domain account is used. It must be assigned a role which provides at least the following permissions:

version: readonly
volume: readonly
vserver: readonly
vserver fpolicy: all

Please note that all Storage Vaults on a Storage Virtual Machine must use the same login and the same management access method.

3.3 FPolicy Scope

When configuring a Storage Vault the Data Source path of the Storage Vault will be specified. PoINT NetApp FPolicy Server uses ONTAPI to map this CIFS path to the local path on the Storage Virtual Machine and determines the volume which contains this path and all volumes which are mounted below in the hierarchy. The list of volumes will be specified as 'volumes-to-include' for the FPolicy scope when configuring the FPolicy policy. The scope will automatically be updated if volume mount points have been changed as described in 3.6, Volume Junction.

3.4 FPolicy Timeouts

When creating the FPolicy policies, the following options will be applied for the FPolicy External Engine:

Request Abort Timeout: 90 seconds
Request Cancel Timeout: 90 seconds
Server Progress Timeout: 100 seconds
Max Server Requests: 200

These values are suitable for most use cases. However, if it is necessary to adjust these values, please refer to next chapter for more information how to manually change the FPolicy configuration.

3.5 Change the FPolicy Configuration

It may be necessary to change the configuration of the FPolicy policies. For example, if the IP address of the computer running the FPolicy Server has changed or another local port number shall be used by the FPolicy Server. When activating a Storage Vault the PoINT NetApp FPolicy Server verifies the FPolicy configuration and eventually reports that the configuration must be updated. It does not automatically change the configuration because this requires deactivating the policy, so that the storage system may return wrong data for purged files. Therefore, the administrator must first ensure that no clients access the storage system and then manually disable the FPolicy policies created by PoINT Storage Manager. In order to change some settings, e.g. timeout or queue length settings for the External Engine, those changes can be performed now and then activate the policies. In order to rebuild the policies using the default values, just activate the Storage Vaults while the policies are disabled. PoINT NetApp FPolicy Server will automatically create the new policies.

The names of the policies created by the PoINT NetApp FPolicy Server will be logged to the "Log File for PoINT Storage Agent".

3.6 Volume Junction Paths

PoINT NetApp FPolicy Server detects and handles changes of volume mount points (junction paths) and it automatically adjusts the FPolicy scope if it detects that a volume has been moved or that a new volume has been mounted. However, it is recommended to prevent all file system accesses and to deactivate all Storage Vaults before changing volume mount points. Also, when moving a volume outside of the scope of a Storage Vault, you must ensure that the volume does not contain purged files because access to these files will not be possible after moving the volume outside of the Storage Vault scope.

3.7 Snapshots

PoINT NetApp FPolicy Server supports access to purged files (stubs) in snapshots as long as that file version exists in the Archive or Capacity Tier.

During job cycles, PoINT Storage Manager ignores hidden directories with name “~snapshot”, because these directories contain read-only copies of older file versions which cannot be archived.

3.8 Access File Stubs on Mirror or Clone Volumes

Purged files (file stubs) can only be accessed, if the related volume is monitored by a PoINT NetApp FPolicy Server. To achieve this, it is possible to configure a ‘dummy’ Storage Vault whose data source path includes the mirrored volume. This Storage Vault must be configured on the same PoINT Storage Manager installation which has the Storage Vault which archives and monitors the original volume. The ‘dummy’ Storage Vault does not need any archiving or migration policies, it just must exist and must be active. The archive device for the ‘dummy’ Storage Vault may be the same which is also used by the Storage Vault for the original volume.

Both of the Storage Vaults must be active to successfully access purged files on the mirror volumes.

3.9 Redundant FPolicy Server

In order to avoid PoINT Storage Manager as a single point of failure, the optional PoINT Secondary Access Server can be configured as secondary FPolicy server which provides access to purged files while PoINT Storage Manager is not available.

Please refer to the PoINT Storage Manager product documentation for more information about PoINT Secondary Access Server.

3.10 Removing a Storage Vault

When deleting a Storage Vault in PoINT Storage Manager, PoINT NetApp FPolicy Server adjusts the FPolicy scope accordingly or deletes the configured FPolicy policy when removing the last Storage Vault on a Storage Virtual Machine.

Before removing a Storage Vault make sure that all purged files have been recalled. It is also recommended to execute the command line tool TagRemover.exe to remove metadata which have been appended to archived files. Refer to the ReadMe file of PoINT Storage Manager for a detailed description of this command line tool.

4 Restrictions

The following restrictions apply to the PoINT NetApp FPolicy Server for Cluster Mode and must be considered:

- There must not be other FPolicy Servers which provide stubbing functionality configured for the same volumes. However, other FPolicy Servers – including other PoINT Storage Manager installations – may register policies for other volumes.
- Up to four different NetApp Storage Virtual Machines (vServers) can be accessed by one PoINT Storage Manager installation.
- The FPolicy functionality is not supported for Infinite Volumes. Therefore PoINT NetApp FPolicy Server can only be used for Flex Volumes.
- The functionality to purge files, i.e. replace archived files by a stub file, cannot be used on SnapLock volumes. Trying to purge such files will result in error messages during job execution.
- Because the Windows 'offline'-attribute is used to identify purged files, it is recommended that no files have this attribute set by other applications. Otherwise PoINT Storage Manager may remove this attribute for files which have not been purged by PoINT Storage Manager.

5 Installation and Uninstallation

5.1 Installation

To install PoINT NetApp FPolicy Server for Cluster Mode log on to the computer where the PoINT Storage Manager server has been installed and run the installer with administrative privileges. If Storage Vaults have already been configured, it is necessary to restart the PoINT Storage Manager Service after installing this module.

The installer also copies this documentation to installation directory of PoINT Storage Manager.

5.2 Uninstallation

After uninstalling PoINT NetApp FPolicy Server for Cluster Mode it is not possible to access purged files on the NetApp FAS system. Therefore it is strongly recommended to first restore all purged files to the NetApp FAS system. After restoring all files, stop PoINT Storage Manager and remove the file DLLFPC64.DLL from the installation directory of PoINT Storage Manager. Finally, use ONTAP shell to disable and destroy the FPolicy policies which have been created by PoINT NetApp FPolicy Server for Cluster Mode. The names of the policies have been logged to the “Log file for PoINT Storage Agent”.

If you plan to use existing Storage Vaults on NetApp FAS without the FPolicy Server, refer to chapter 5.3, Using PoINT NetApp FAS Agent without the FPolicy Server, for more information.

5.3 Using PoINT NetApp FAS Agent without the FPolicy Server

It is possible to use Storage Vaults on NetApp FAS systems without PoINT NetApp FPolicy Server for Cluster Mode. In this case it is not possible to purge files. In order to use NetApp FAS without FPolicy Server, a license key must be installed which disables the support for the FPolicy Server.

6 Logging and Error Reporting

PoINT NetApp FPolicy Server for Cluster Mode logs connection related warning and error messages to the "Log File of PoINT Storage Agent" and Storage Vault specific messages to the “Migration Job Log File” of the Storage Vault. These log files can be opened in the "Log Files View" of PoINT Storage Manager.