Plan the FPolicy event configuration

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/nas-audit/plan-fpolicy-event-config-concept.html on April 20, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Plan the FPolicy event configuration . . . 1
Plan the FPolicy event configuration overview . . . 1
Supported file operation and filter combinations that FPolicy can monitor for SMB . . . 6
Supported file operation and filter combinations that FPolicy can monitor for NFSv3 . . . 7
Supported file operation and filter combinations that FPolicy can monitor for NFSv4 . . . 8
Complete the FPolicy event configuration worksheet . . . 10

Plan the FPolicy event configuration

Plan the FPolicy event configuration overview

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

What it means to create an FPolicy event

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

- Storage virtual machine (SVM) name
- Event name
- Which protocols to monitor

  FPolicy can monitor SMB, NFSv3, and NFSv4 file access operations.

- Which file operations to monitor

  Not all file operations are valid for each protocol.

- Which file filters to configure

  Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.

- Whether to monitor volume mount and unmount operations

> There is a dependency with three of the parameters (`-protocol`, `-file-operations`, `-filters`). The following combinations are valid for the three parameters:
>
> - You can specify the `-protocol` and `-file-operations` parameters.
> - You can specify all three of the parameters.
> - You can specify none of the parameters.

What the FPolicy event configuration contains

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

Type of information	Option

SVM Specifies the SVM name that you want to associate with this FPolicy event. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver` `vserver_name`
Event name Specifies the name to assign to the FPolicy event. When you create the FPolicy policy you associate the FPolicy event with the policy using the event name. The name can be up to 256 characters long. The name should be up to 200 characters long if configuring the event in a MetroCluster or SVM disaster recovery configuration. The name can contain any combination of the following ASCII-range characters: • `a` through `z` • `A` through `Z` • `0` through `9` • " _ ", “-”, and “.”	`-event-name` `event_name`
Protocol Specifies which protocol to configure for the FPolicy event. The list for `-protocol` can include one of the following values: • `cifs` • `nfsv3` • `nfsv4` If you specify `-protocol`, then you must specify a valid value in the `-file-operations` parameter. As the protocol version changes, the valid values might change.	`-protocol` `protocol`

File operations Specifies the list of file operations for the FPolicy event. The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file-operations` can include one or more of the following values: • `close` for file close operations • `create` for file create operations • `create-dir` for directory create operations • `delete` for file delete operations • `delete_dir` for directory delete operations • `getattr` for get attribute operations • `link` for link operations • `lookup` for lookup operations • `open` for file open operations • `read` for file read operations • `write` for file write operations • `rename` for file rename operations • `rename_dir` for directory rename operations • `setattr` for set attribute operations • `symlink` for symbolic link operations ⓘ If you specify `-file-operations`, then you must specify a valid protocol in the `-protocol` parameter.	`-file-operations file_operations,...`

Filters
 	
Specifies the list of filters for a given file operation for the specified protocol. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:
 	
> If you specify the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.
 	
- `monitor-ads` option to filter the client request for alternate data stream.
- `close-with-modification` option to filter the client request for close with modification.
- `close-without-modification` option to filter the client request for close without modification.
- `first-read` option to filter the client request for first read.
- `first-write` option to filter the client request for first write.
- `offline-bit` option to filter the client request for offline bit set.
 	
  Setting this filter results in the FPolicy server receiving notification only when offline files are accessed.
 	
- `open-with-delete-intent` option to filter the client request for open with delete intent.
 	
  Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.
 	
- `open-with-write-intent` option to filter client request for open with write intent.
 	
  Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it.
 	
- `write-with-size-change` option to filter the client request for write with size change.
	`-filters filter, ...`

Filters continued • `setattr-with-owner-change` option to filter the client setattr requests for changing owner of a file or a directory. • `setattr-with-group-change` option to filter the client setattr requests for changing the group of a file or a directory. • `setattr-with-sacl-change` option to filter the client setattr requests for changing the SACL on a file or a directory. This filter is available only for the SMB and NFSv4 protocols. • `setattr-with-dacl-change` option to filter the client setattr requests for changing the DACL on a file or a directory. This filter is available only for the SMB and NFSv4 protocols. • `setattr-with-modify-time-change` option to filter the client setattr requests for changing the modification time of a file or a directory. • `setattr-with-access-time-change` option to filter the client setattr requests for changing the access time of a file or a directory. • `setattr-with-creation-time-change` option to filter the client setattr requests for changing the creation time of a file or a directory. This option is available only for the SMB protocol. • `setattr-with-mode-change` option to filter the client setattr requests for changing the mode bits on a file or a directory. • `setattr-with-size-change` option to filter the client setattr requests for changing the size of a file. • `setattr-with-allocation-size-change` option to filter the client setattr requests for changing the allocation size of a file. This option is available only for the SMB protocol. • `exclude-directory` option to filter the client requests for directory operations. When this filter is specified, the directory operations are not monitored.	`-filters filter, ...`

Is volume operation required
 	
Specifies whether monitoring is required for volume mount and unmount operations. The default is `false`.
	`-volume-operation {true|false}`
	
	`-filters filter, ...`

FPolicy access denied notifications Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. These notifications are valuable for security, ransomware protection, and governance. Notifications will be generated for file operation failed due to lack of permission, which includes: • Failures due to NTFS permissions. • Failures due to Unix mode bits. • Failures due to NFSv4 ACLs.	`-monitor-fileop-failure {true|false}`

Supported file operation and filter combinations that FPolicy can monitor for SMB

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported file operations	Supported filters
close	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory
create	monitor-ads, offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	monitor-ads, offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit, exclude-dir
open	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
read	monitor-ads, offline-bit, first-read
write	monitor-ads, offline-bit, first-write, write-with-size-change
rename	monitor-ads, offline-bit

rename_dir	Currently no filter is supported for this file operation.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported access denied file operation	Supported filters
open	NA

Supported file operation and filter combinations that FPolicy can monitor for NFSv3

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported file operations	Supported filters
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
link	offline-bit
lookup	offline-bit, exclude-dir
read	offline-bit, first-read
write	offline-bit, first-write, write-with-size-change

rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	offline-bit

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported access denied file operation	Supported filters
access	NA
create	NA
create_dir	NA
delete	NA
delete_dir	NA
link	NA
read	NA
rename	NA
rename_dir	NA
setattr	NA
write	NA

Supported file operation and filter combinations that FPolicy can monitor for NFSv4

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access

operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 file access events is provided in the following table:

Supported file operations	Supported filters
close	offline-bit, exclude-directory
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit, exclude-directory
link	offline-bit
lookup	offline-bit, exclude-directory
open	offline-bit, exclude-directory
read	offline-bit, first-read
write	offline-bit, first-write, write-with-size-change
rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	offline-bit

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of NFSv4 file access events is provided in the following table:

Supported access denied file operation	Supported filters

access	NA
create	NA
create_dir	NA
delete	NA
delete_dir	NA
link	NA
open	NA
read	NA
rename	NA
rename_dir	NA
setattr	NA
write	NA

Complete the FPolicy event configuration worksheet

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Event name	Yes	Yes	
Protocol	No		
File operations	No		
Filters	No		

Volume operation	No		
Access denied events (support beginning with ONTAP 9.13)	No		

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.