Plan the FPolicy policy configuration

ONTAP 9

NetApp
September 19, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/nas-audit/plan-fpolicy-policy-config-concept.html on September 19, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Plan the FPolicy policy configuration 1
Plan the FPolicy policy configuration overview 1
Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine 5
Complete the FPolicy policy worksheet 6

Plan the FPolicy policy configuration

Plan the FPolicy policy configuration overview

Before you configure the FPolicy policy, you must understand which parameters are required when creating the policy as well as why you might want to configure certain optional parameters. This information helps you to determine which values to set for each parameter.

When creating an FPolicy policy you associate the policy with the following:

- The storage virtual machine (SVM)
- One or more FPolicy events
- An FPolicy external engine

You can also configure several optional policy settings.

What the FPolicy policy configuration contains

You can use the following list of available FPolicy policy required and optional parameters to help you plan your configuration:

Type of information	Option	Required	Default
SVM name Specifies the name of the SVM on which you want to create an FPolicy policy.	`-vserver vserver_name`	Yes	None

Policy name Specifies the name of the FPolicy policy. The name can be up to 256 characters long. ⓘ The name should be up to 200 characters long if configuring the policy 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 "."	`-policy-name policy_name`	Yes	None
Event names Specifies a comma-delimited list of events to associate with the FPolicy policy. • You can associate more than one event to a policy. • An event is specific to a protocol. • You can use a single policy to monitor file access events for more than one protocol by creating an event for each protocol that you want the policy to monitor, and then associating the events to the policy. • The events must already exist.	`-events event_name, ...`	Yes	None

External engine name Specifies the name of the external engine to associate with the FPolicy policy. • An external engine contains information required by the node to send notifications to an FPolicy server. • You can configure FPolicy to use the ONTAP native external engine for simple file blocking or to use an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management. • If you want to use the native external engine, you can either not specify a value for this parameter or you can specify `native` as the value. • If you want to use FPolicy servers, the configuration for the external engine must already exist.	`-engine engine_name`	Yes (unless the policy uses the internal ONTAP native engine)	`native`
Is mandatory screening required Specifies whether mandatory file access screening is required. • The mandatory screening setting determines what action is taken on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. • When set to `true`, file access events are denied. • When set to `false`, file access events are allowed.	`-is-mandatory {true|false}`	No	`true`

Allow privileged access Specifies whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection. If configured, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data connection. For privileged data access, SMB must be licensed on the cluster and all the data LIFs used to connect to the FPolicy servers must be configured to have `cifs` as one of the allowed protocols. If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access.	`-allow -privileged -access {yes|no}`	No (unless passthrough-read is enabled)	`no`
Privileged user name Specifies the user name of the account the FPolicy servers use for privileged data access. • The value for this parameter should use the “domain\user name” format. • If `-allow-privileged-access` is set to `no`, any value set for this parameter is ignored.	`-privileged -user-name user_name`	No (unless privileged access is enabled)	None

Allow passthrough-read Specifies whether the FPolicy servers can provide passthrough-read services for files that have been archived to secondary storage (offline files) by the FPolicy servers: • Passthrough-read is a way to read data for offline files without restoring the data to the primary storage. Passthrough-read reduces response latencies because there is no need to recall files back to primary storage before responding to the read request. Additionally, passthrough-read optimizes storage efficiency by eliminating the need to consume primary storage space with files that are recalled solely to satisfy read requests. • When enabled, the FPolicy servers provide the data for the file over a separate privileged data channel opened specifically for passthrough-reads. • If you want to configure passthrough-read, the policy must also be configured to allow privileged access.	`-is-passthrough-read-enabled {true|false}`	No	`false`

Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine

If you configure the FPolicy policy to use the native engine, there is a specific requirement for how you define the FPolicy scope configured for the policy.

The FPolicy scope defines the boundaries on which the FPolicy policy applies, for example whether the FPolicy applies to specified volumes or shares. There are a number of parameters that further restrict the scope to which the FPolicy policy applies. One of these parameters, `-is-file-extension-check-on-directories-enabled`, specifies whether to check file extensions on directories. The default value is `false`, which means that file extensions on directories are not checked.

When an FPolicy policy that uses the native engine is enabled on a share or volume and the `-is-file-extension-check-on-directories-enabled` parameter is set to `false` for the scope of the policy, directory access is denied. With this configuration, because the file extensions are not checked for directories, any directory operation is denied if it falls under the scope of the policy.

To ensure that directory access succeeds when using the native engine, you must set the `-is-file-extension-check-on-directories-enabled parameter` to `true` when creating the scope.

With this parameter set to `true`, extension checks happen for directory operations and the decision whether to allow or deny access is taken based on the extensions included or excluded in the FPolicy scope configuration.

Complete the FPolicy policy worksheet

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

Type of information	Include	Your values
Storage virtual machine (SVM) name	Yes	
Policy name	Yes	
Event names	Yes	
External engine name		
Is mandatory screening required?		
Allow privileged access		
Privileged user name		
Is passthrough-read enabled?		

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.