LIFs and service policies

ONTAP System Manager

NetApp
December 14, 2020

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking-app/lifs_and_service_policies.html on December 18, 2020. Always check docs.netapp.com for the latest.

Table of Contents

LIFs and service policies

You can assign service policies (instead of LIF roles) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.

Service policies for system SVMs

The admin SVM and any system SVM contain service policies that can be used for LIFs in that SVM, including management and intercluster LIFs. These policies are automatically created by the system when an IPspace is created. The following table lists the built-in policies for LIFs in system SVMs:

Policy	Included services	Equivalent role	Description
default-intercluster	intercluster-core	intercluster	Used by LIFs carrying intercluster traffic. Note: Available from ONTAP 9.5 with the name net-intercluster service policy.
default-route-announce	management-bgp	-	Used by LIFs carrying BGP peer connections Note: Available from ONTAP 9.5 with the name net-route-announce service policy.
default-management	management-core, management-ems, management-ssh, management-https, management-autosupport	node-mgmt, or cluster-mgmt	Used by LIFs handling management requests. Management-ems controls which LIFs can publish EMS content.

The following table lists the services that can be used on a system SVM along with any restrictions each service imposes on a LIF's failover policy:

Service	Failover limitations	Description
intercluster-core	home-node-only	Core intercluster services
management-core	-	Core management services
management-ssh	-	Services for SSH management access
management-https	-	Services for HTTPS management access
management-autosupport	-	Services related to posting AutoSupport payloads
management-bgp	home-port-only	Services related to BGP peer interactions

Service policies for data SVMs

All data SVMs contain service policies that can be used by LIFs in that SVM. The following table lists the built-in policies for LIFs in data SVMs:

Policy	Included services	Equivalent data protocol	Description
default-management	management-ssh, management-https	none	Used by LIFs handling management requests
default-data-blocks	data-iscsi	iscsi	Used by LIFs carrying block-oriented SAN data traffic
default-data-files	data-nfs, data-cifs, data-flexcache, data-fpolicy-client	nfs, cifs, fcache	Used by LIFs carrying file-oriented NAS data traffic.

The following table lists the services that can be used on a data SVM along with any restrictions each service imposes on a LIF's failover policy:

Policy	Included services	Equivalent data protocol	Description
management-ssh	-	-	Services for SSH management access
management-https	-	-	Services for HTTPS management access
data-core	-	data-only	Core data services (see for more details.
data-nfs	-	data-only	Protocols related to NFS data service
data-cifs	-	data-only	Protocols related to CIFS data service
data-flexcache	-	data-only	Protocols related to FlexCache data service
data-iscsi	home-port-only	data-only	Protocols related to iSCSI data service

You should be aware of how the service policies are assigned to the LIFs in data SVMs:

- If a data SVM is created with a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using the specified services.
- If a data SVM is created without specifying a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using a default list of data services.

  The default data services list includes the iSCSI, NFS, SMB, and FlexCache services.

- When a LIF is created with a list of data protocols, a service policy equivalent to the specified data protocols is assigned to the LIF.

  If an equivalent service policy does not exist, a custom service policy is created.

- When a LIF is created without a service policy or list of data protocols, the default-data-files service policy is assigned to the LIF by default.

Data-core service

The data-core service allows components that previously used LIFs with the data role to work as expected on clusters that have been upgraded to manage LIFs using service policies instead of LIF roles (which are deprecated in ONTAP 9.6).

Specifying data-core as a service does not open any ports in the firewall, but the service should be included in any service policy in a data SVM. For example, the default-data-files service policy contains the following services by default:

- data-core
- data-nfs
- data-cifs
- data-flexcache

The data-core service should be included in the policy to ensure all applications using the LIF work as expected, but the other three services can be removed, if desired.

Copyright Information

Copyright © 2020 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.