What's new in NetApp HCI

HCI

Michael Wallis, Ann-Marie Grissino, amitha
September 29, 2020

This PDF was generated from https://docs.netapp.com/us-en/hci/docs/rn_whatsnew.html on November 05, 2020.
Always check docs.netapp.com for the latest.

NetApp®

Table of Contents

What's new in NetApp HCI 1
NetApp HCI 1.8P1 1
Element 12.2 1

What's new in NetApp HCI

NetApp periodically updates NetApp HCI to bring you new features, enhancements, and bug fixes. NetApp HCI 1.8P1 includes Element 12.2 for storage clusters.

- The NetApp HCI 1.8P1 section describes new features and updates in NetApp HCI version 1.8P1.
- The Element 12.2 section describes new features and updates in NetApp Element 12.2.

NetApp HCI 1.8P1

NetApp HCI 1.8P1 includes security and stability improvements.

NetApp HCI documentation enhancements

You can now access NetApp HCI upgrading, expansion, monitoring, and concepts information in an easy-to-navigate format here.

NetApp Element Plug-in for vCenter Server 4.5 availability

The NetApp Element Plug-in for vCenter Server 4.5 is available outside of the management node 12.2 and NetApp HCI 1.8P1 releases. To upgrade the plug-in, follow the instructions in the NetApp HCI Upgrades documentation.

NetApp Hybrid Cloud Control enhancements

NetApp Hybrid Cloud Control is enhanced for version 1.8P1. Learn more.

Element 12.2

NetApp HCI 1.8P1 includes Element 12.2 for storage clusters. Element 12.2 introduces SolidFire Enterprise SDS, software encryption at rest, maintenance mode, enhanced volume access security, Fully Qualified Domain Name (FQDN) access to UIs, storage node firmware updates, and security updates.

SolidFire Enterprise SDS

Element 12.2 introduces SolidFire Enterprise SDS (eSDS). SolidFire eSDS provides the benefits of SolidFire scale out technology and NetApp Element software data services on the hardware of your choice that meets the reference configuration for SolidFire eSDS. Learn more.

The following are new Element API methods related to SolidFire eSDS (Element 12.2 API information for SolidFire eSDS has more information):

- `GetLicenseKey`
- `SetLicenseKey`

Software encryption at rest

Element 12.2 introduces software encryption at rest, which you can enable when you create a storage cluster (and is enabled by default when you create a SolidFire Enterprise SDS storage cluster). This feature encrypts all data stored on the SSDs in the storage nodes and causes only a very small (~2%) performance impact on client IO.

The following are Element API methods related to software encryption at rest (the Element API Reference Guide has more information):

- `CreateCluster`

Maintenance mode

Element 12.2 introduces maintenance mode, which enables you to take a storage node offline for maintenance such as software upgrades or host repairs, while preventing a full sync of all data. If one or more nodes need maintenance, you can minimize the I/O impact to the rest of the storage cluster by enabling maintenance mode for those nodes before you begin. You can use maintenance mode with both appliance nodes as well as SolidFire eSDS nodes.

Enhanced volume access security

You can now restrict volume access to certain initiators based on VLAN (virtual network) association. You can associate new or existing initiators with one or more virtual networks, restricting that initiator to iSCSI targets accessible via those virtual networks.

The following are updated Element API methods related to these security improvements (the Element API Reference Guide has more information):

- `CreateInitiators`
- `ModifyInitiators`
- `AddAccount`
- `ModifyAccount`

Fully Qualified Domain Name (FQDN) access to UIs

Element 12.2 supports cluster web interface access using FQDNs. On Element 12.2 storage clusters, if you use the FQDN to access web user interfaces such as the Element web UI, per-node UI, or management node UI, you must first add a storage cluster setting to identify the FQDN used by the cluster. This setting enables the cluster to properly redirect a login session and facilitates better integration with external services like key managers and identity providers for multi-factor

authentication. This feature requires management services version 2.15 or later.

You can do this by following these steps:

1. Create the following cluster interface preference using the `CreateClusterInterfacePreference` API method, inserting the cluster MVIP FQDN for the preference value:
   - Name: `mvip_fqdn`
   - Value: <Fully Qualified Domain Name for the Cluster MVIP>
2. Change the management node settings using the management node REST API:
   a. Access the REST API UI for the management node by entering the management node IP address followed by `/mnode/2/`. For example: `https://[management node IP]/mnode/2/`
   b. Click **Authorize** or any lock icon and complete the following:
      i. Enter the cluster user name and password.
      ii. Enter the client ID as `mnode-client`.
      iii. Click **Authorize** to begin a session.
      iv. Close the window.
   c. Click **GET /settings**.
   d. Click **Try it out**.
   e. Click **Execute**.
   f. Record any proxy settings reported in the response body.
   g. Click **PUT /settings**.
   h. Click **Try it out**.
   i. In the request body area, enter the management node FQDN as the value for the `mnode_fqdn` parameter.
   j. Enter any proxy setting values you recorded earlier in the remaining parameters in the request body. If you leave the proxy parameters empty or do not include them in the request body, existing proxy settings will be removed.
   k. Click **Execute**.

Storage node firmware updates

Element 12.2 includes firmware updates for storage nodes. Learn more.

Security enhancements

Element 12.2 resolves security vulnerabilities for storage nodes and the management node. Learn more about these security enhancements.

New SMART warning for failing drives

Element 12.2 now performs periodic health checks on SolidFire appliance drives using SMART health data from the drives. A drive that fails the SMART health check might be close to failure. If a drive fails the SMART health check, a new critical severity cluster fault appears: `Drive with serial: <serial number> in slot: <node slot><drive slot> has failed the SMART overall health check. To resolve this fault, replace the drive`.

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center
- Firmware and driver versions for NetApp HCI and NetApp Element software

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.