



# **Security and data encryption**

## **Cloud Volumes ONTAP**

NetApp

January 19, 2024

This PDF was generated from <https://docs.netapp.com/us-en/blexp-cloud-volumes-ontap/aws/task-encrypting-volumes.html> on January 19, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Security and data encryption ..... 1
  - Encrypting volumes with NetApp encryption solutions. .... 1
  - Manage keys with AWS Key Management Service ..... 1
  - Improving protection against ransomware ..... 2

# Security and data encryption

## Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable FIPS 140-2–compliant data-at-rest encryption of volumes. [Learn more about these encryption solutions.](#)

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- AWS Key Management Service (beginning in 9.12.0)

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

### What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- [Adding NetApp Support Site accounts to BlueXP](#)
- [Registering pay-as-you-go systems](#)



BlueXP doesn't install the NVE license on systems that reside in the China region.

### Steps

1. Review the list of supported key managers in the [NetApp Interoperability Matrix Tool](#).



Search for the **Key Managers** solution.

2. [Connect to the Cloud Volumes ONTAP CLI.](#)
3. Configure external key management.
  - AWS: [AWS Key Management Service](#)

## Manage keys with AWS Key Management Service

You can use [AWS's Key Management Service \(KMS\)](#) to protect your ONTAP encryption keys in an AWS-deployed application.

Key management with the AWS KMS can be enabled with the CLI or the ONTAP REST API.

When using the KMS, be aware that by default a data SVM's LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with AWS's authentication

services. If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Before you begin

- Cloud Volumes ONTAP must be running version 9.12.0 or later
- You must have installed the Volume Encryption (VE) license and
- You must have installed the Multi-tenant Encryption Key Management (MTEKM) license installed.
- You must be a cluster or SVM administrator
- You must have an active AWS subscription



You can only configure keys for a data SVM.

## Configuration

### AWS

1. You must create a [grant](#) for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:
  - DescribeKey
  - Encrypt
  - DecryptTo create a grant, refer to [AWS documentation](#).
2. [Add a policy to the appropriate IAM role](#). The policy should support the DescribeKey, Encrypt, and Decrypt operations.

### Cloud Volumes ONTAP

1. Switch to your Cloud Volumes ONTAP environment.
2. Switch to the advanced privilege level:  
`set -privilege advanced`
3. Enable the AWS key manager:  
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:  
`security key-manager external aws show -vserver svm_name`

## Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. BlueXP enables you to implement two NetApp solutions for ransomware: Protection from common ransomware file extensions and Autonomous Ransomware Protection (ARP). These solutions provide effective tools for visibility, detection, and remediation.

## Protection from common ransomware file extensions

Available through BlueXP, the Ransomware Protection setting allows you to utilize the ONTAP FPolicy functionality to guard against common ransomware file extension types.

### Steps

1. On the Canvas page, double-click the name of the system you configure to ransomware protection.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Ransomware Protection**.

Information		Features
Working Environment Tags		Tags 
Scheduled Downtime		Off 
S3 Storage Classes	Standard-Infrequent Access 	
Instance Type		m5.xlarge 
Write Speed		Normal 
Ransomware Protection		Off 
Support Registration		Not Registered 
CIFs Setup		

3. Implement the NetApp solution for ransomware:

- Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

- b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

The default FPolicy scope blocks files that have the following extensions:

micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



BlueXP creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the `vserver fpolicy policy scope` commands from the Cloud Volumes ONTAP CLI.

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection

50 %  
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

## Autonomous Ransomware Protection

Cloud Volumes ONTAP supports the Autonomous Ransomware Protection (ARP) feature, which performs analyses on workloads to proactively detect and warn about abnormal activity that might indicate a ransomware attack.

Separate from the file extension protections provided through the [ransomware protection setting](#), the ARP feature uses workload analysis to alert the user on potential attacks based on detected "abnormal activity". Both the ransomware protection setting and the ARP feature can be used in conjunction for comprehensive ransomware protection.

The ARP feature is available for use with BYOL licenses only (1 to 36 month terms) on both node-based and capacity-based licensing models. You must contact your NetApp sales representative to purchase a new, separate, add-on license for use with the ARP feature in Cloud Volumes ONTAP.

The ARP license is considered a "floating" license, which means it is not bound to a single Cloud Volumes ONTAP instance and can be applied to multiple Cloud Volumes ONTAP environments.



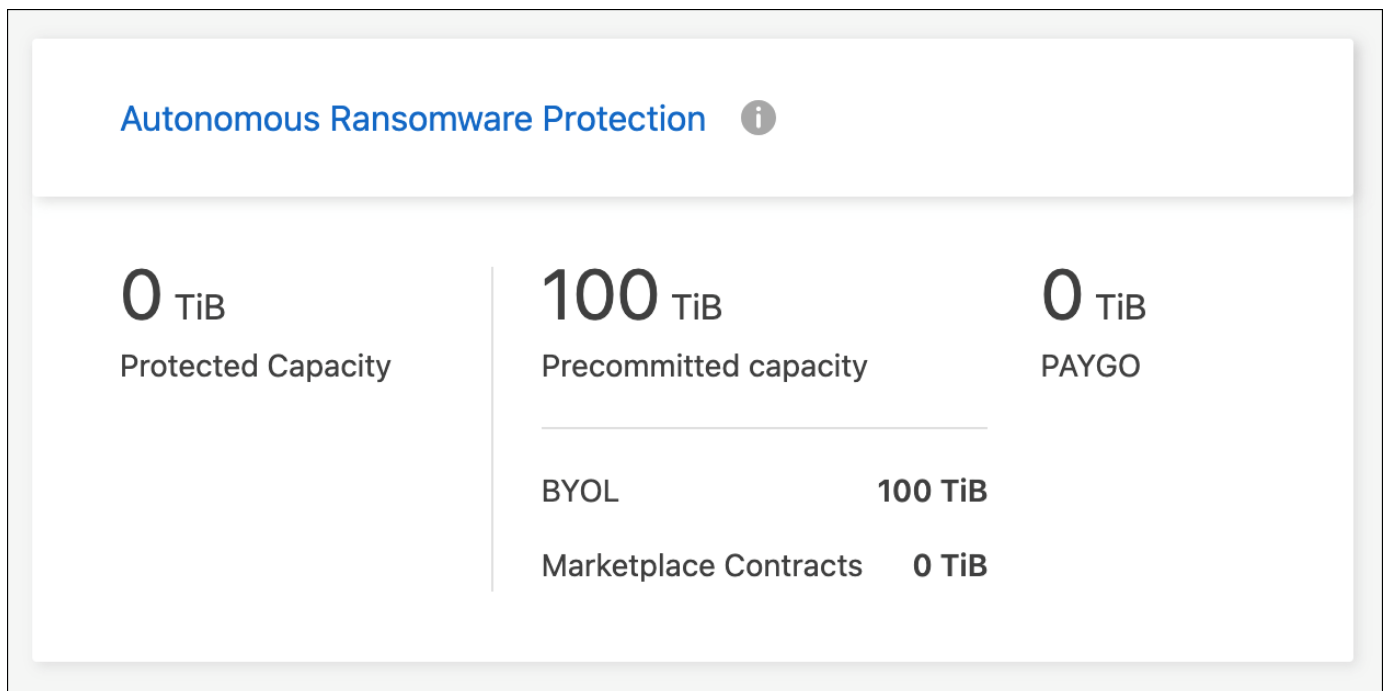
The usage of the ARP feature with node-based Cloud Volumes ONTAP licenses is not currently reflected in Digital Wallet. The ability to view node-based ARP usage will be available under Digital Wallet in a future release.

Upon purchase of an add-on license and adding it to the Digital Wallet, you can enable ARP on a per volume basis with Cloud Volumes ONTAP. Charging for ARP is metered at a volume level, according to the total provisioned capacity of volumes with the ARP feature enabled. The minimum license capacity is 1TB. However, there is no minimum capacity charging for the ARP feature.

ARP enabled volumes have a designated state of "Learning mode" or "Active". Any volume with an ARP state of "Disabled" is excluded from charging. For example, a Cloud Volumes ONTAP environment with 30 TiB of provisioned capacity can elect to have only a subset of 15 TiB volumes with ARP enabled.

Configuration of ARP for volumes is performed through ONTAP System Manager and ONTAP CLI.

For more information on how to enable ARP with ONTAP System Manager and CLI, see [Enable Autonomous Ransomware Protection](#).



Support is not available for the use of licensed features without a license.



## 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.