Security and data encryption

Cloud Volumes ONTAP

NetApp
September 22, 2023

Table of Contents

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:

- Google Cloud Key Management Service

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.
   - Google Cloud: Google Cloud Key Management Service

Manage keys with Google's Cloud Key Management Service

You can use Google Cloud Platform's Key Management Service (Cloud KMS) to protect your ONTAP encryption keys in a Google Cloud Platform-deployed application.

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

When using Cloud 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 the cloud provider's

authentication services (oauth2.googleapis.com). 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 9.10.1 or later
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed, starting with Cloud Volumes ONTAP 9.12.1 GA.
- You must be a cluster or SVM administrator
- An active Google Cloud Platform subscription

Limitations

- Cloud KMS can only be configured on a data SVM

Configuration

Google Cloud

1. In your Google Cloud environment, create a symmetric GCP key ring and key.
2. Create a custom role for your Cloud Volumes ONTAP service account.

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. Assign the custom role to the Cloud KMS key and Cloud Volumes ONTAP service account:
`gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`
4. Download service account JSON key:
`gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.
2. Switch to the advanced privilege level:
`set -privilege advanced`
3. Create a DNS for the data SVM.
`dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver`

SVM_name

4. Create CMEK entry:
`security key-manager external gcp enable -vserver SVM_name -project-id project -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
5. When prompted, enter the service account JSON key from your GCP account.
6. Confirm the enabled process succeeded:
`security key-manager external gcp check -vserver svm_name`
7. OPTIONAL: Create a volume to test encryption `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Improving protection against ransomware

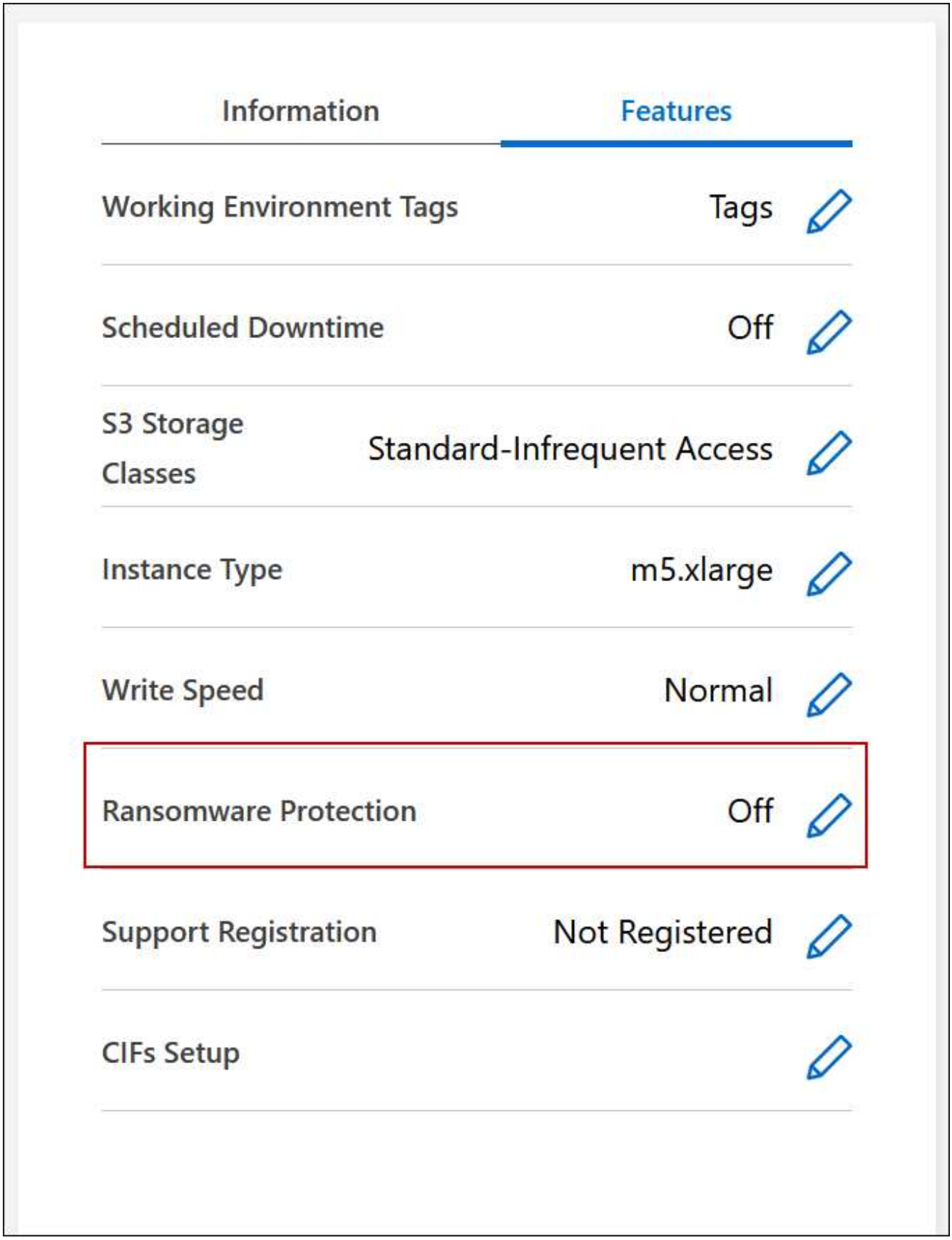
Ransomware attacks can cost a business time, resources, and reputation. BlueXP enables you to implement two NetApp solutions for ransomware: Protection from common ransomware file extensions and Autonomous Ransomware Protection (ARP). These solutions provide effective tools for visibility, detection,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



3. Implement the NetApp solution for ransomware:
   a. 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.

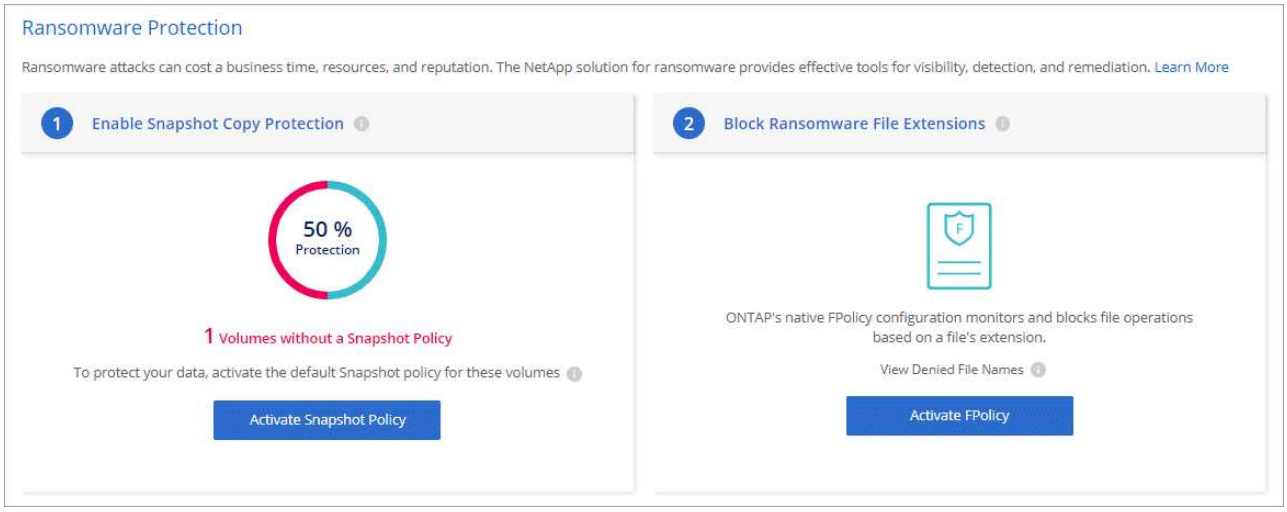
b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

   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.



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.

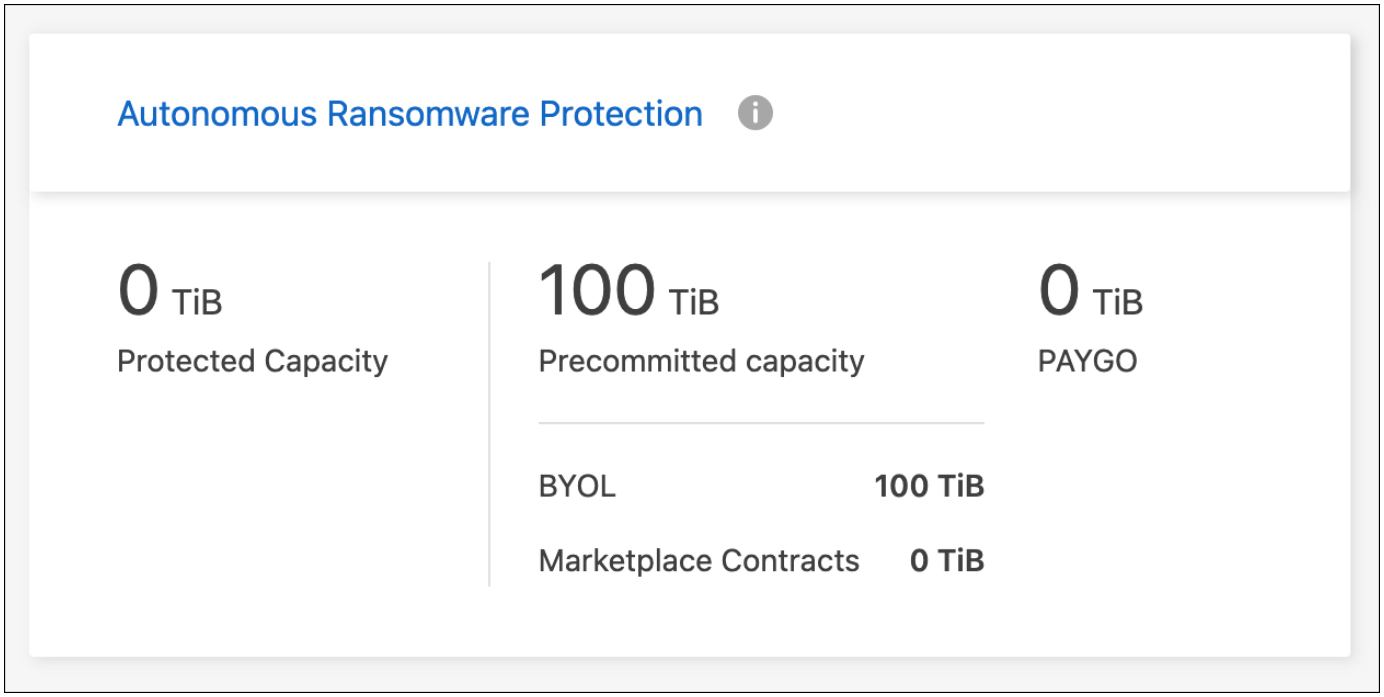
The ARP feature is available for use with BYOL licenses only (one, two, and three year terms) on both node-based and capacity-based licensing models. You must contact your NetApp sales representative to purchase a new, separate, add-on license for use with the ARP feature in Cloud Volumes ONTAP.

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. 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

Trademark information