Sicurezza e crittografia dei dati

Cloud Volumes ONTAP

NetApp
April 23, 2024

Sommario

Sicurezza e crittografia dei dati

Crittografia dei volumi con le soluzioni di crittografia NetApp

Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp (NVE) e la crittografia aggregata NetApp (NAE). NVE e NAE sono soluzioni software che consentono la crittografia dei volumi a riposo dei dati conforme a FIPS 140-2. "Scopri di più su queste soluzioni di crittografia".

NVE e NAE sono supportati con un gestore di chiavi esterno.

Gestione delle chiavi con AWS Key Management Service

È possibile utilizzare "KMS (Key Management Service) di AWS" Per proteggere le chiavi di crittografia ONTAP in un'applicazione implementata da AWS.

La gestione delle chiavi con AWS KMS può essere abilitata con l'interfaccia CLI o l'API REST ONTAP.

Quando si utilizza il KMS, tenere presente che per impostazione predefinita viene utilizzata la LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi del cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione di AWS. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.12.0 o successiva
- È necessario aver installato la licenza Volume Encryption (VE) e.
- È necessario aver installato la licenza MTEKM (Multi-tenant Encryption Key Management).
- Devi essere un amministratore del cluster o di SVM
- È necessario disporre di un abbonamento AWS attivo

> È possibile configurare le chiavi solo per una SVM dati.

Configurazione

AWS

1. È necessario creare un "concedi" Per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     Per creare una sovvenzione, fare riferimento a. "Documentazione AWS".
2. "Aggiungere un criterio al ruolo IAM appropriato." La policy dovrebbe supportare `DescribeKey`, `Encrypt`, e. `Decrypt` operazioni.

Cloud Volumes ONTAP

1. Passa all'ambiente Cloud Volumes ONTAP.
2. Passare al livello di privilegio avanzato:
   `set -privilege advanced`
3. Abilitare il gestore delle chiavi AWS:
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando richiesto, inserire la chiave segreta.
5. Verificare che AWS KMS sia stato configurato correttamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Gestisci le chiavi con Azure Key Vault

È possibile utilizzare "Azure Key Vault (AKV)" Per proteggere le chiavi di crittografia ONTAP in un'applicazione implementata da Azure.

AKV può essere utilizzato per proteggere "Chiavi NetApp Volume Encryption (NVE)" Solo per SVM di dati.

La gestione delle chiavi con AKV può essere abilitata con la CLI o l'API REST ONTAP.

Quando si utilizza AKV, tenere presente che per impostazione predefinita viene utilizzata una LIF SVM di dati per comunicare con l'endpoint di gestione delle chiavi cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.10.1 o successiva
- Licenza di crittografia dei volumi (VE) installata (la licenza di crittografia dei volumi NetApp viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp)
- È necessario disporre di una licenza per la gestione delle chiavi di crittografia multi-tenant (MT_EK_MGMT)
- Devi essere un amministratore del cluster o di SVM
- Un abbonamento Active Azure

Limitazioni

- AKV può essere configurato solo su una SVM dati
- NAE non può essere usato con AKV. NAE richiede un server KMIP supportato dall'esterno.

Processo di configurazione

I passaggi descritti spiegano come registrare la configurazione di Cloud Volumes ONTAP con Azure e come creare un archivio chiavi Azure. Se la procedura è già stata completata, assicurarsi di disporre delle impostazioni di configurazione corrette, in particolare nella sezione Creare un vault Azure Key, quindi passare a. Configurazione di Cloud Volumes ONTAP.

- Registrazione dell'applicazione Azure
- Creare un segreto per il client Azure

- Creare un vault Azure Key
- Creare una chiave di crittografia
- Creazione di un endpoint Azure Active Directory (solo ha)
- Configurazione di Cloud Volumes ONTAP

Registrazione dell'applicazione Azure

1. È necessario prima registrare l'applicazione nell'abbonamento Azure che si desidera utilizzare per accedere al vault delle chiavi Cloud Volumes ONTAP. All'interno del portale Azure, selezionare **registrazioni app**.
2. Selezionare **Nuova registrazione**.
3. Fornire un nome per l'applicazione e selezionare un tipo di applicazione supportato. Il tenant singolo predefinito è sufficiente per l'utilizzo di Azure Key Vault. Selezionare **Registra**.
4. Nella finestra Panoramica di Azure, selezionare l'applicazione registrata. Copiare l'ID **applicazione (client)** e l'ID **directory (tenant)** in una posizione sicura. Saranno richiesti più avanti nel processo di registrazione.

Creare un segreto per il client Azure

1. Nel portale Azure per la registrazione dell'applicazione Azure Key Vault, seleziona il pannello **certificati e segreti**.
2. Selezionare **nuovo segreto client**. Immettere un nome significativo per il client secret. NetApp consiglia un periodo di scadenza di 24 mesi; tuttavia, le policy di governance del cloud specifiche potrebbero richiedere un'impostazione diversa.
3. Fare clic su **Aggiungi** per creare il segreto del client. Copiare la stringa segreta elencata nella colonna **valore** e memorizzarla in una posizione sicura per utilizzarla successivamente in Configurazione di Cloud Volumes ONTAP. Il valore segreto non viene visualizzato di nuovo dopo aver allontanato la pagina.

Creare un vault Azure Key

1. Se si dispone già di un vault delle chiavi Azure, è possibile collegarlo alla configurazione di Cloud Volumes ONTAP; tuttavia, è necessario adattare i criteri di accesso alle impostazioni in questo processo.
2. Nel portale Azure, accedere alla sezione **Vaults chiave**.
3. Fare clic su **+Crea** e inserire le informazioni richieste, tra cui gruppo di risorse, regione e livello di prezzo. Inoltre, immettere il numero di giorni per conservare i vault cancellati e selezionare **Enable purge Protection** (attiva protezione di eliminazione) nel vault delle chiavi.
4. Selezionare **Avanti** per scegliere una policy di accesso.
5. Selezionare le seguenti opzioni:
   a. In **Configurazione Access**, selezionare **criterio di accesso al vault**.
   b. In **accesso alle risorse**, selezionare **crittografia disco Azure per la crittografia del volume**.
6. Selezionare **+Crea** per aggiungere una policy di accesso.
7. In **Configura da un modello**, fare clic sul menu a discesa, quindi selezionare il modello **Gestione chiavi, segreti e certificati**.
8. Scegliere ciascuno dei menu a discesa delle autorizzazioni (chiave, segreto, certificato), quindi **Seleziona tutto** nella parte superiore dell'elenco dei menu per selezionare tutte le autorizzazioni disponibili. Dovresti avere:
   - **Permessi chiave**: 20 selezionato
   - **Permessi segreti**: 8 selezionati

- **Permessi del certificato**: 16 selezionato

Create an access policy

1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Cryptographic Operations

- [x] Select all
- [x] Decrypt
- [x] Encrypt
- [x] Unwrap Key
- [x] Wrap Key
- [x] Verify
- [x] Sign

Privileged Key Operations

- [x] Select all
- [x] Purge
- [x] Release

Rotation Policy Operations

- [x] Select all
- [x] Rotate
- [x] Get Rotation Policy
- [x] Set Rotation Policy

Secret permissions

Secret Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Set
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Privileged Secret Operations

- [x] Select all
- [x] Purge

Certificate permissions

Certificate Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore
- [x] Manage Contacts
- [x] Manage Certificate Authorities
- [x] Get Certificate Authorities
- [x] List Certificate Authorities
- [x] Set Certificate Authorities
- [x] Delete Certificate Authorities

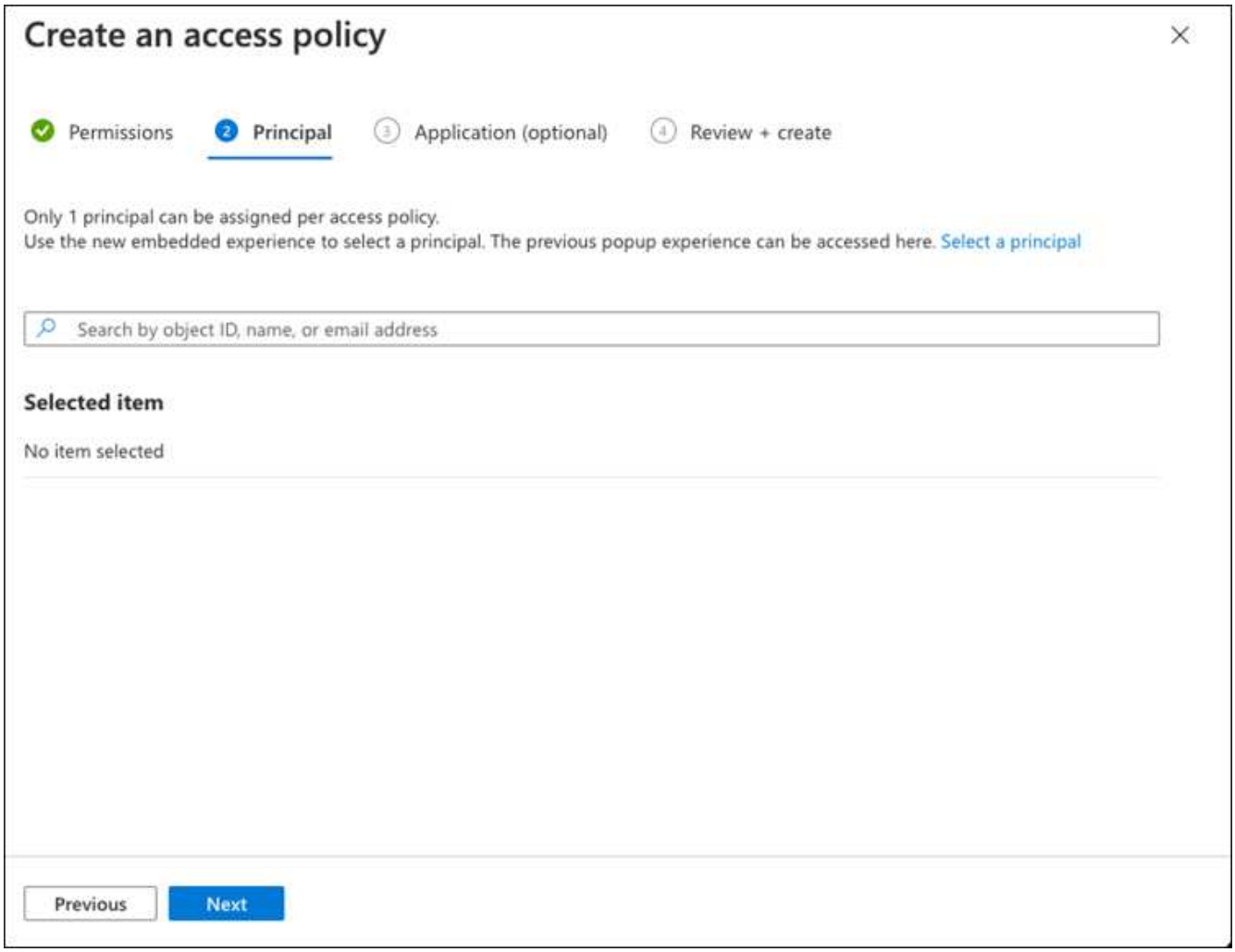
Privileged Certificate Operations

- [x] Select all
- [x] Purge

Previous Next

9. Fare clic su **Avanti** per selezionare l'applicazione registrata **Principal** Azure in cui è stata creata Registrazione dell'applicazione Azure. Selezionare **Avanti**.

> È possibile assegnare un solo principal per policy.



10. Fare clic su **Avanti** due volte fino a visualizzare **Rivedi e crea**. Quindi, fare clic su **Crea**.
11. Selezionare **Avanti** per passare alle opzioni **rete**.
12. Scegliere il metodo di accesso alla rete appropriato o selezionare **tutte le reti** e **Rivedi + Crea** per creare il vault delle chiavi. (Il metodo di accesso alla rete può essere prescritto da una policy di governance o dal tuo team di sicurezza del cloud aziendale).
13. Registrare l'URI del vault delle chiavi: Nel vault delle chiavi creato, accedere al menu Overview (Panoramica) e copiare l'URI del vault** dalla colonna di destra. Questo è necessario per un passaggio successivo.

Creare una chiave di crittografia

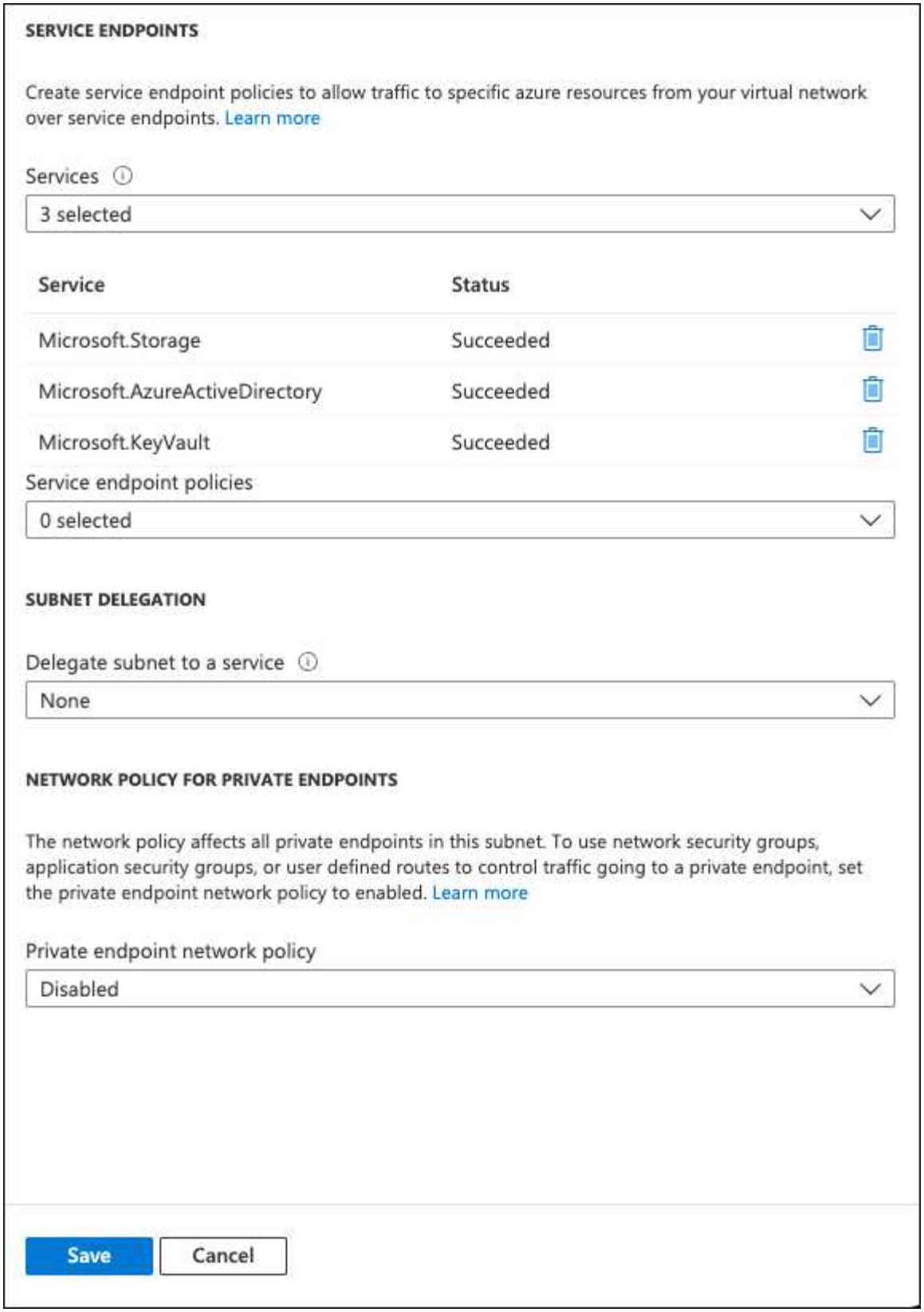
1. Nel menu del vault delle chiavi creato per Cloud Volumes ONTAP, selezionare l'opzione **chiavi**.
2. Selezionare **genera/importa** per creare una nuova chiave.
3. Lasciare l'opzione predefinita impostata su **genera**.
4. Fornire le seguenti informazioni:

- Nome della chiave di crittografia
- Tipo di chiave: RSA
- Dimensione chiave RSA: 2048
- Abilitato: Sì

5. Selezionare **Crea** per creare la chiave di crittografia.
6. Tornare al menu **tasti** e selezionare la chiave appena creata.
7. Selezionare l'ID della chiave in **versione corrente** per visualizzare le proprietà della chiave.
8. Individuare il campo **Key Identifier**. Copiare l'URI fino alla stringa esadecimale, ma non inclusa.

Creazione di un endpoint Azure Active Directory (solo ha)

1. Questo processo è necessario solo se si configura Azure Key Vault per un ambiente di lavoro ha Cloud Volumes ONTAP.
2. Nel portale Azure, accedere a **reti virtuali**.
3. Selezionare la rete virtuale in cui è stato implementato l'ambiente di lavoro Cloud Volumes ONTAP e selezionare il menu **subnet** sul lato sinistro della pagina.
4. Selezionare dall'elenco il nome della subnet per la distribuzione Cloud Volumes ONTAP.
5. Passare all'intestazione **endpoint del servizio**. Nel menu a discesa, selezionare:
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage** (opzionale)



6. Selezionare **Salva** per acquisire le impostazioni.

Configurazione di Cloud Volumes ONTAP

1. Connettersi alla LIF di gestione del cluster con il client SSH preferito.
2. Accedere alla modalità avanzata dei privilegi in ONTAP:

```
set advanced -con off
```

3. Identificare i dati SVM desiderati e verificarne la configurazione DNS:
   `vserver services name-service dns show`
   a. Se esiste una voce DNS per i dati SVM desiderati e contiene una voce per il DNS di Azure, non è richiesta alcuna azione. In caso contrario, aggiungere una voce del server DNS per la SVM dei dati che punta al DNS Azure, al DNS privato o al server on-premise. Questo deve corrispondere alla voce per l'amministratore del cluster SVM:
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`
   b. Verificare che il servizio DNS sia stato creato per i dati SVM:
      `vserver services name-service dns show`
4. Abilitare Azure Key Vault utilizzando l'ID client e l'ID tenant salvati dopo la registrazione dell'applicazione:
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > Il `_full_key_URI` il valore deve utilizzare `<https:// <key vault host name>/keys/<key label>` formato.

5. Dopo aver attivato con successo il vault delle chiavi di Azure, immettere il `client secret value` quando richiesto.
6. Controllare lo stato del gestore delle chiavi:
   `security key-manager external azure check`L'output sarà simile a:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Se il `service_reachability` lo stato non è `OK`, SVM non può raggiungere il servizio Azure Key Vault con tutte le autorizzazioni e la connettività richieste. Assicurati che le policy di rete e il routing di Azure non blocchino il tuo VNET privato dal raggiungere l'endpoint pubblico di Azure KeyVault. In caso affermativo, prendere in considerazione l'utilizzo di un endpoint Azure Private per accedere al vault delle chiavi

dall'interno di VNET. Per risolvere l'indirizzo IP privato dell'endpoint, potrebbe essere necessario aggiungere una voce di host statici sulla SVM.

Il `kms_wrapped_key_status` verrà segnalato `UNKNOWN` alla configurazione iniziale. Il suo stato cambierà in `OK` dopo la crittografia del primo volume.

7. FACOLTATIVO: Creare un volume di test per verificare la funzionalità di NVE.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   Se configurato correttamente, Cloud Volumes ONTAP crea automaticamente il volume e attiva la crittografia del volume.

8. Verificare che il volume sia stato creato e crittografato correttamente. In tal caso, il `-is-encrypted` il parametro viene visualizzato come `true`.
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```

Gestisci le chiavi con il Cloud Key Management Service di Google

È possibile utilizzare "Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)" Per proteggere le chiavi di crittografia ONTAP in un'applicazione implementata dalla piattaforma cloud Google.

La gestione delle chiavi con Cloud KMS può essere abilitata con la CLI o l'API REST di ONTAP.

Quando si utilizza Cloud KMS, tenere presente che per impostazione predefinita viene utilizzata la LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi del cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (oauth2.googleapis.com). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.10.1 o successiva
- Licenza VE (Volume Encryption) installata
- Licenza di gestione delle chiavi di crittografia multi-tenant (MTEKM) installata, a partire da Cloud Volumes ONTAP 9.12.1 GA.
- Devi essere un amministratore del cluster o di SVM
- Un abbonamento attivo a Google Cloud Platform

Limitazioni

- Cloud KMS può essere configurato solo su una SVM dati

Configurazione

Google Cloud

1. Nel tuo ambiente Google Cloud, "Creare un anello e una chiave GCP simmetrici".
2. Creare un ruolo personalizzato per l'account del servizio Cloud Volumes ONTAP.

```
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. Assegnare il ruolo personalizzato alla chiave KMS cloud e all'account del servizio Cloud Volumes ONTAP:
   `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. Scarica la chiave JSON dell'account di servizio:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Connettersi alla LIF di gestione del cluster con il client SSH preferito.
2. Passare al livello di privilegio avanzato:
   `set -privilege advanced`
3. Creare un DNS per i dati SVM.
   `dns create -domains c.`*`<project>`*`.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
4. Crea voce CMEK:
   `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. Quando richiesto, inserire la chiave JSON dell'account di servizio dal proprio account GCP.
6. Confermare che il processo di abilitazione è riuscito:
   `security key-manager external gcp check -vserver` *`svm_name`*
7. FACOLTATIVO: Creare un volume per verificare la crittografia `vol create` *`volume_name`* `-aggregate` *`aggregate`* `-vserver` *`vserver_name`* `-size 10G`

Risolvere i problemi

Se è necessario risolvere il problema, è possibile eseguire il tail dei log REST API raw nei due passaggi precedenti:

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

Miglioramento della protezione contro ransomware

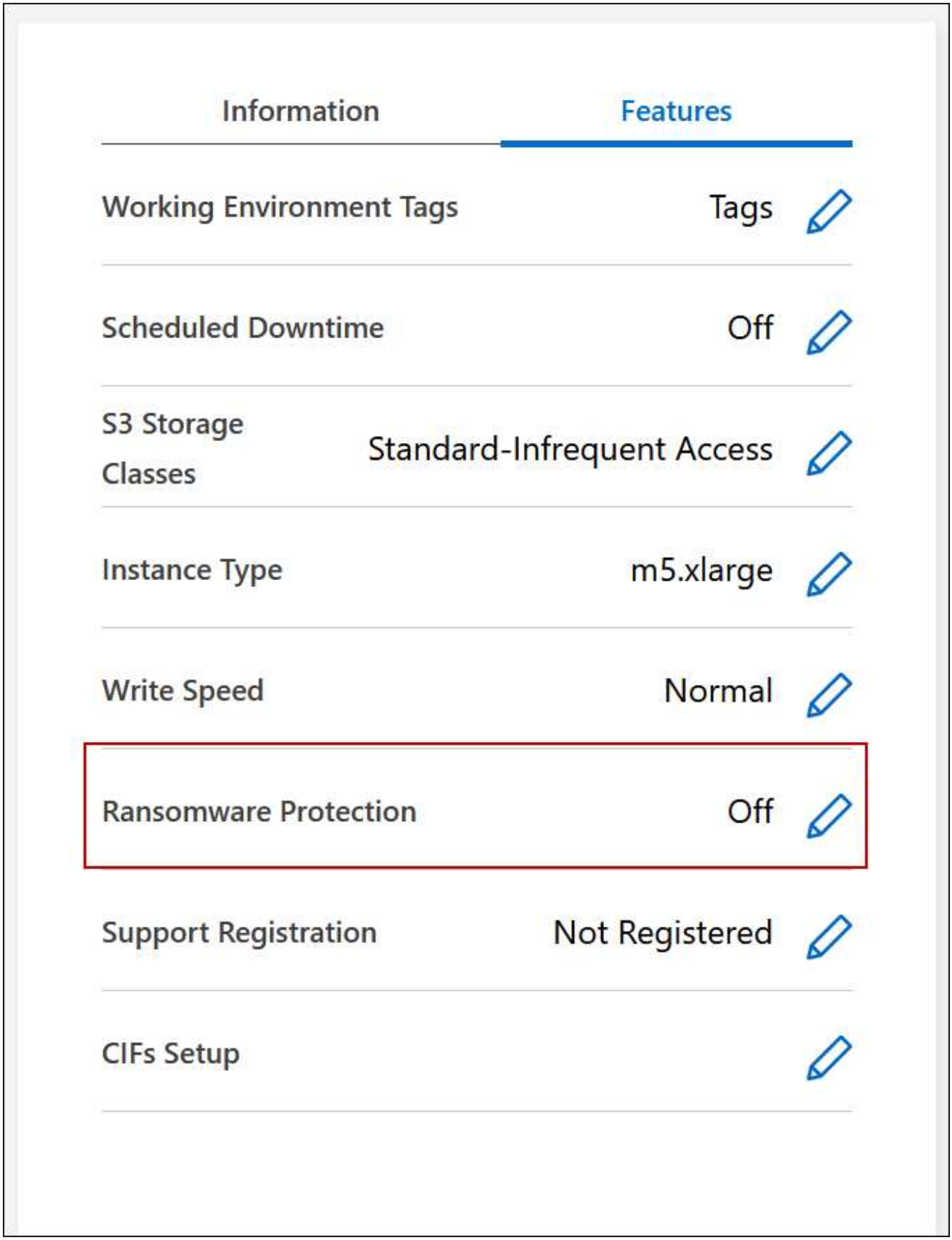
Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. BlueXP ti permette di implementare due soluzioni NetApp per il ransomware: Protezione dalle comuni estensioni di file ransomware e protezione autonoma dal ransomware (ARP). Queste soluzioni forniscono strumenti efficaci per visibilità, rilevamento e correzione.

Protezione dalle comuni estensioni di file ransomware

Disponibile tramite BlueXP, l'impostazione di protezione ransomware consente di utilizzare la funzionalità FPolicy di ONTAP per proteggersi dai comuni tipi di estensione di file ransomware.

Fasi

1. Nella pagina Canvas, fare doppio clic sul nome del sistema configurato per la protezione ransomware.
2. Nella scheda Overview (Panoramica), fare clic sul pannello Features (funzionalità), quindi sull'icona a forma di matita accanto a **ransomware Protection**.



3. Implementare la soluzione NetApp per ransomware:

   a. Fare clic su **Activate Snapshot Policy** (attiva policy Snapshot) se si dispone di volumi che non hanno

una policy Snapshot attivata.

La tecnologia Snapshot di NetApp offre la migliore soluzione del settore per la risoluzione dei problemi ransomware. La chiave per un ripristino corretto è il ripristino da backup non infetti. Le copie Snapshot sono di sola lettura, impedendo la corruzione del ransomware. Possono inoltre offrire la granularità necessaria per creare immagini di una singola copia di file o di una soluzione completa di disaster recovery.

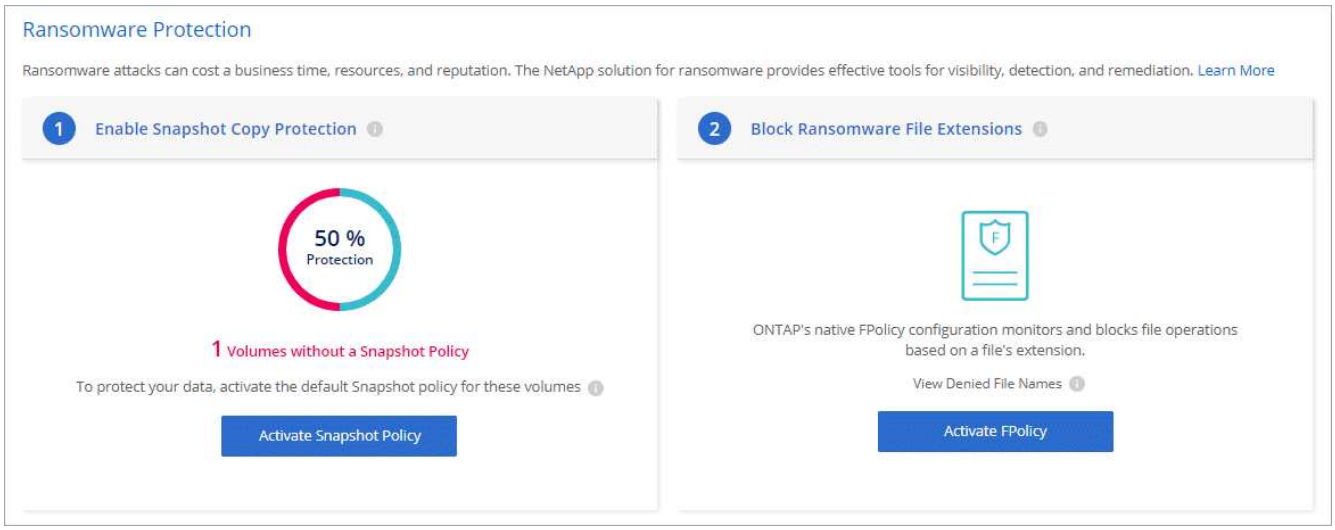
b. Fare clic su **Activate FPolicy** (attiva FPolicy) per attivare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione di un file.

   Questa soluzione preventiva migliora la protezione dagli attacchi ransomware bloccando i tipi di file ransomware più comuni.

   L'ambito FPolicy predefinito blocca i file con le seguenti estensioni:

   micro, crittografato, bloccato, criptato, criptato, Crinf, r5a, XRNT, XTBL, R16M01D05, PzDC, Good, LOL!, OMG!, RDM, RRK, encodedRS, crjoker, encifered, LeChiffre

   BlueXP crea questo ambito quando si attiva FPolicy su Cloud Volumes ONTAP. L'elenco si basa su tipi di file ransomware comuni. È possibile personalizzare le estensioni dei file bloccati utilizzando i comandi *vserver fpolicy scope* della CLI di Cloud Volumes ONTAP.



Protezione ransomware autonoma

Cloud Volumes ONTAP supporta la funzionalità di protezione ransomware autonoma (ARP), che esegue analisi sui carichi di lavoro per rilevare e avvisare in modo proattivo in caso di attività anomale che potrebbero indicare un attacco ransomware.

Separare dalle protezioni di estensione file fornite attraverso "impostazione di protezione dal ransomware", La funzione ARP utilizza l'analisi del carico di lavoro per avvisare l'utente in caso di potenziali attacchi in base a "attività anomala" rilevata. Sia l'impostazione di protezione dal ransomware che la funzione ARP possono essere utilizzate insieme per una protezione completa dal ransomware.

La funzione ARP è disponibile solo con le licenze BYOL (da 1 a 36 mesi) sia sui modelli di licenza basati sulla capacità che su nodi. Per acquistare una nuova licenza aggiuntiva separata da utilizzare con la funzionalità ARP di Cloud Volumes ONTAP, è necessario contattare il rappresentante commerciale NetApp.

La licenza ARP è considerata una licenza "mobile", il che significa che non è legata a una singola istanza Cloud Volumes ONTAP e può essere applicata a più ambienti Cloud Volumes ONTAP.

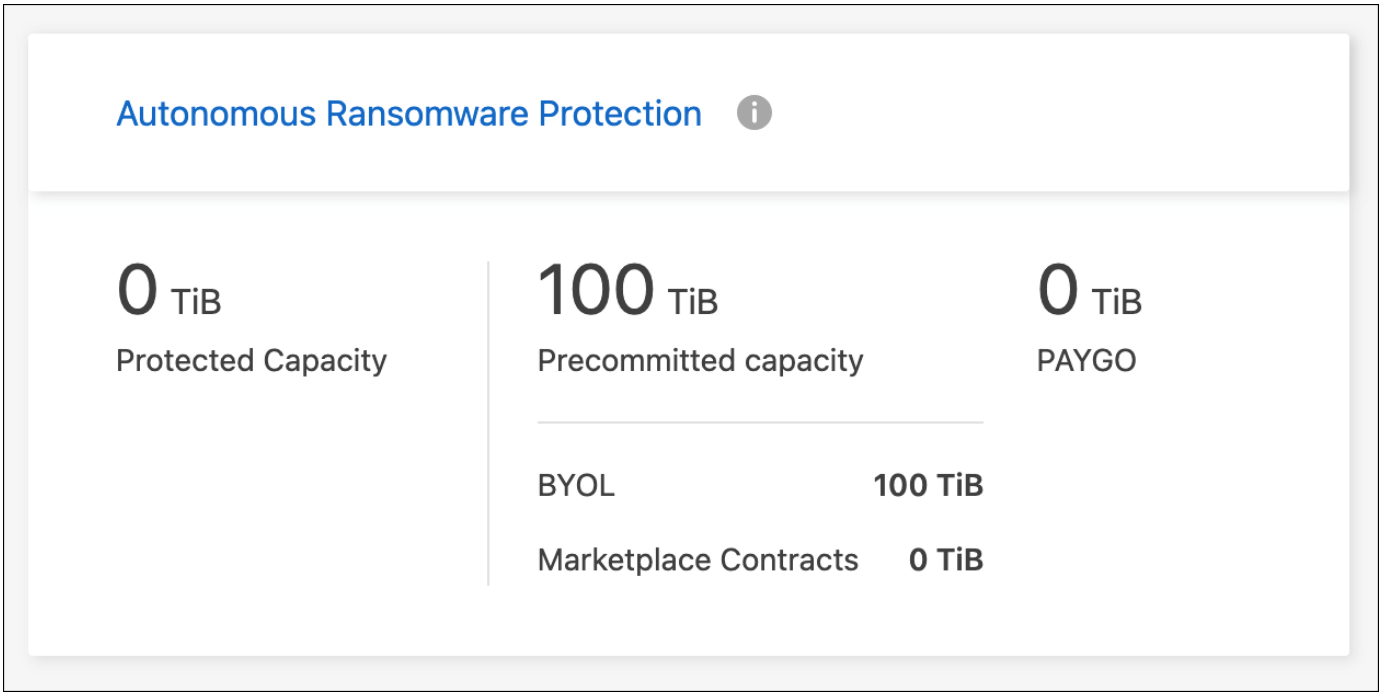
> L'utilizzo della funzione ARP con le licenze Cloud Volumes ONTAP basate su nodi non è attualmente presente nel Digital Wallet. La possibilità di visualizzare l'utilizzo dell'ARP basato su nodi sarà disponibile in Digital Wallet in una versione futura.

Acquistando una licenza add-on e aggiungendola al portafoglio digitale, puoi abilitare ARP per volume con Cloud Volumes ONTAP. La ricarica per ARP viene misurata a un livello di volume, in base alla capacità totale dei volumi con la funzione ARP abilitata. La capacità minima di licenza è di 1TB TB. Tuttavia, non è prevista una ricarica della capacità minima per la funzione ARP.

I volumi abilitati per ARP hanno lo stato designato "modalità di apprendimento" o "attivo". Qualsiasi volume con stato ARP "Disabilitato" è escluso dalla ricarica. Ad esempio, un ambiente Cloud Volumes ONTAP con 30 TiB di capacità sottoposta a provisioning può scegliere di avere solo un sottoinsieme di volumi TIB 15 con ARP attivato.

La configurazione di ARP per i volumi viene eseguita tramite Gestore di sistema di ONTAP e CLI di ONTAP.

Per ulteriori informazioni su come attivare ARP con Gestione di sistema e CLI di ONTAP, vedere "Attiva la protezione ransomware autonoma".



> Il supporto non è disponibile per l'uso di funzioni con licenza senza licenza.