Exercise 5: Configuring the S3 Protocol in a Storage VM

In this exercise, you use best practice tools to create a Simple Storage Service (S3) server in a storage VM. The S3 protocol and NAS protocols can coexist in the same storage VM. However, S3 user accounts are separate from NFS and SMB users and do not belong to the same authentication domain. Therefore, NetApp recommends creating a separate storage VM for S3.

Objectives

This exercise focuses on enabling you to do the following:

- Create a storage VM to host the S3 protocol
- Create and verify S3 buckets
- Create S3 user accounts
- Access an S3 bucket from an S3 client
- Configure S3 protocol access to a NAS share

Case Study

Zarrot Industries wants to create an S3 object store to support mobile-friendly applications.

You create a storage VM to host the S3 object store and enable the S3 access protocol.

You create S3 user accounts to control access to the S3 object store.

You create an S3 bucket and verify that users can access it.

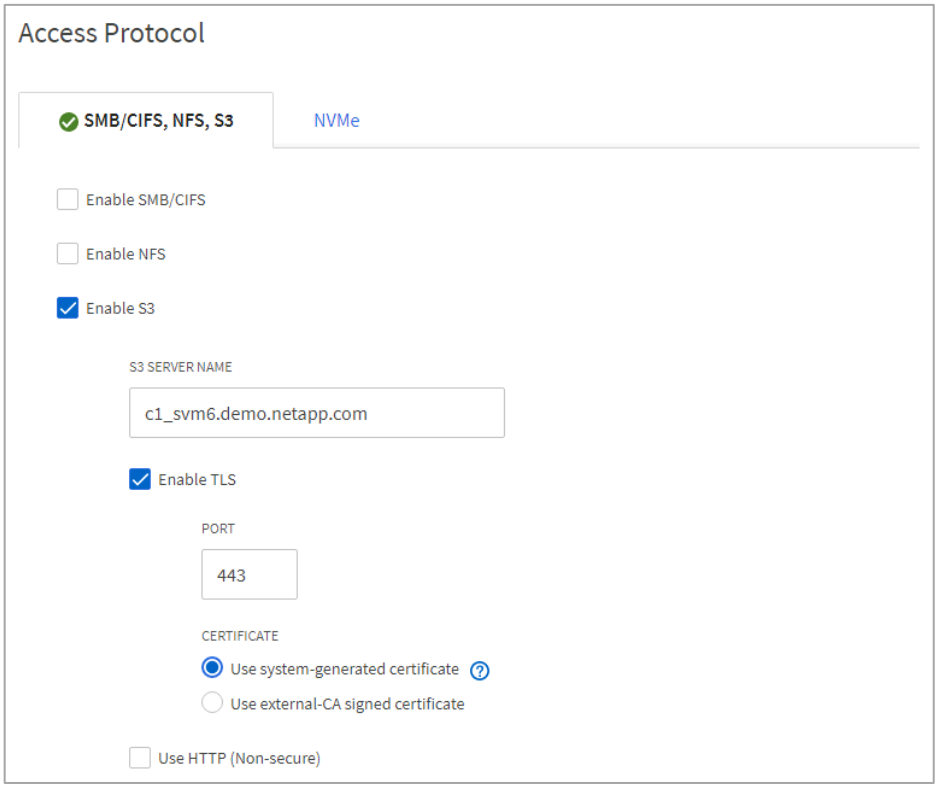
Lab Equipment

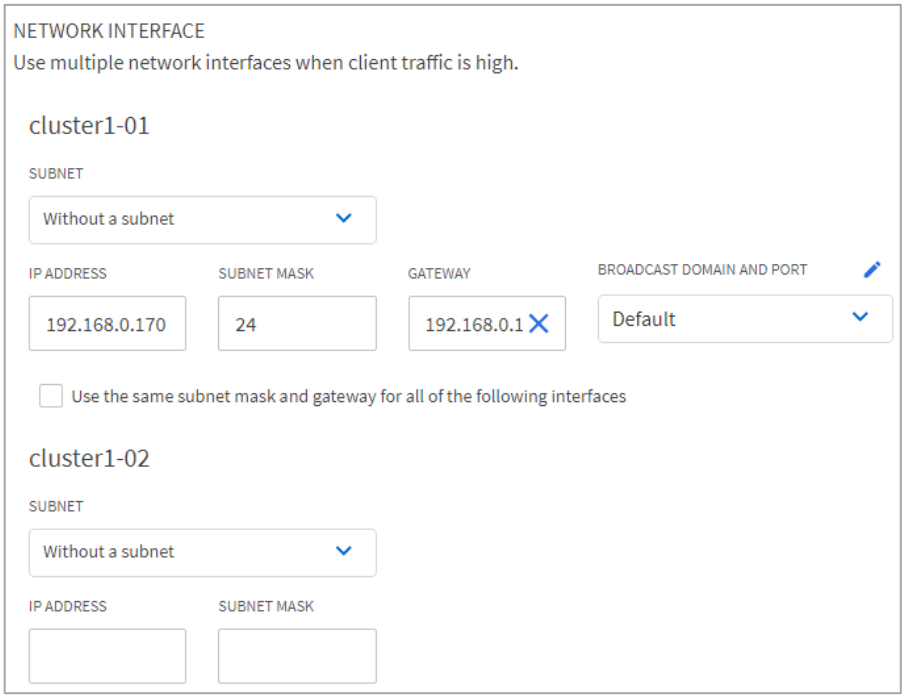
Use the following equipment to complete the exercise:

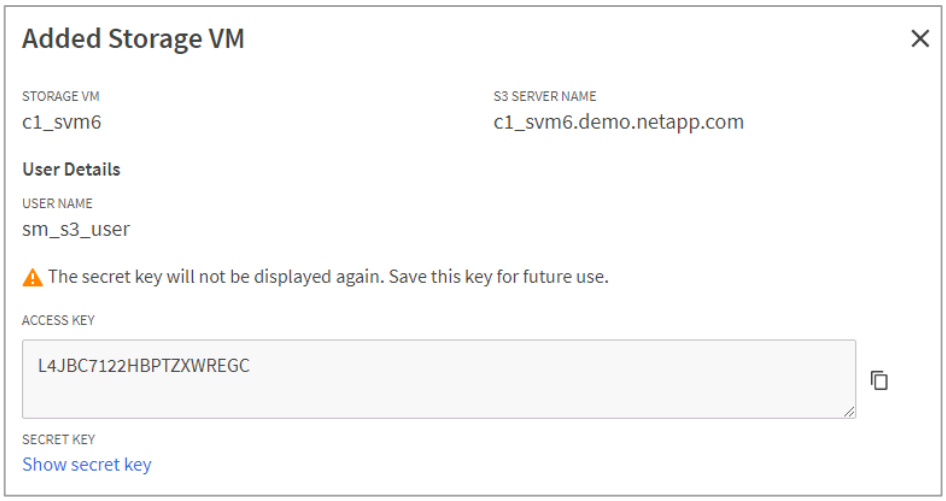
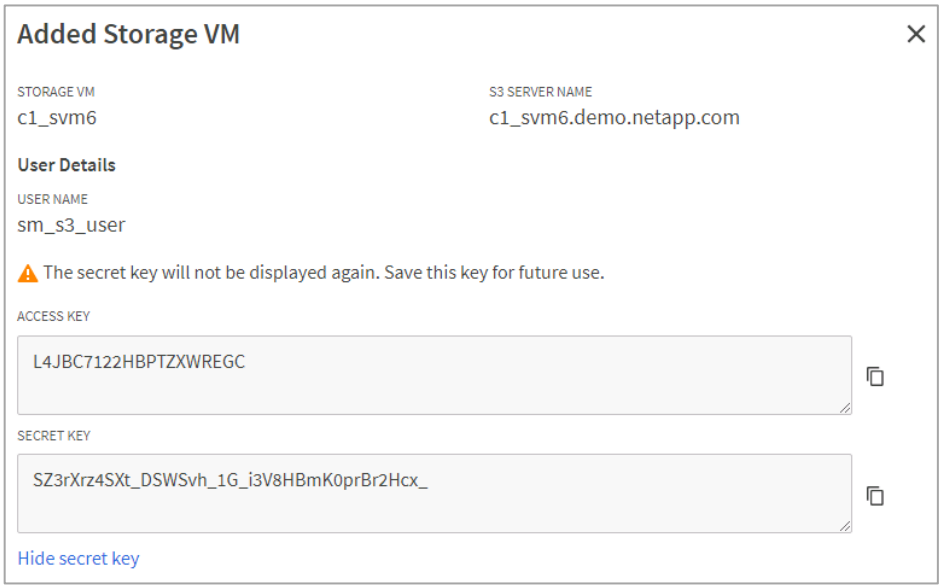
f	Host Name	IP Addresses	User Name	Password
Windows Server	Jumphost	192.168.0.5	DEMO\Administrator	Netapp1!
ONTAP cluster-management LIF (cluster1)	cluster1	192.168.0.101	admin (case sensitive)	Netapp1!

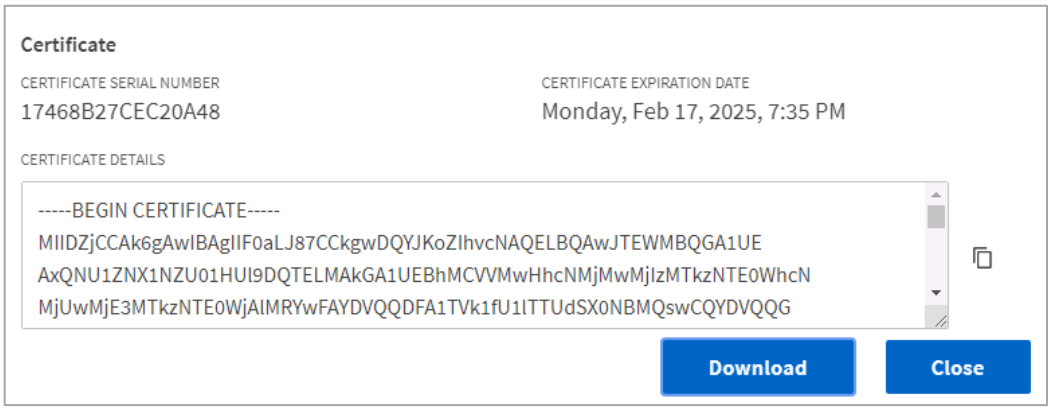
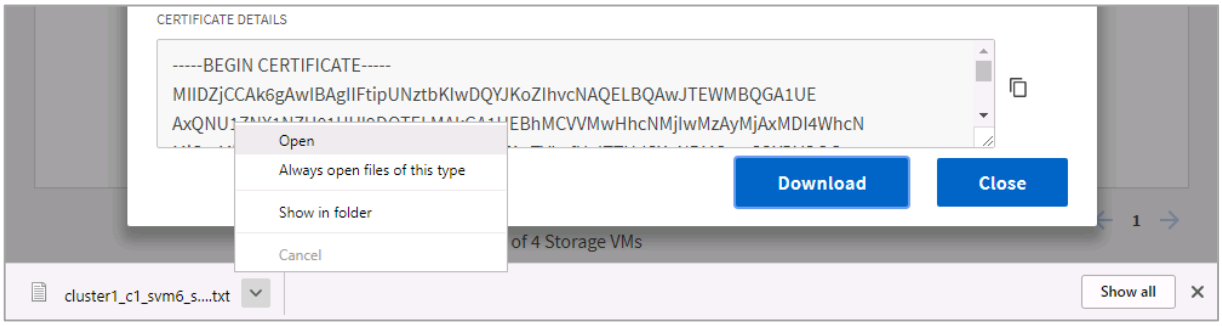
Task 1: Enable the S3 Protocol in a Storage VM

Step	Action
1-1	Log in to NetApp ONTAP System Manager for **cluster1**.
1-2	From the System Manager menu, select **Storage > Storage VMs**.
1-3	Click **Add**.
1-4	On the Add Storage VM page, in the Storage VM Name field, enter **c1_svm6**. 

Step	Action
1-5	Scroll to the Access Protocol section, and then specify the following settings: • Enable S3: **<selected>** • S3 Server Name: **c1_svm6.demo.netapp.com** • Enable TLS: **<selected>** (default) • Port: **443** (default) • Use system-generated certificate: **<selected>** (default) 
1-6	Accept the default language. 

Step	Action
1-7	In the Network Interface section, specify the following settings: • Subnet: **Without a subnet** (default) • IP Address: **192.168.0.170** • Subnet mask: **24** • Gateway: **192.168.0.1** (default) • Broadcast Domain and Port: **Default** 
1-8	Do not delegate administration of this storage VM. 
1-9	Review the configuration, and then click **Save**.

Step	Action
1-10	On the Added Storage VM page, observe the S3 server information and the name of the automatically created user account. 
1-11	Click **Show secret key**.
1-12	Observe the S3 user access key and secret access key. 
1-13	This window is your only opportunity to view and capture the S3 user access keys. If you have not downloaded or otherwise saved the keys, and the keys are lost, you must generate new access keys for the user.

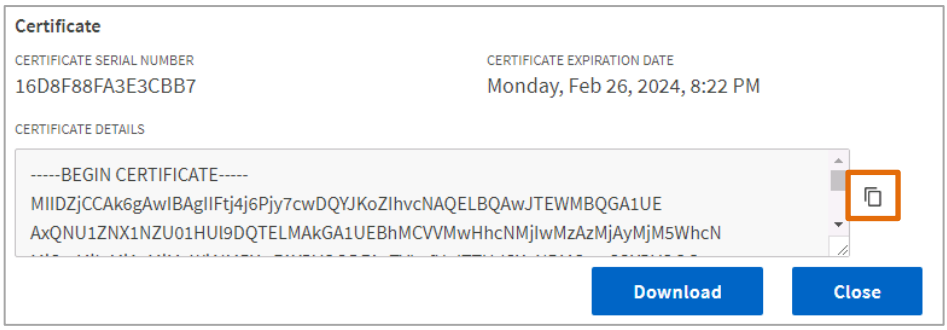
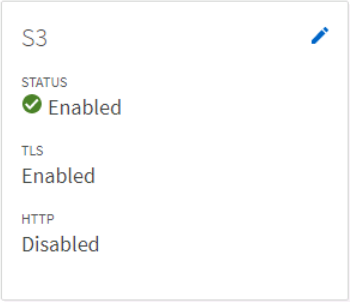
Step	Action
1-14	When you use a system-generated certificate, the certificate information is included in the Added Storage VM page. You can also view the storage VM Transport Layer Security (TLS) certificate on the Storage VM Settings page. 
1-15	Click **Download**.
1-16	Open the downloaded file. 

Step	Action
1-17	Examine the contents of the downloaded file and identify the following information: • S3 server name • S3 server IP address • S3 user name • S3 user access key • S3 user secret access key • S3 server security certificate

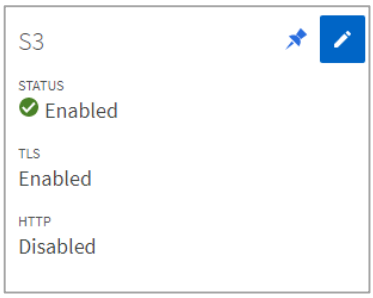
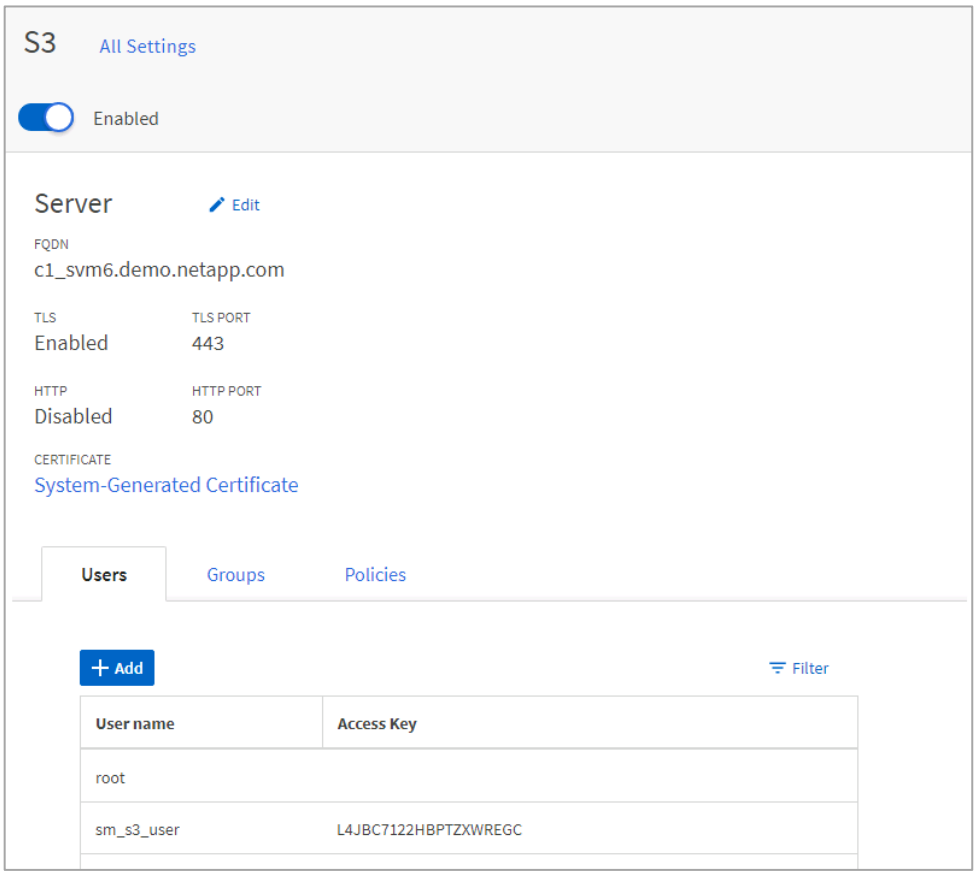
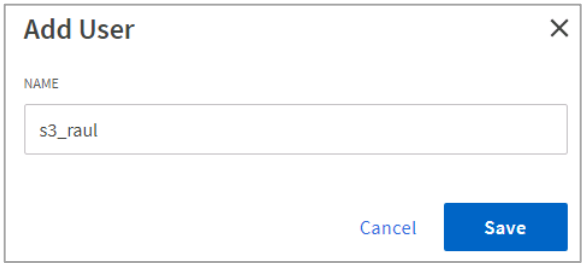
cluster1_c1_svm6_s3_details (1) - Notepad

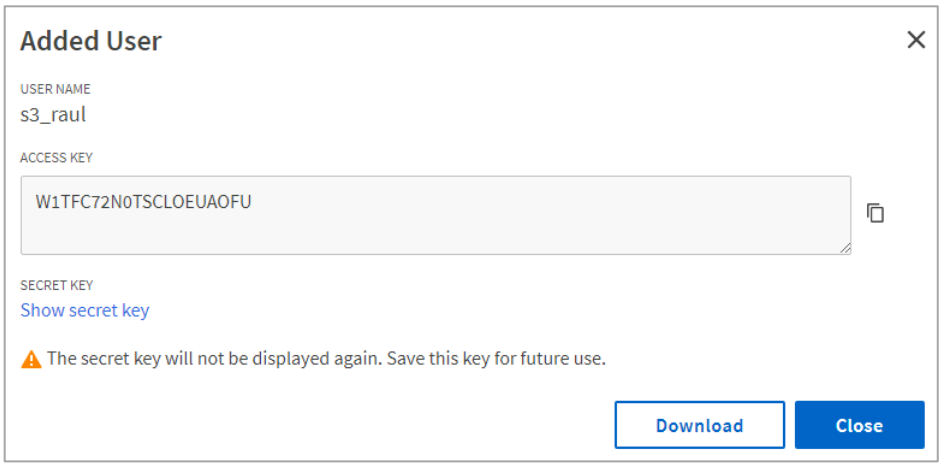
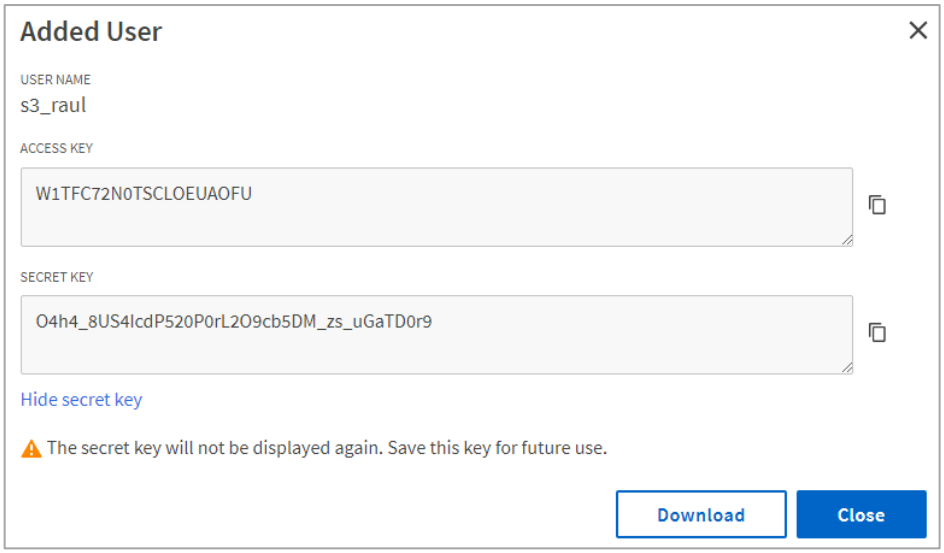
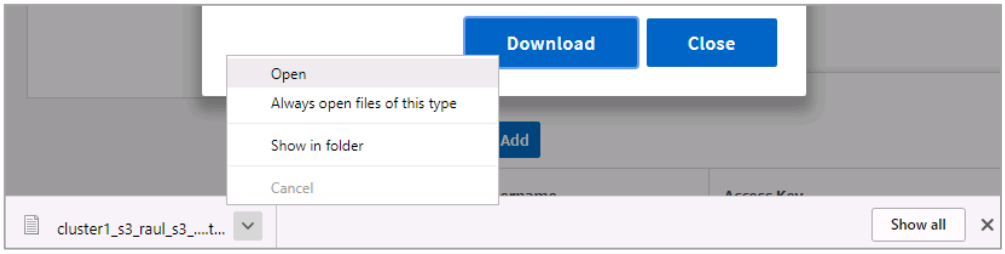
File Edit Format View Help

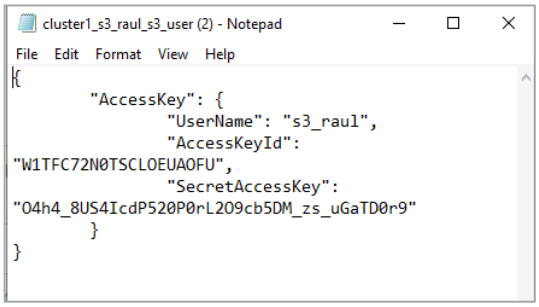
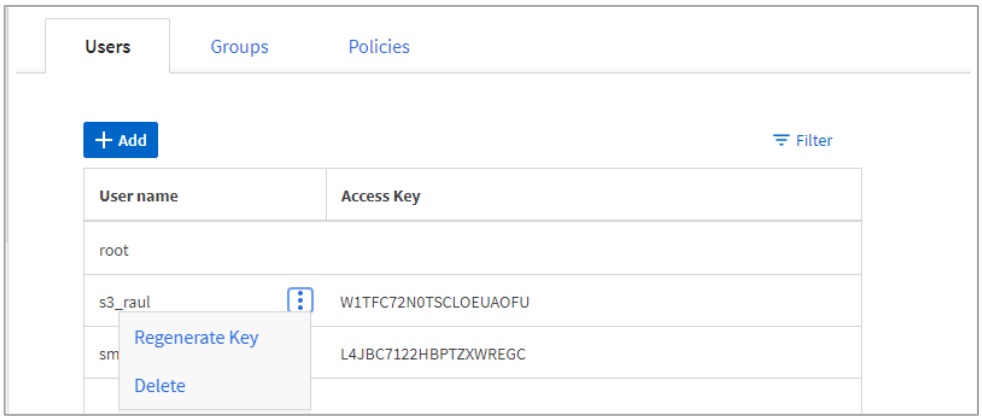

```
Storage VM:
c1_svm6

S3 Server Name:
c1_svm6.demo.netapp.com

Network IP Interfaces:
192.168.0.170

User Name:
sm_s3_user

Access Key:
L4JBC7122HBPTZXWREGC

Secret Key:
SZ3rXrz4SXt_DSWSvh_1G_i3V8HBmK0prBr2Hcx_

CERTIFICATE SERIAL NUMBER:
16D8F88FA3E3CBB7

CERTIFICATE DETAILS:
-----BEGIN CERTIFICATE-----
MIIDZjCCAk6gAwIBAgIIFtj4j6Pjy7cwDQYJKoZIhvcNAQELBQAwJTEWMBQGA1UE
AxQNU1ZNX1NZU01HU19DQTELMAkGA1UEBhMCVVMwHhcNMjIwMzAzMjAyMjM5WhcN
MjQwMjI2MjAyMjM5WjAlMRYwFAYDVQQDFA1TVk1fU11TTUdSX0NBMQswCQYDVQQG
EwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALXPvG8eXqajlugf
AYKpJHa1UkeX7c9tb+1UF0LiVsurPtQhet23EFeH8KlJldv7v/bZEBjVMBEGbgzF
S9YhdzOYf1n2SNkLcUQcxwL4vZGNvEIVZE3f4ZXQUWP5C1UpoFzOsN1H9tDzyepr
PkW1TjTy5mMv+VVE6BuCZeTqWA4FuHYnovjbWcJ748X8c+dYTvDlN2btxPrT+8/D
uQ9u47YlFAkgY8gpe/gc0dFVp6ItzGQ0rZU0Ftc2uIgqS5HpvH/5GqUv/qFU7ZCo
WAbfcEe8+6QWtnsolC4l4GY6N9fEyd6lVEsNxxXkt35ypfXXE29P9O91d9WAmZyP
ScMVehsCAwEAAaOBmTCBljAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIB
BjAdBgNVHQ4EFgQU8mN3AFKx3hlWwo0R3EuO0KM7heswVAYDVR0jBE0wS4AU8mN3
AFKx3hlWwo0R3EuO0KM7heuhKaQnMCUxFjAUBgNVBAMUDVNWTV9TWVNNR1JfQ0Ex
CzAJBgNVBAYTAlVTgggW2PiPo+PLtzANBgkqhkiG9w0BAQsFAAOCAQEAlnWVG+Ac
8AkVX+D1Ak8yzH/wFnkLDY7jgQmF74K7Wm26fKA6aMsnImG2er3V2MH97QM4xGy7
uPHg9Gd9In6MMCgjEdJXB4pLHAd6JsqpCGC6vG1LWUU+4lbdnOCSttFfpnityrVH
p1YIwtzVRuSYMK67+ng/F8IQXHRrIj/zRlWeIKwwJthXlbqi/+/HX2eU3znCEmgZ
ws17k3Igry6Ufk1DhPyGLtBh8ZbXSsZ2iUaCquxyiJ+yNNrkMzCk5MAmmh+NxG73
/nZZNej1oz+KkHkq0qPij7mzCSN76dqpkW14kyfud/YYuV54RuMdnilg8Z8ENEFX
3+T7UGluliPzXg==
-----END CERTIFICATE-----
```

Step	Action
1-18	Copy the TLS certificate to your clipboard, either manually or by using the copy to clipboard icon. 
1-19	Open a new Notepad window, paste the certificate text into the window, and then save the file as **svm6cert.crt**. 
1-20	Verify that no extra spaces or lines appear before the Begin Certificate or after the End Certificate statements.
1-21	Return to System Manager, and then click **Close** to close the Added Storage VM window.
1-22	On the Storage VMs page, click **c1_svm6**, and then click the **Settings** tab.
1-23	Verify that the S3 protocol is enabled. 

Task 2: Create an S3 User Account

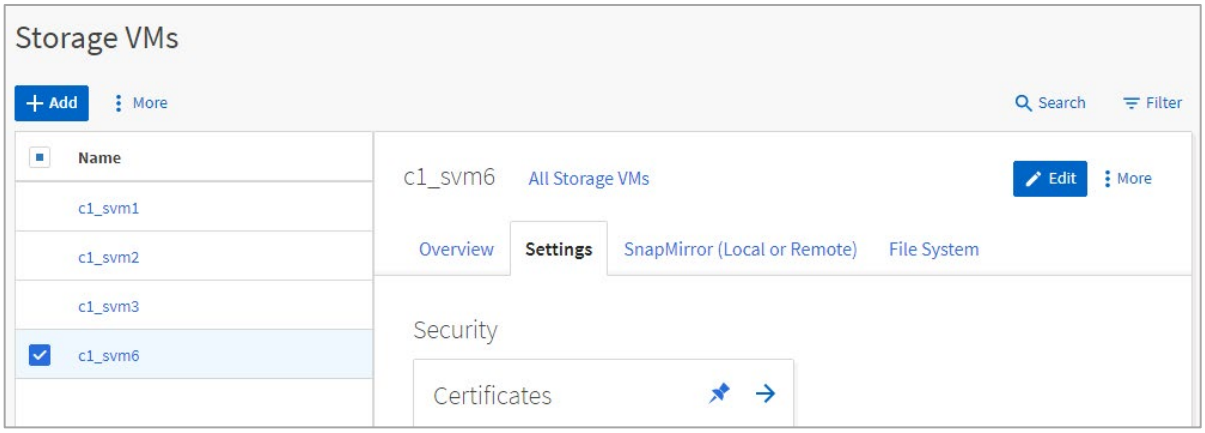
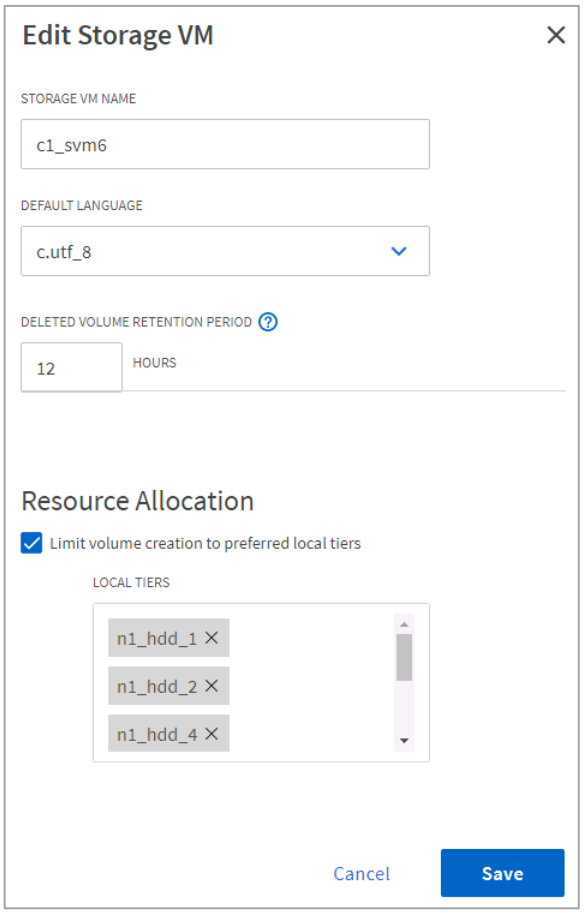
Step	Action
2-1	Click the edit (pencil) icon in the S3 pane to change the S3 settings. 
2-2	On the Users tab of the S3 server page, click the **Add** button. 
2-3	Enter a name for your S3 user account, and then click **Save**. 

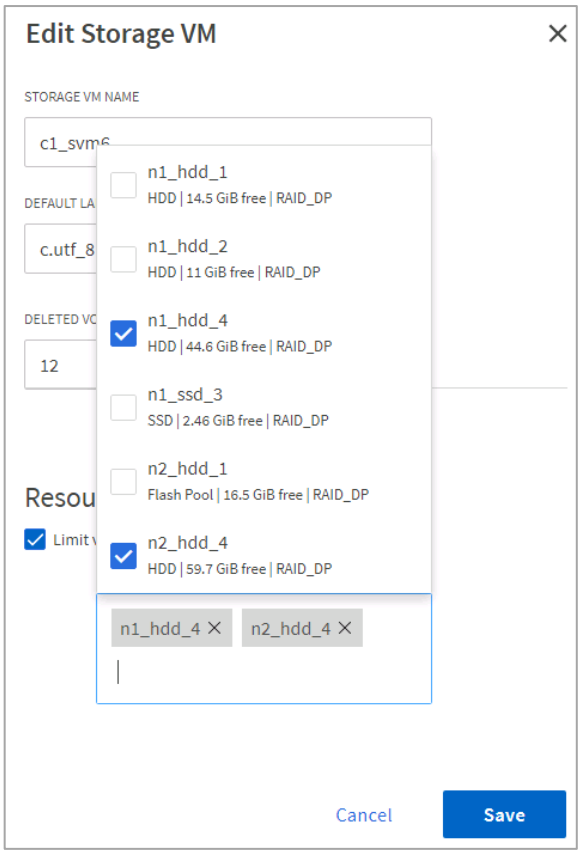
Step	Action
2-4	In the Added User page, observe the S3 user information and access key. 
2-5	Click **Show secret key**.
2-6	Observe the S3 user access key and secret access key. 
2-7	This window is your only opportunity to view and capture the S3 user access keys. If you have not downloaded or otherwise saved the keys and the keys are lost, you must generate new access keys for the user.
2-8	Click **Download**.
2-9	Open the downloaded file. 

Step	Action
2-10	Examine the contents of the downloaded file and identify the following information: • S3 user name • S3 user access key • S3 user secret access key 
2-11	Return to System Manager, and then click **Close** to close the Added User window.
2-12	On the S3 Server page, position your cursor over the new S3 user name, and then click the More menu icon. 
2-13	Dismiss the More menu.
2-14	Click **All Settings** to return to the SVM details page.

Task 3: Control Storage VM Access to Aggregates

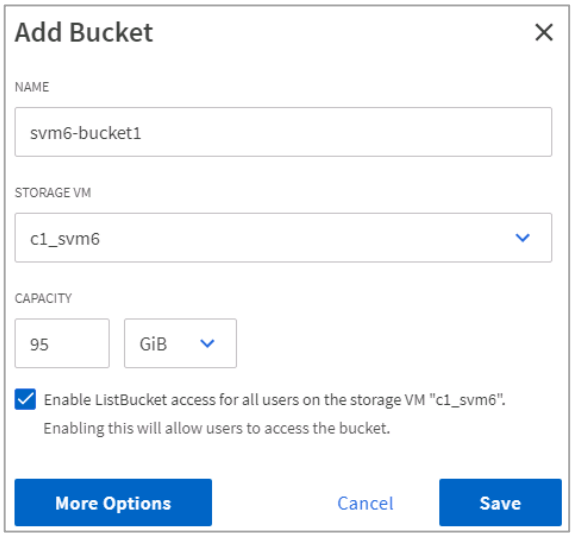
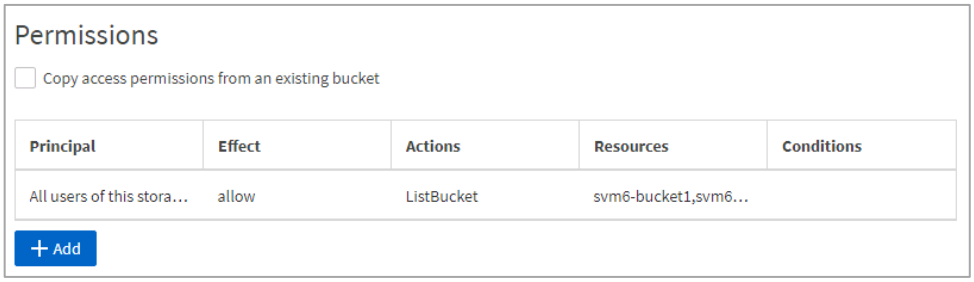
Specify in which aggregates a storage VM may create volumes.

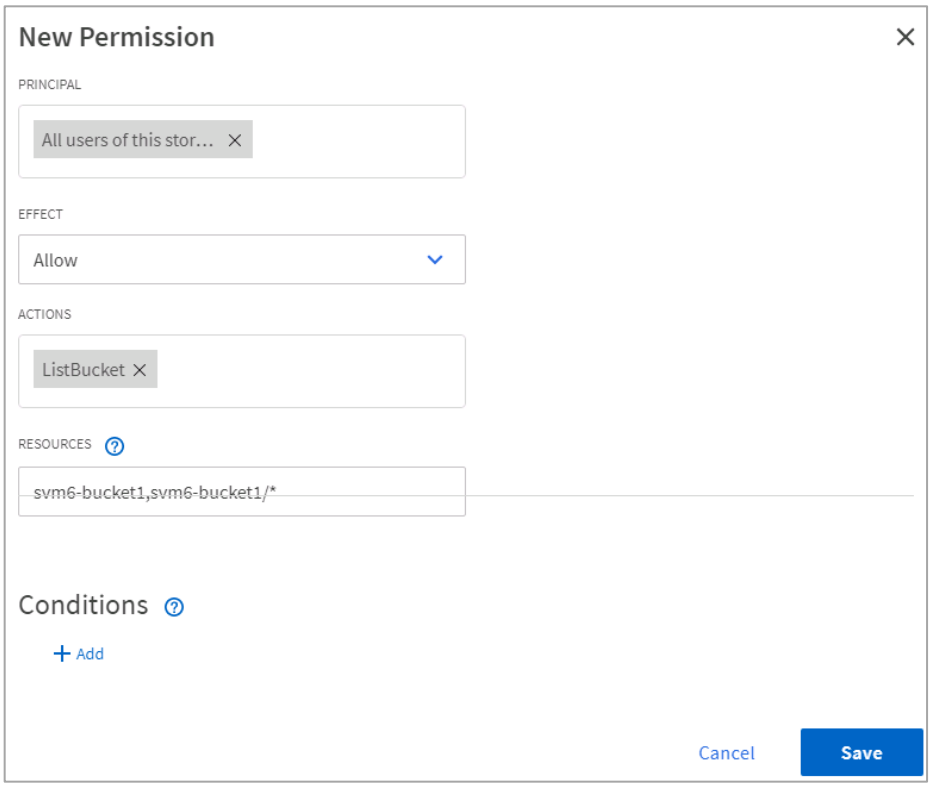
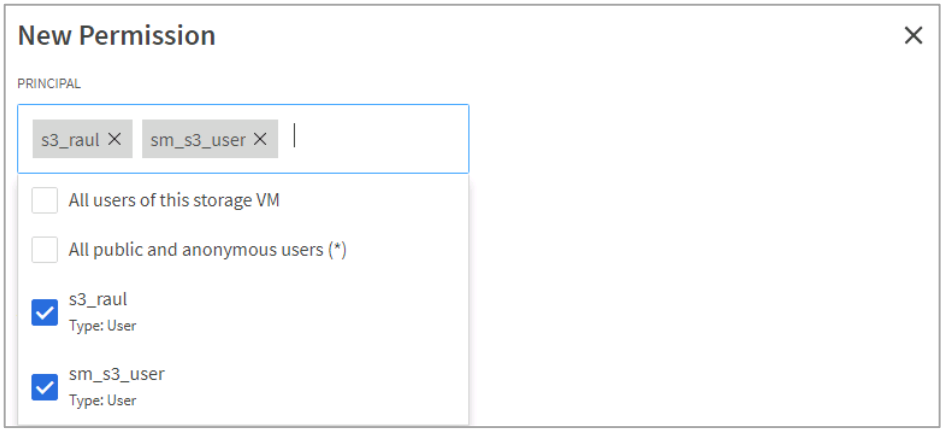
Step	Action
3-1	On the c1_svm6 details page, click **Edit**. 
3-2	In the Resource Allocation section, select the **Limit volume creation to preferred local tiers** checkbox. 

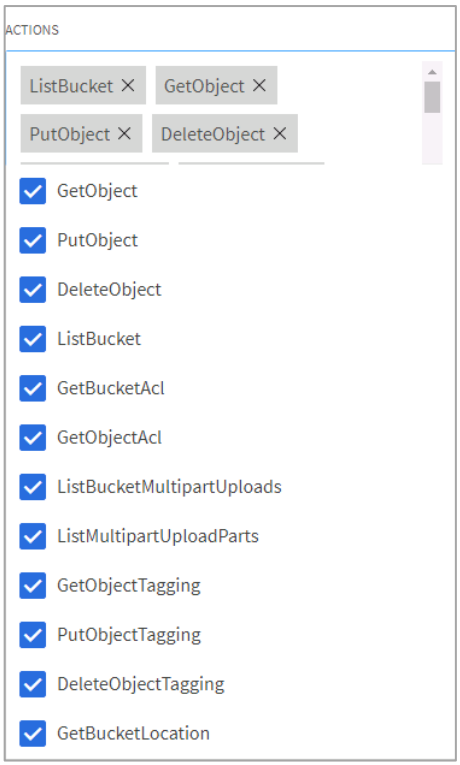
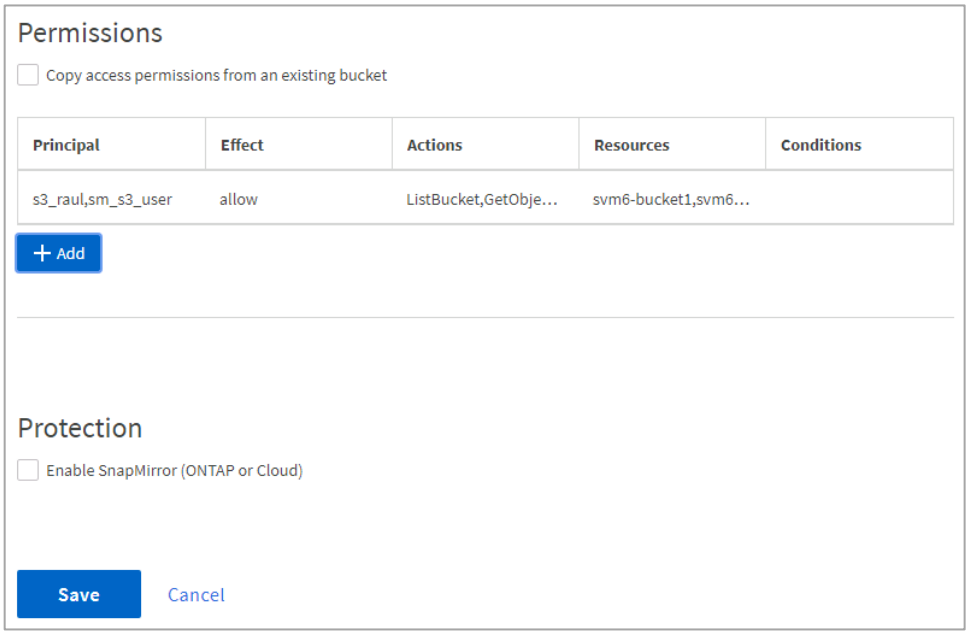
Step	Action
3-3	Remove each of the local tiers, except for n1_hdd_4 and n2_hdd_4, from the preferred tiers list. 
3-4	Click in the Local tiers box to open a menu of local tiers from which you can select.
3-5	Click **Save**.

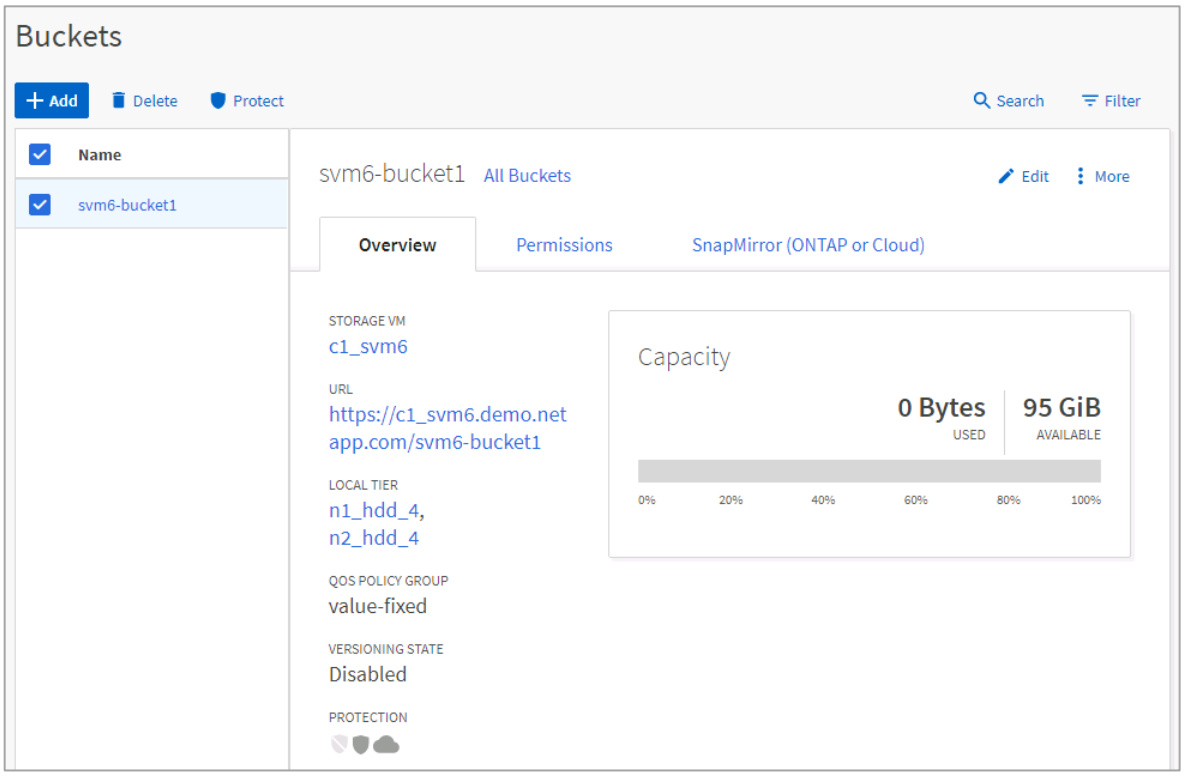
Task 4: Create an S3 Bucket

Step	Action
4-1	From the System Manager menu, select **Storage > Buckets**, and then click **Add**.

Step	Action
4-2	On the Add Bucket page, specify the following settings: • Name: **svm6-bucket1** • Storage VM: **c1_svm6** • Capacity: **95 GiB** 
4-3	Click **More Options**.
4-4	Scroll to the Permissions section and note that the default access permission is to allow all S3 users of this storage system to list the contents of the svm6-bucket1 S3 bucket. 

Step	Action
4-5	Click **Add**. 
4-6	Click the X to remove “All users of this storage VM” from the access permission principal. 
4-7	Click in the Principal field, and then select your S3 user from the list. 

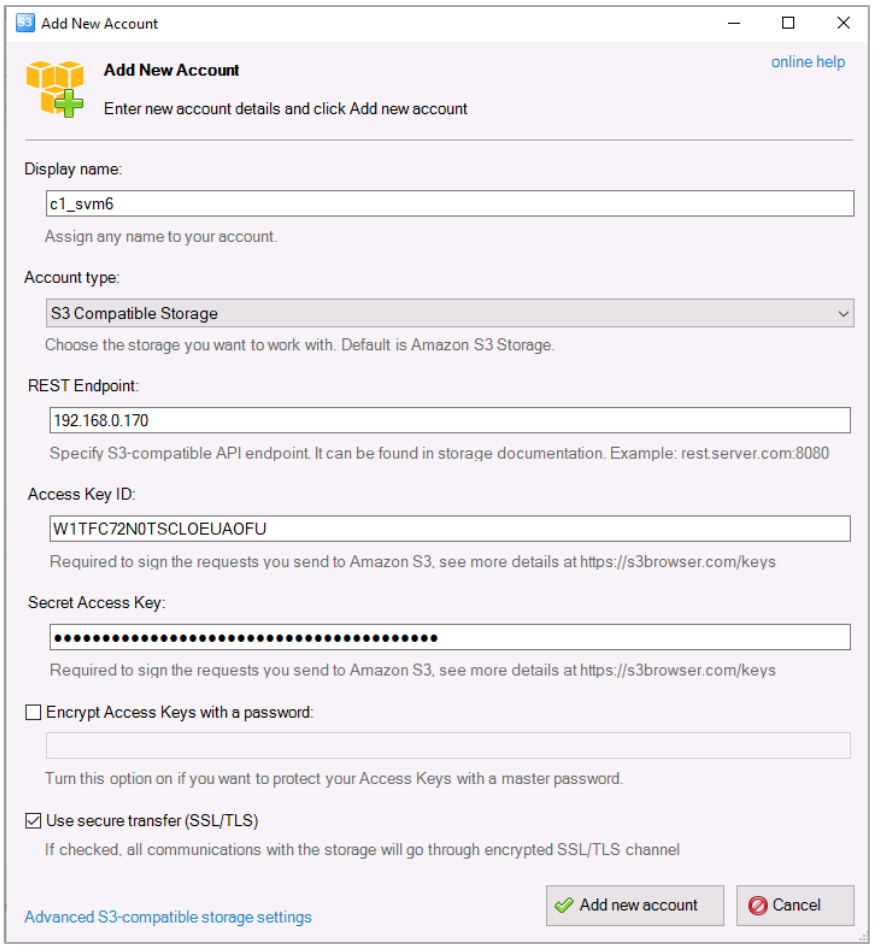
Step	Action
4-8	Click in the **Actions** field, and then select all the checkboxes to allow your S3 user to perform all operations. 
4-9	Click **Save**.
4-10	On the Add Bucket page, click **Save**. 

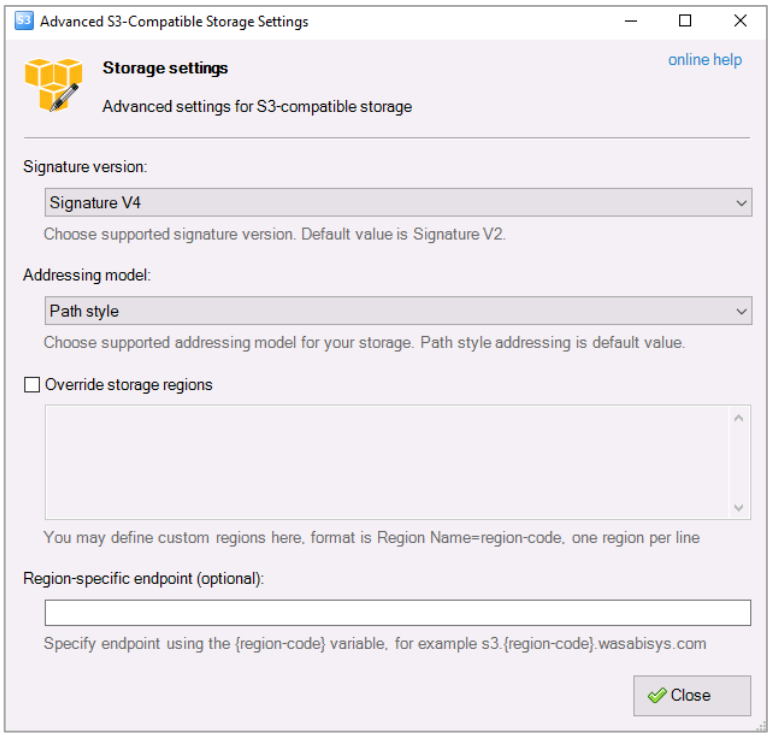
Step	Action
4-11	On the Buckets page, click **svm6-bucket1**, and then note the URL. 

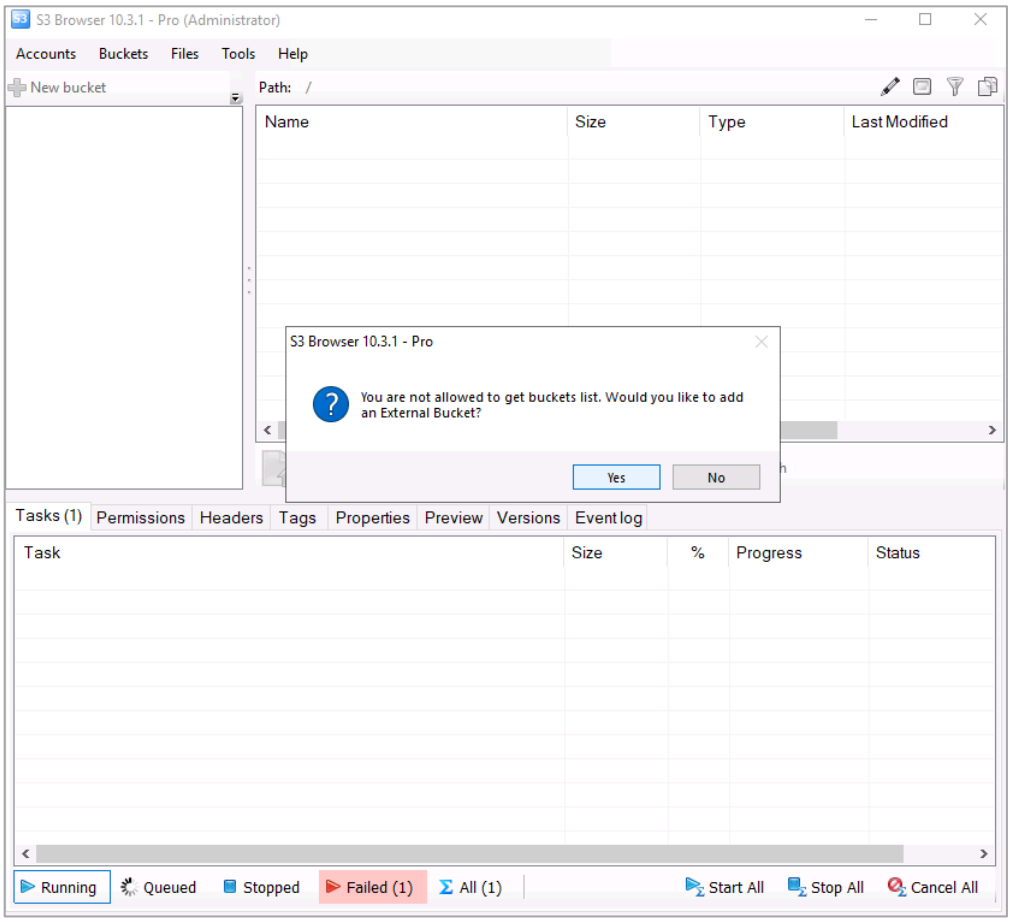
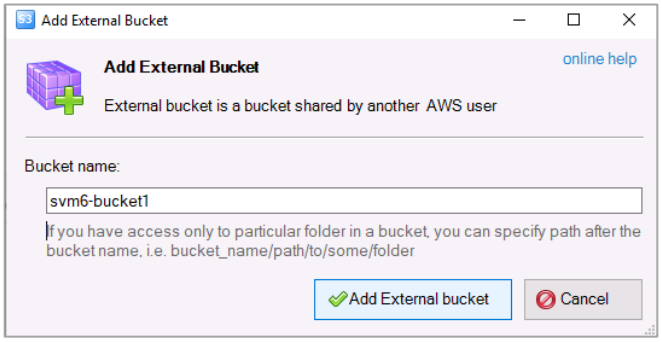
Task 5: Verify Access to the S3 Object Store

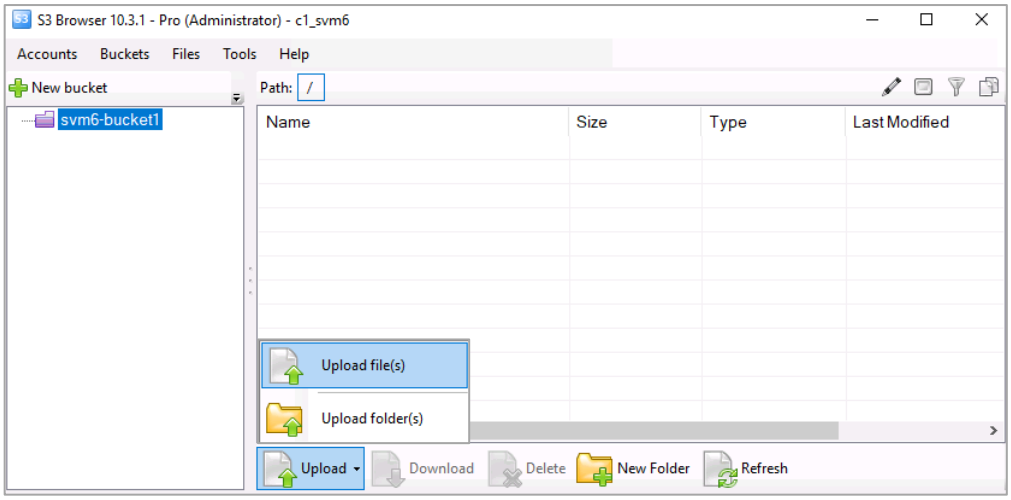
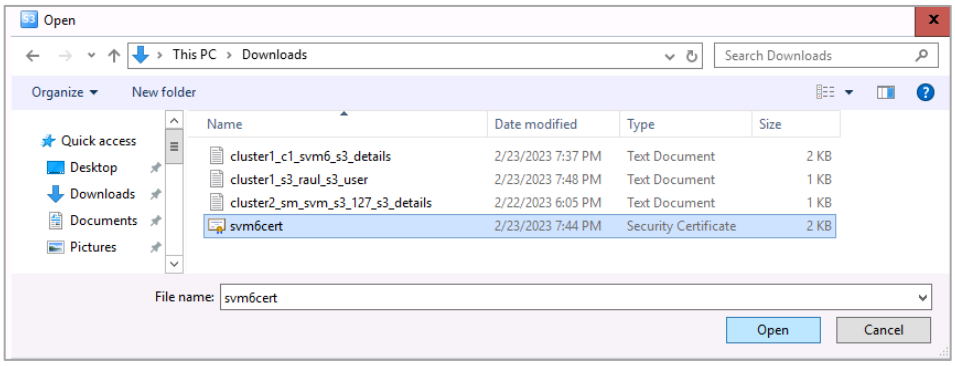
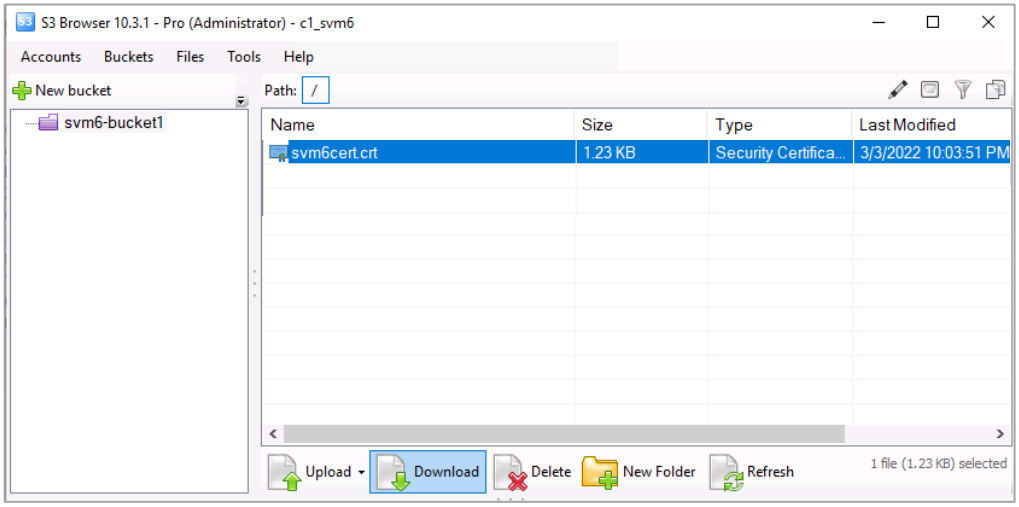
In this task, you use the S3 Browser to connect to the object store served by the ONTAP S3 enabled storage VM.

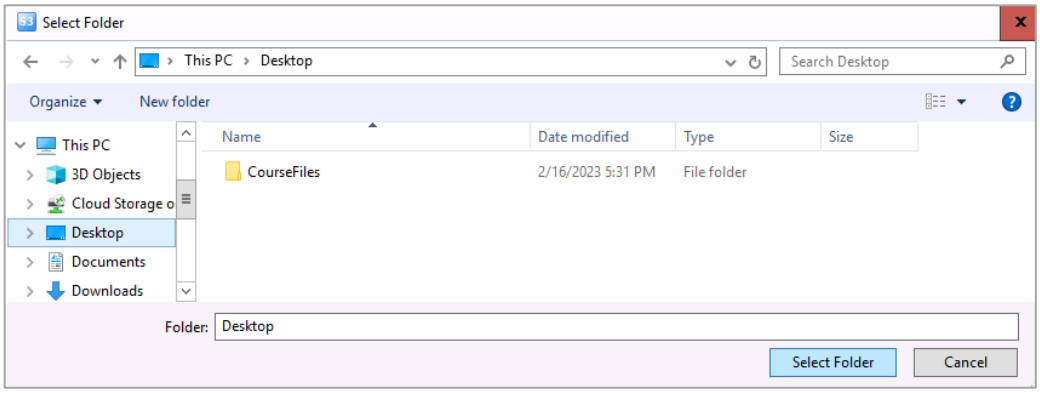
Step	Action
5-1	From the desktop of the Windows jump host, double-click the S3 Browser icon.  The S3 Browser starts on the Add New Account page.

Step	Action
5-2	Specify the parameters for connecting to the ONTAP S3 storage VM: • Display name: **c1_svm6** • Account Type: **S3 Compatible Storage** • REST Endpoint: **192.168.0.170** • Access Key ID: ***<copy the value from your saved file>*** • Secret Access Key: ***<copy the value from your saved file>*** • Encrypt Access Keys with a password: **<not selected>** (default) • Use secure transfer (SSL/TLS): **<selected>** (default) 
5-3	Click **Advanced S3-compatible storage settings**.

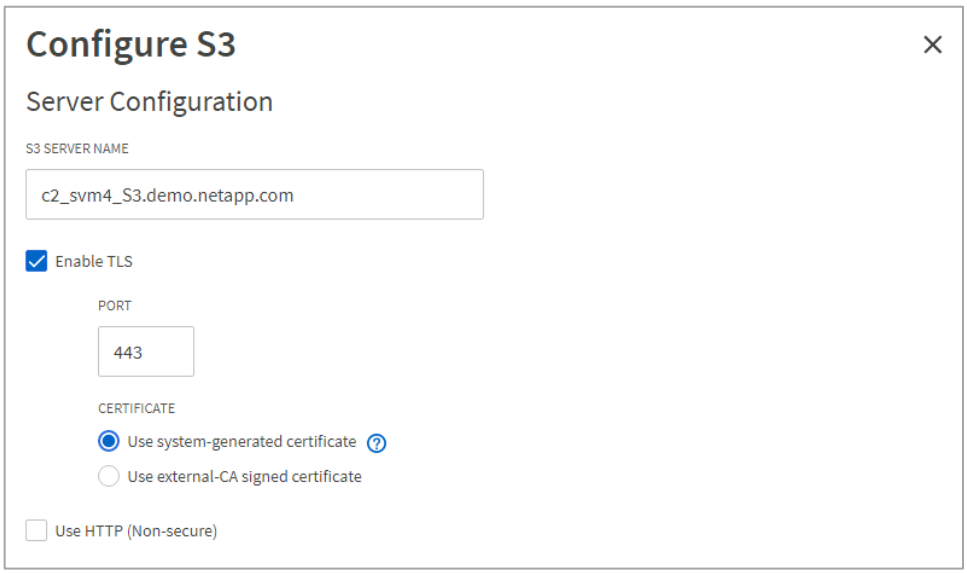
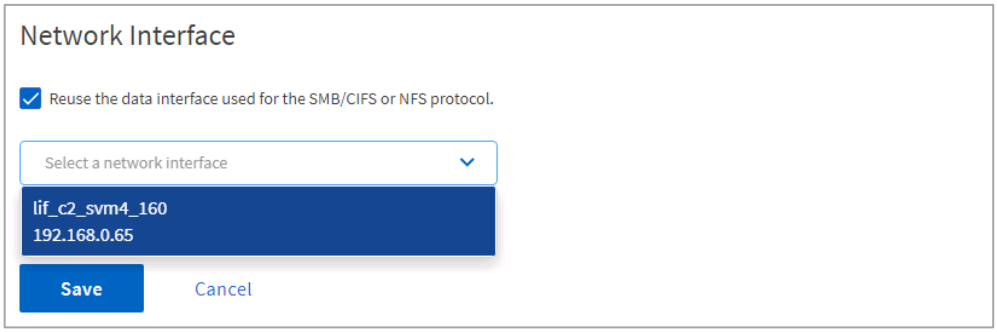
Step	Action
5-4	Specify the parameters for connecting to the ONTAP S3 storage VM: • Signature version: **Signature V4** • Addressing mode: **Path style** (default) • Override storage regions: **<not selected>** (default) • Region-specific endpoint: **<not selected>** (default) 
5-5	Click **Close**.
5-6	Click **Add new account**.

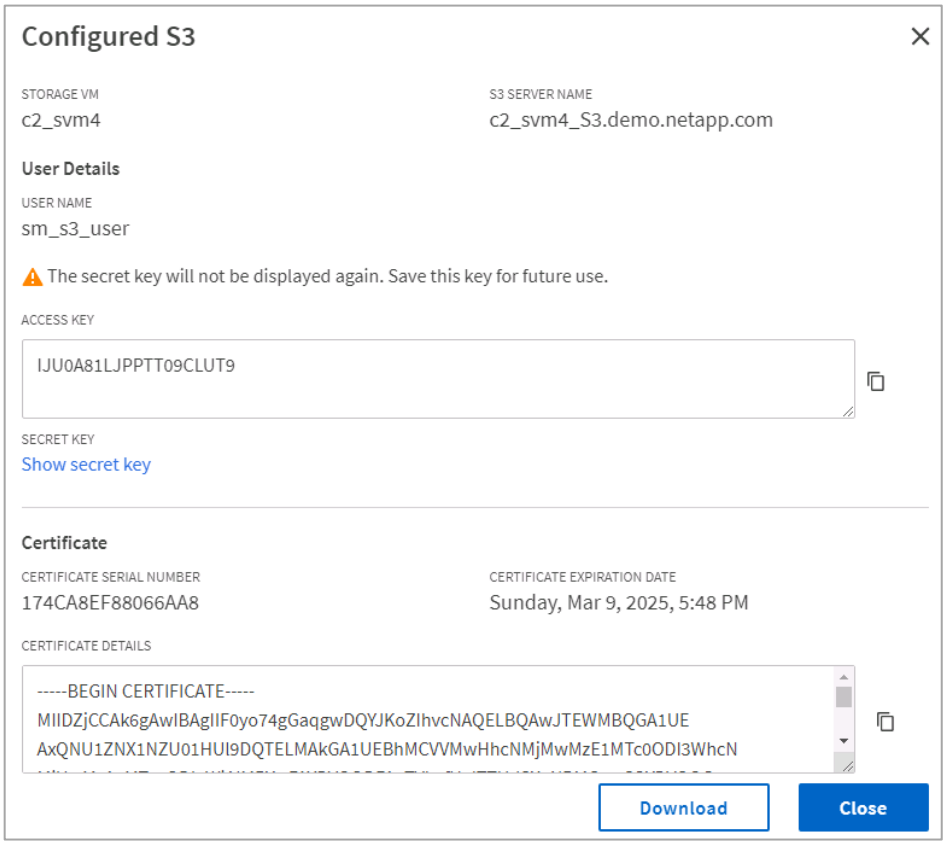
Step	Action
5-7	In the S3 Browser Pro window, click **Yes** to connect to an external bucket. 
5-8	Enter **svm6-bucket1** into the bucket name textbox and click **Add External bucket**. 

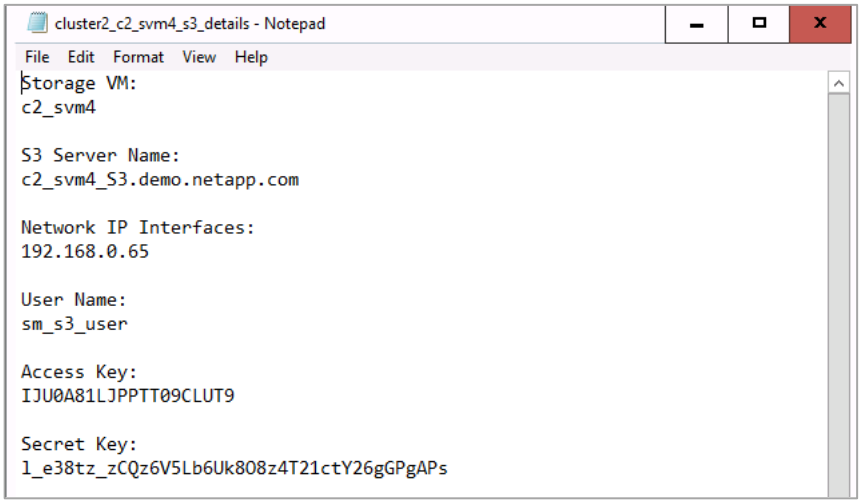
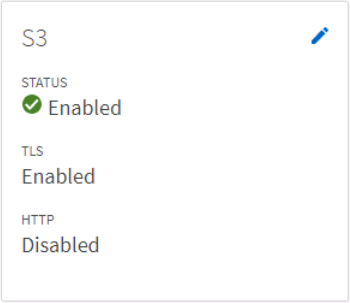
Step	Action
5-9	In the S3 Browser Pro window, with the svm6-bucket1 bucket selected, click **Upload**, then **Upload file(s)**. 
5-10	Select the **svm6cert.crt** file in the Downloads folder and click **Open**. 
5-11	In the S3 Browser Pro window, select the **svm6cert.crt** object in the svm6-bucket bucket and click **Download**. 

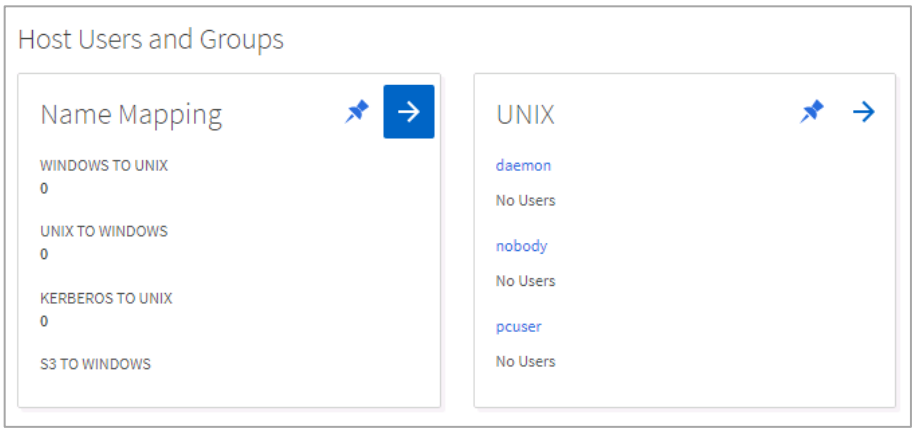
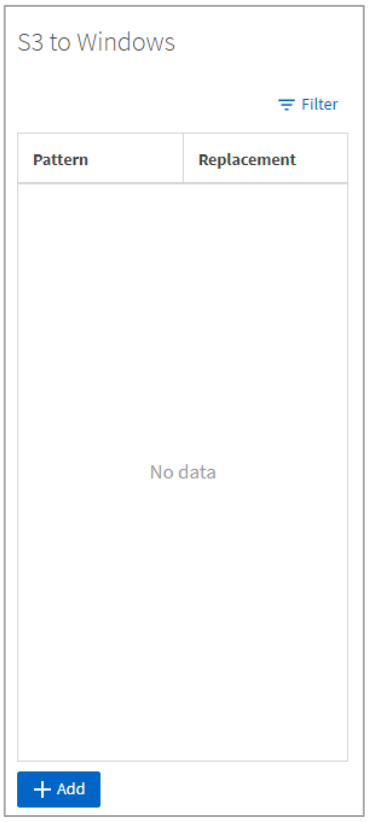
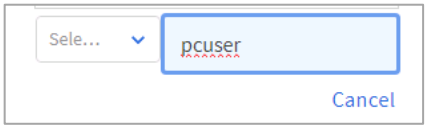
Step	Action
5-12	Save the **svm6cert.crt** object to the Desktop folder on the Windows client host. 

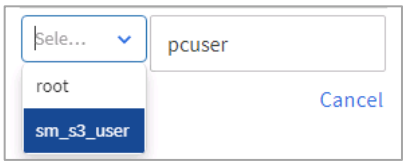
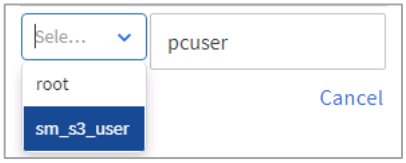
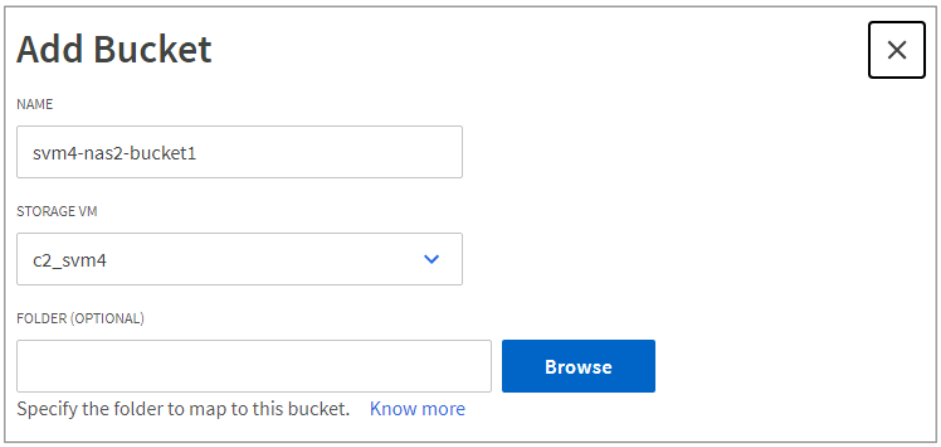
Task 6: Configure S3 Protocol Access to a NAS Share

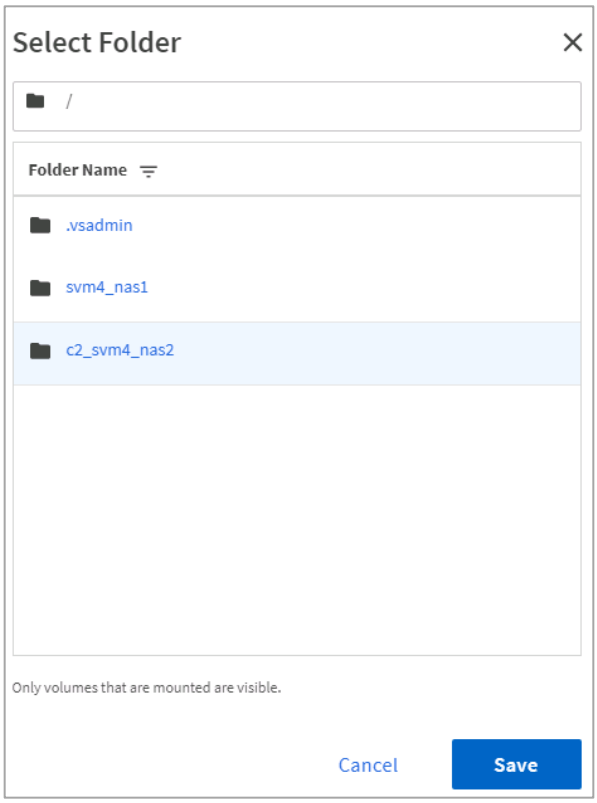
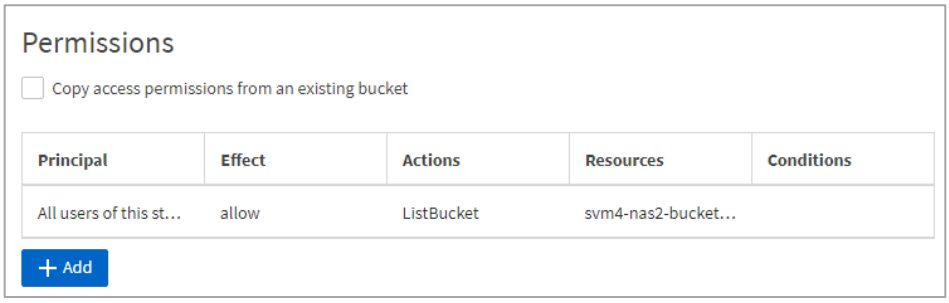
Step	Action
6-1	Return to the ONTAP System Manager session with cluster2.
6-2	From the System Manager menu, select **Storage > Storage VMs**.
6-3	From the list of storage VMs, click **c2_svm4**.
6-4	On the c2_svm4 details page, click the **Settings** tab.
6-5	In the S3 protocol pane, click the gear icon.
6-6	In the Configure S3 page, specify the following settings: • S3 Server Name: **c2_svm4_S3.demo.netapp.com** • Enable TLS: <selected> (default) • Port: **443** (default) • Use system-generated certificate: <selected> (default) 
6-7	In the Network Interface section, select the **Reuse the data interface used for the SMB/CIFS protocol or NFS protocol** checkbox.
6-8	Select the logical network interface that you created in the NFS protocol exercise. 

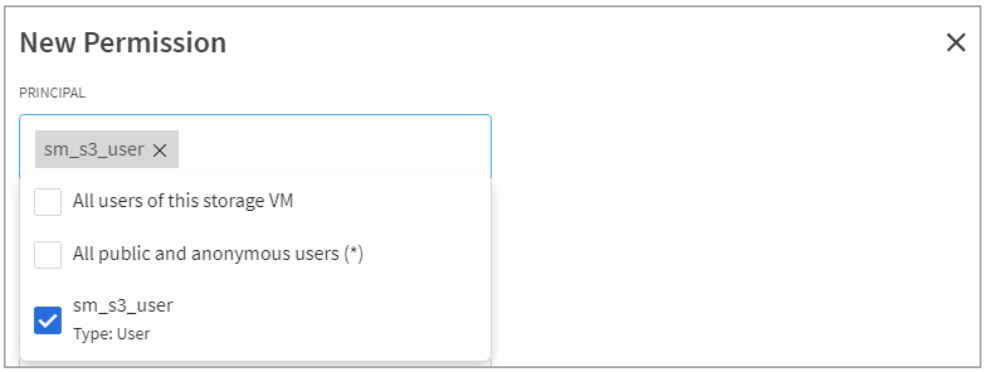
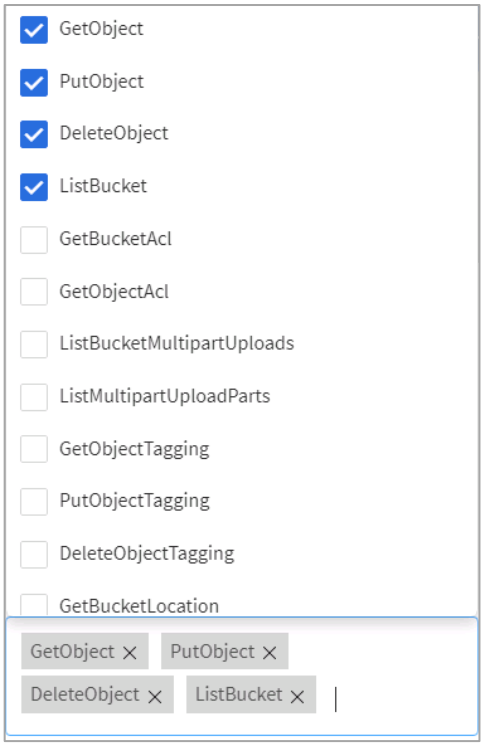
Step	Action
6-9	Review the configuration, and then click **Save**.
6-10	On the Configured S3 page, observe the S3 server information and the name of the automatically created user account. 
6-11	This window is your only opportunity to view and capture the S3 user access keys. If you have not downloaded or otherwise saved the keys and the keys are lost, you must generate new access keys for the user.
6-12	Click **Download**.
6-13	Open the downloaded file.

Step	Action
6-14	Examine the contents of the downloaded file, and identify the following information: • S3 server name • S3 server IP address • S3 user name • S3 user access key • S3 user secret access key 
6-15	Return to System Manager, and then click **Close** to close the Added Storage VM window.
6-16	On the Storage VMs page, click **c2_svm4**, and then click the **Settings** tab.
6-17	Verify that the S3 protocol is enabled. 

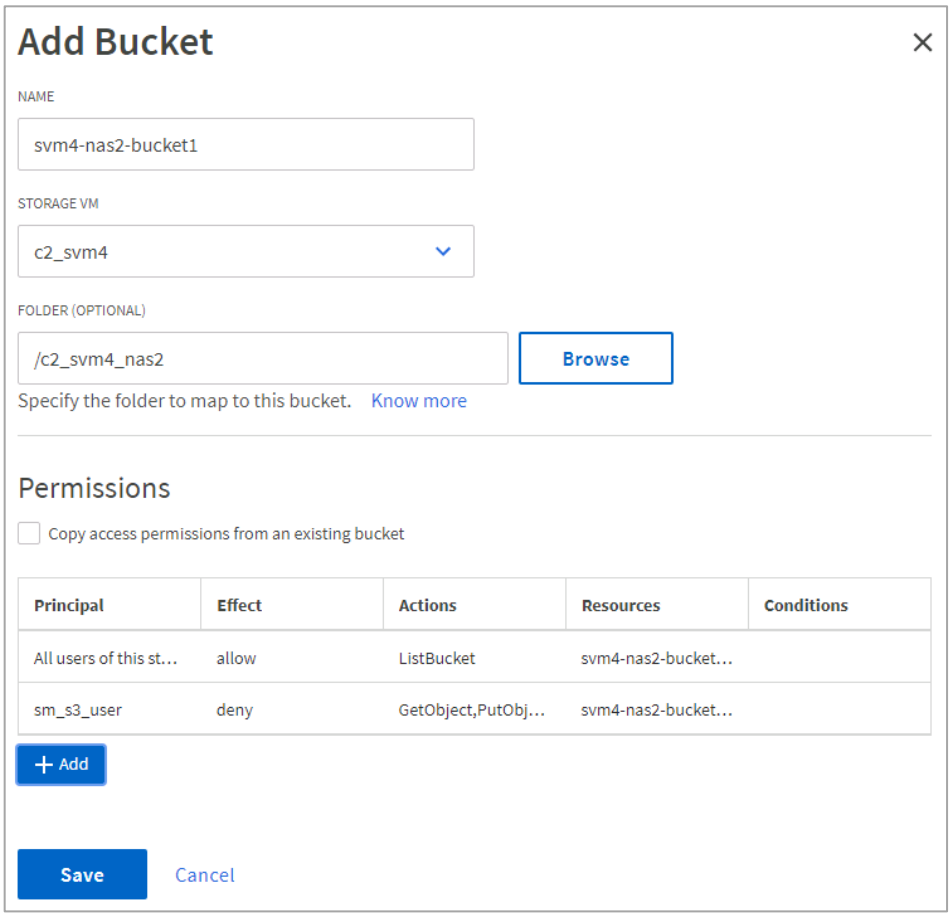
Step	Action
6-18	In the Name Mapping pane, click the right arrow. 
6-19	In the S3 to Windows pane, click **Add**. 
6-20	Enter **pcuser** into the replacement name text box. 

Step	Action
6-21	Select the **sm_s3_user** name for the S3 user name pattern. 
6-22	In the S3 to UNIX pane, click **Add**.
6-23	Enter **pcuser** into the replacement name text box, and select **sm_s3_user** name for the S3 user name pattern. 
6-24	Instead of configuring user mapping, you can configure a default local Windows or UNIX user name that all S3 users map into. You can use the `vserver object-store-server modify` command to configure a default Windows user, a default Unix user, or both. `cluster1::>` **`vserver object-store-server modify -vserver svm1 -default-unix-user pcuser -default-win-user pcuser`**
6-25	From the System Manager menu, select **Storage > Buckets**.
6-26	Click **Add**.
6-27	In the Add Bucket page, specify the following settings: • Name: **svm4-nas2-bucket1** • Storage VM: **c2_svm4** 
6-28	Click **Browse**.

Step	Action
6-29	Select the **c2_svm4_nas2** volume, and click **Save**. 
6-30	In the Permissions section, note that the default access permission is to allow all S3 users of this storage system to list the contents of the NAS bucket. 
6-31	Click **Add**.
6-32	Click the **X** to remove “All users of this storage VM” from the access permission principal. 

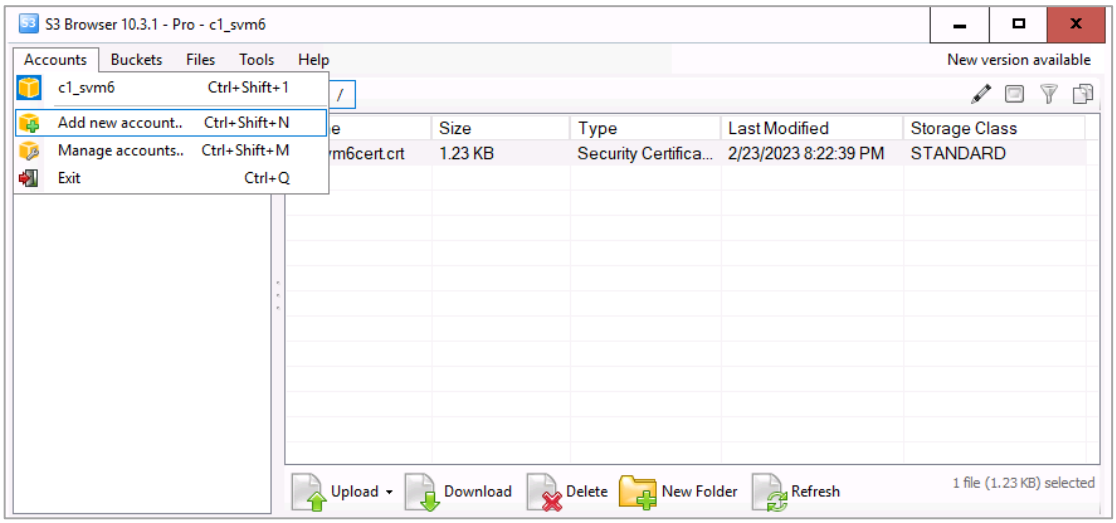
Step	Action
6-33	Click in the Principal field, and then select the **sm_s3_user** S3 user from the list. 
6-34	Click in the **Actions** field, and then select only the following checkboxes: • **GetObject** • **PutObject** • **DeleteObject** • **ListBucket** 
6-35	Click **Save**.

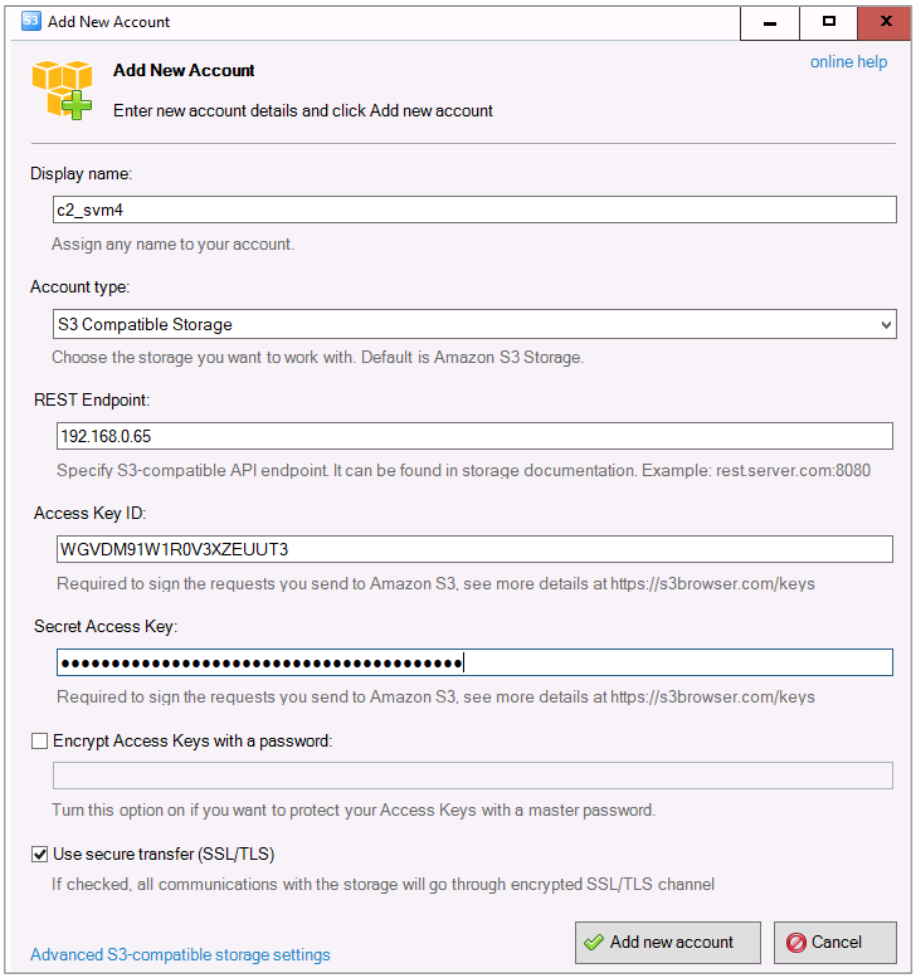
Step	Action
6-36	On the Add Bucket page, click **Save**.

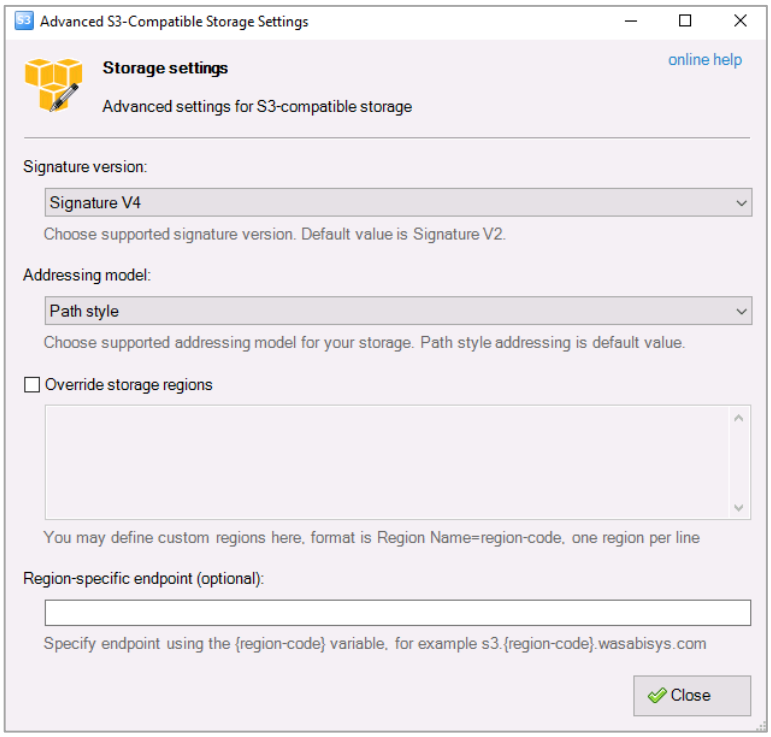
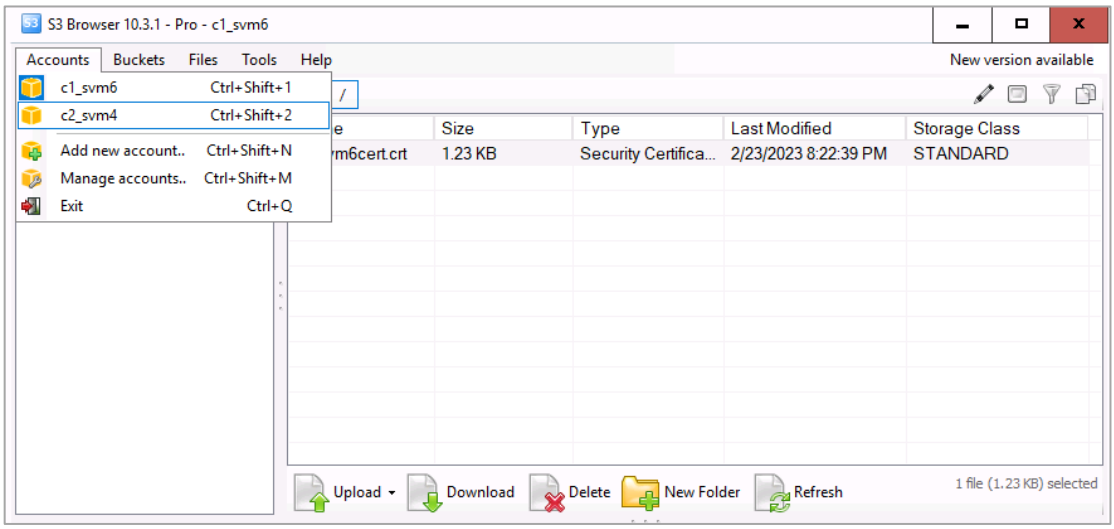


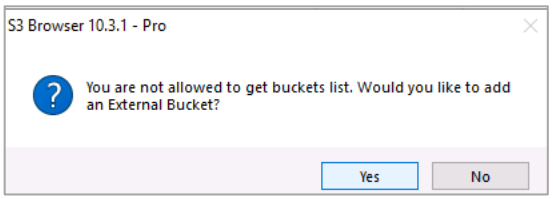
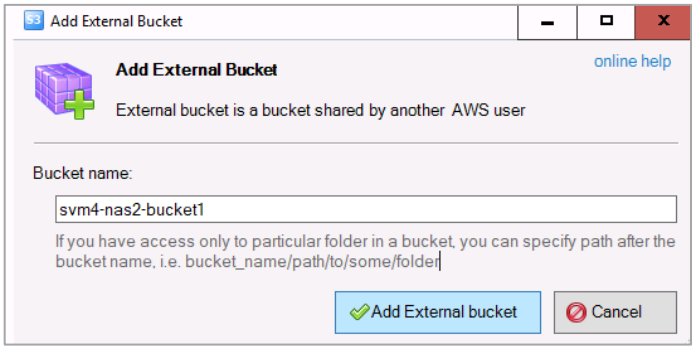
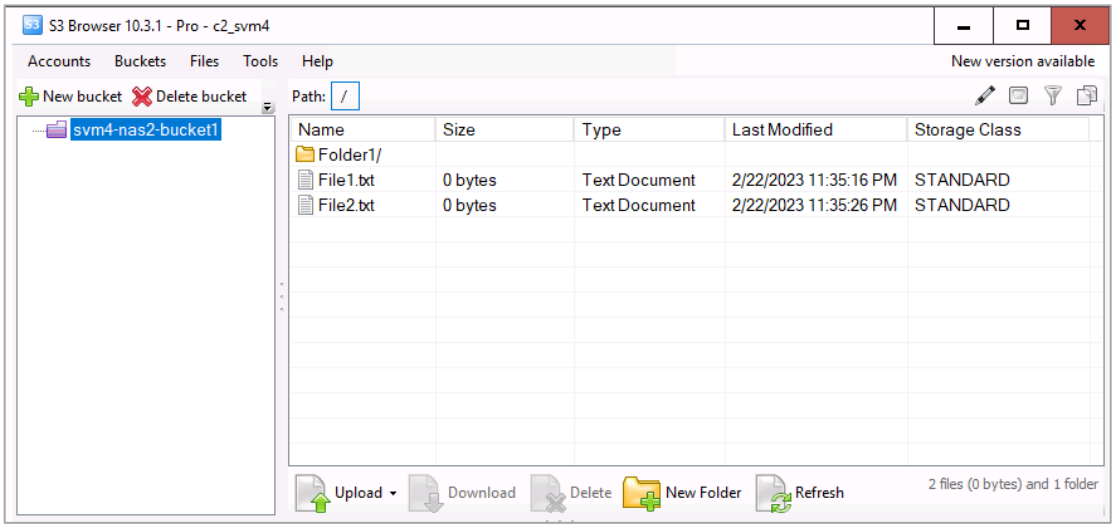
6-37	From the desktop of the Windows jump host, double-click the S3 Browser icon.

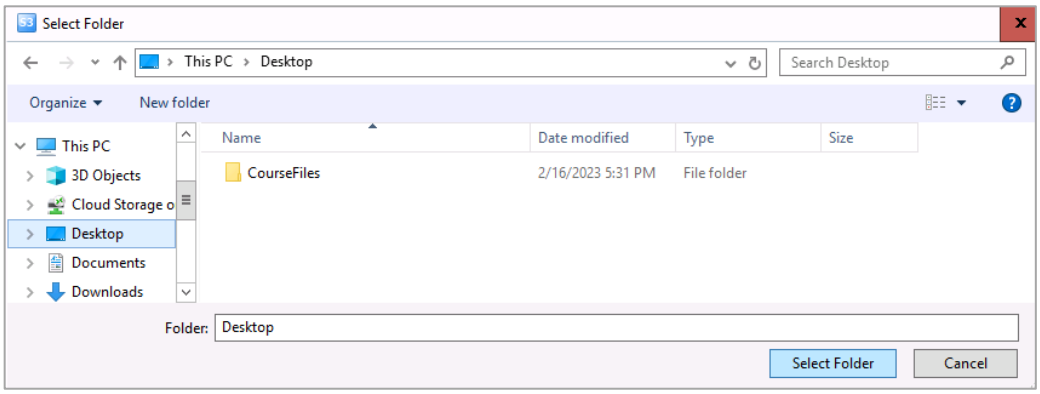
6-38	In the S3 Browser, select **Accounts > Add New Account**.



Step	Action
6-39	Specify the parameters for connecting to the ONTAP S3 storage VM: • Display name: **c2_svm4** • Account type: **S3 Compatible Storage** • REST Endpoint: **192.168.0.65** • Access Key ID: *<copy the value from your saved file>* • Secret Access Key: *<copy the value from your saved file>* • Encrypt Access Keys with a password: <not selected> (default) • Use secure transfer (SSL/TLS): <selected> (default) 
6-40	Click **Advanced S3-compatible storage settings**.

Step	Action
6-41	Specify the parameters for connecting to the ONTAP S3 storage VM: • Signature version: **Signature V4** • Addressing model: **Path style** (default) • Override storage regions: <not selected> (default) • Region-specific endpoint: <not selected> (default) 
6-42	Click **Close**.
6-43	Click **Add new account**.
6-44	In the S3 Browser, select **Accounts > c2_svm4**. 

Step	Action
6-45	In the S3 Browser Pro window, click **Yes** to connect to an external bucket. 
6-46	In the bucket name textbox, enter **svm4-nas2-bucket1**, and click **Add External bucket**. 
6-47	In the S3 Browser window, with the svm4-nas2-bucket1 bucket selected, click **Path: /**. 
6-48	Select a NAS file in the svm4-nas2-bucket1 bucket, and click **Download**.

Step	Action
6-49	Save the NAS file to the Desktop folder on the Windows client host. 

Task 7: Access to the S3 Object Store using the AWS CLI (Optional)

Step	Action
7-1	On the landing host desktop, open a CLI or Windows PowerShell window.
7-2	From the PowerShell CLI, move to the Downloads folder. `PS> cd ~\Downloads`

7-3	Use the **aws** command to create an S3 connection profile. Enter the access key ID and secret access key for the ONTAP S3 user account:
	`aws configure`
	`AWS Access Key ID [None: <access key>`
	`AWS Secret Access Key [None]: <secret key>`
	`Default region name [None]:`
	`Default output format [None]:`
	Sample output:
	`PS C:\Users\Administrator.DEMO\Downloads> aws configure`
	`AWS Access Key ID [None]: W1TFC72N0TSCLOEUAOFU`
	`AWS Secret Access Key [None]: O4h4_8US4IcdP520P0rL2O9cb5DM_zs_uGaTD0r9`
	`Default region name [None]:`
	`Default output format [None]:`

7-4	Copy a file into the svm6-bucket1 bucket in the S3 object store:
	`aws s3 --endpoint-url https://192.168.0.170 --no-verify-ssl cp svm6cert.crt s3://svm6-bucket1/file1`
	Sample output:
	`PS C:\Users\Administrator.DEMO\Downloads> aws s3 --endpoint-url https://192.168.0.170 --no-verify-ssl cp svm6cert.crt s3://svm6-bucket1/file1`
	`urllib3\connectionpool.py:1013: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.0.170'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings`
	`upload: .\svm6cert.crt to s3://svm6-bucket1/file1`

7-5	Copy a second file into the svm6-bucket1 bucket in the S3 object store:
	`aws s3 --endpoint-url https://192.168.0.170 --no-verify-ssl cp svm6cert.crt s3://svm6-bucket1/file2`
	Sample output:
	`PS C:\Users\Administrator.DEMO\Downloads> aws s3 --endpoint-url https://192.168.0.170 --no-verify-ssl cp svm6cert.crt s3://svm6-bucket1/file2`
	< Insecure Request Warning omitted >
	`upload: .\svm6cert.crt to s3://svm6-bucket1/file2`

Step	Action

7-6	Show the objects in the svm6-bucket1 S3 bucket:
	`aws s3 ls s3://svm6-bucket1/ --endpoint-url https://192.168.0.170 --no-verify-ssl`
	Sample output:
	`PS C:\Users\Administrator.DEMO\Downloads>` **`aws s3 ls s3://svm6-bucket1/ --endpoint-url https://192.168.0.170 --no-verify-ssl`**
	< Insecure Request Warning omitted >
	`2023-03-02 22:03:51  1262 svm6cert.crt`
	`2023-03-02 22:16:24  1264 file1`
	`2023-03-02 22:17:05  1264 file2`

7-7	Retrieve an object from the svm6-bucket1 bucket and place the object into a local folder: **`aws s3 cp s3://svm6-bucket1/file1 C:\CourseFiles\S3_file1 --endpoint-url https://192.168.0.170 --no-verify-ssl`** Sample output: `PS C:\Users\Administrator.DEMO\Downloads>` **`aws s3 cp s3://svm6-bucket1/file1 C:\CourseFiles\S3_file1 --endpoint-url https://192.168.0.170 --no-verify-ssl`** *< Insecure Request Warning omitted >* `download: s3://svm6-bucket1/file1 to ..\..\..\CourseFiles\S3_file1`

7-8	Examine the retrieved object file:
	`ls C:\CourseFiles\S3_file1`
	Sample output:
	`PS C:\Users\Administrator.DEMO\Downloads>` **`ls C:\CourseFiles\S3_file1`**
	`Directory: C:\CourseFiles`
	`Mode  LastWriteTime  Length Name`
	`----  ----------  ------ ----`
	`-a----  3/2/2023  10:16 PM  1264 S3_file1`

7-9	Close the Windows PowerShell window.

End of exercise