



ORACLE



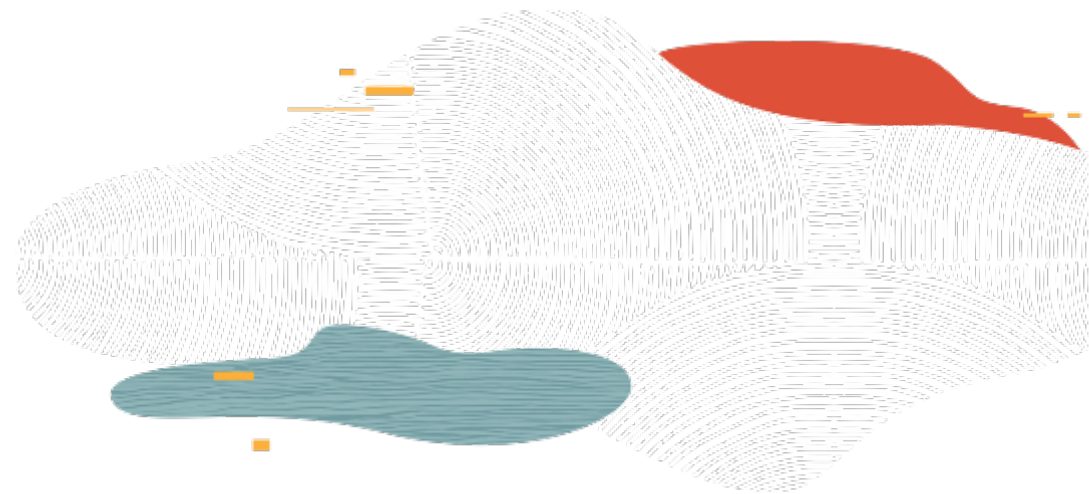
File Storage Service

L100

Rohit Rahi

Oracle Cloud Infrastructure

October, 2019

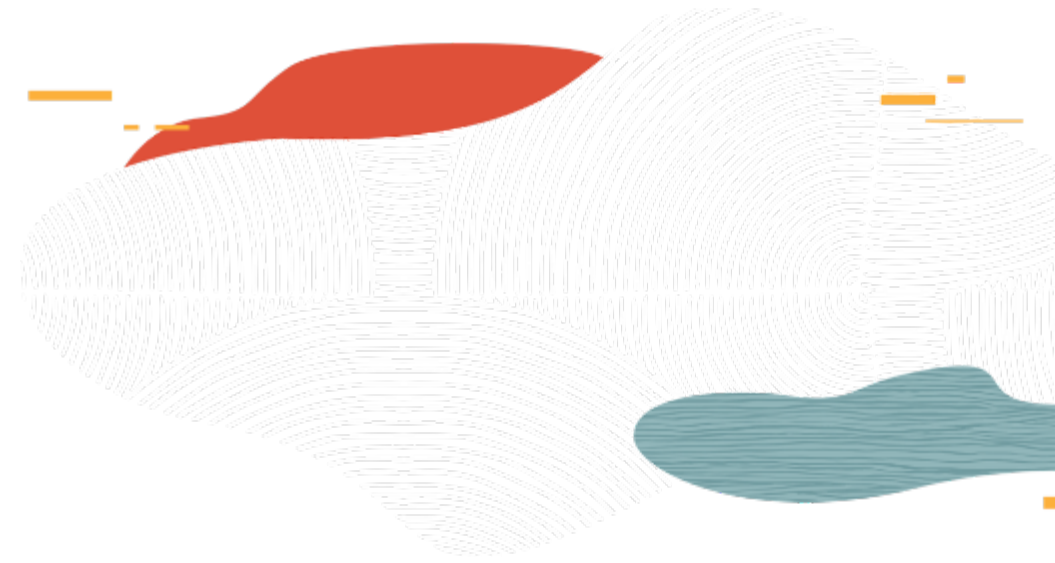


Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

ORACLE

File Storage Service Intro



OCI Storage Services

	Local NVMe	Block Volume	File Storage	Object Storage	Archive Storage
Type	NVMe SSD based temporary storage	NVMe SSD based block storage	NFSv3 compatible file system	Highly durable Object storage	Long-term archival and backup
Durability	Non-persistent; survives reboots	Durable (multiple copies in an AD)	Durable (multiple copies in an AD)	Highly durable (multiple copies across ADs)	Highly durable (multiple copies across ADs)
Capacity	Terabytes+	Petabytes+	Exabytes+	Petabytes+	Petabytes+
Unit Size	51.2 TB for BM, 6.4-25.6 TB for VM	50 GB to 32 TB/vol 32 vols/instance	Up to 8 Exabyte	10 TB/object	10 TB/object
Use cases	Big Data, OLTP, high performance workloads	Apps that require SAN like features (Oracle DB, VMW, Exchange)	Apps that require shared file system (EBS, HPC)	Unstructured data incl. logs, images, videos	Long term archival and backups (Oracle DB backups)

File Storage Service – use cases



Oracle Applications
Lift and Shift



General Purpose
File Systems



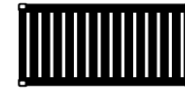
Big Data &
Analytics



HPC
Scale Out Apps



Test / Dev
Databases

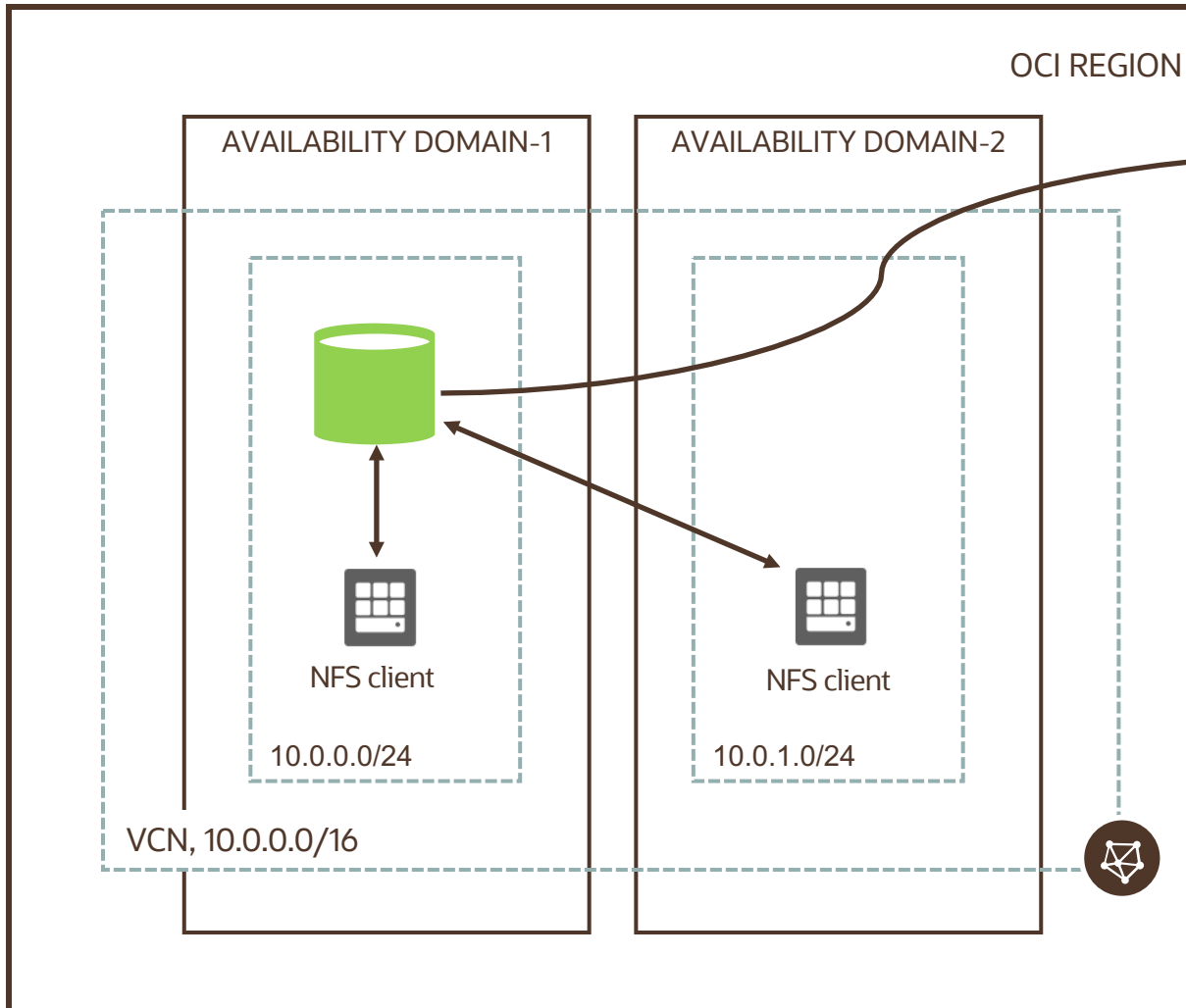


MicroServices
Containers

File Storage service Features

- AD-local service, available in all OCI regions and Availability Domains
- Supports NFS v.3
- Network Lock Management (NLM) for file locking
- Full POSIX semantics
- Data Protection: Snapshots capabilities; 10,000 snapshots per file system
- Security: 128-bit, data-at-rest encryption for all file systems & metadata
- Console management, APIs, CLI, data-path commands, and Terraform
- Create 100 file systems and 2 mount targets per AD per account

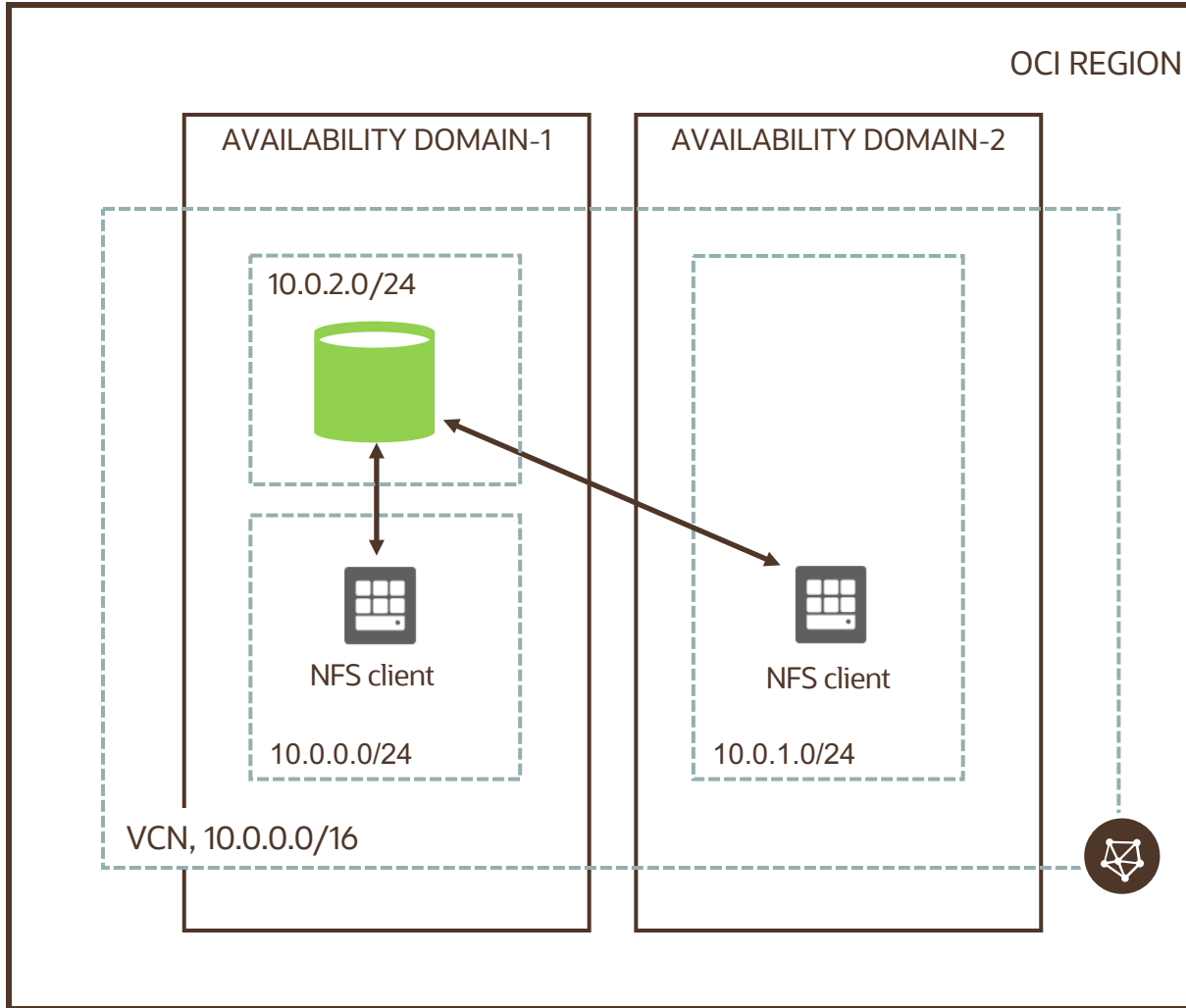
Mount Target



Mount Target

- NFS endpoint that lives in your subnet of choice; AD-specific
- Mount target has an IP address and DNS name that you can use in your mount command. E.g. 10.0.0.6
- Requires three private IP addresses in the subnet (don't use /30 or smaller subnets for the FSS)
- Two of the IP addresses are used during mount target creation; 3rd IP used for HA

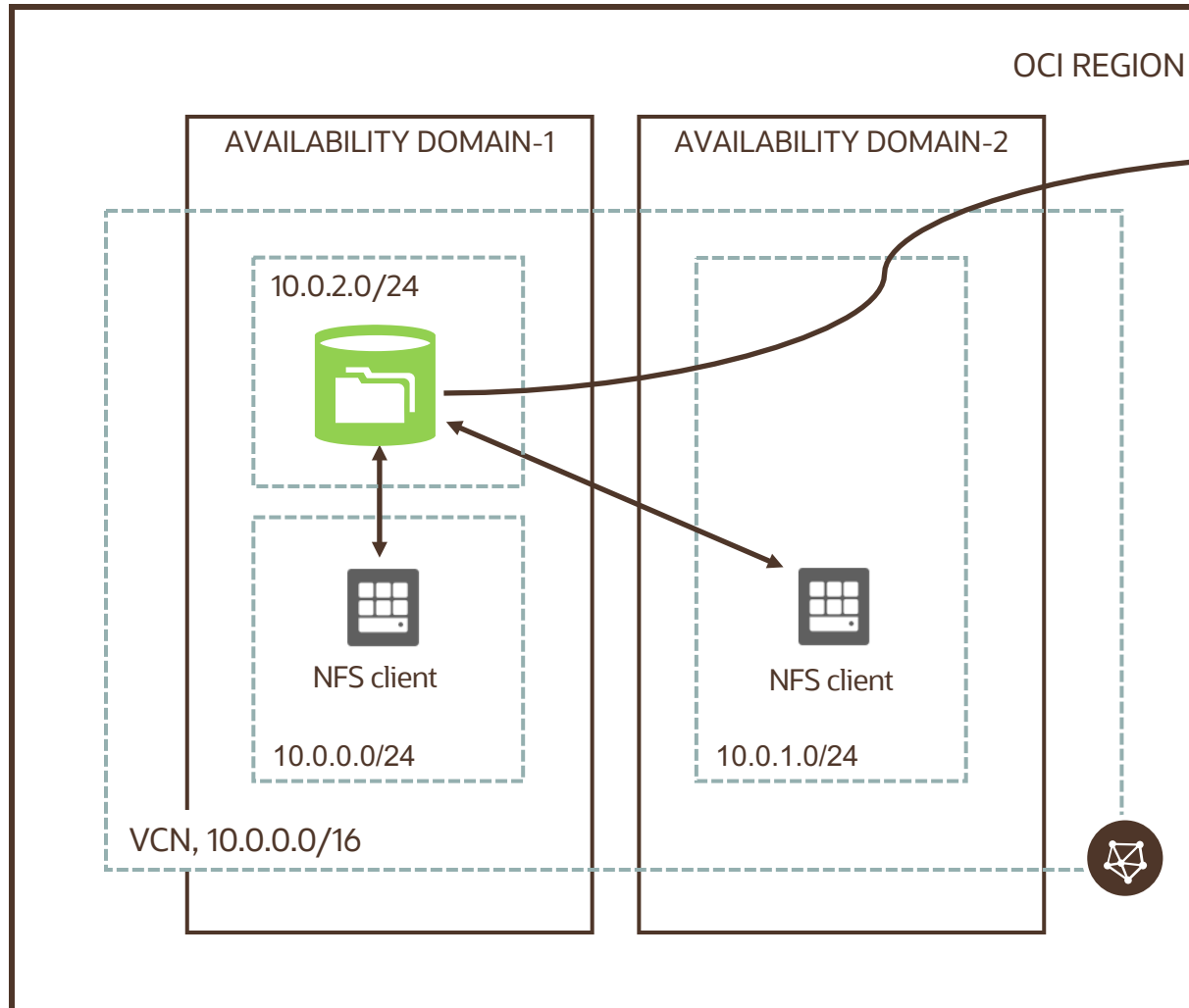
Mount Target



Mount Target

- Placing NFS clients and mount target in the same subnet can result in IP conflicts, as users are not shown which private IPs are used for mount target
- Place FSS mount target in its own subnet, where it can consume IPs as it needs

File System



File System

- Primary resources for storing files in FSS
- To access your file systems, you create a new (or use an existing) mount target
- 100 File Systems per Mount Target
- AD-specific
- Accessible from OCI VM/BM instances
- Accessible from on-premises through FastConnect/VPN

FSS Paths

- Export Path: unique path specified when the file system is associated with a mount target during creation
- No two File systems associated with the same mount target can have overlapping export paths (e.g. FS paths like /example and /example/path are not allowed)



Mount target (NFS endpoint): 10.0.0.6

Export Path1: /example1/path

Export Path1 2: /example2/path

- Export path, along with the mount target IP address, is used to mount the file system to an instance
 - `sudo mount 10.0.0.6:/example1/path /mnt/mountpointA`
 - `sudo mount 10.0.0.6:/example2/path /mnt/mountpointB`
 - /mnt/mountpointA and /mnt/mountpointB are path to the directory on the NFS client instance on which the external file systems are mounted

Mounting an OCI File System

- Launch OCI instance from console
- Use NFSv3 protocol to mount the FSS volume
- Install nfs-utils (Oracle Linux and CentOS) or nfs-common (Ubuntu) in your Linux system
- Create a directory
- On the FSS console, click on Mount Targets
- Use the Private IP address information to mount the volume using nfs command:

```
opc@node01:~$ sudo mkdir -p /<user's target directory>
```

```
opc@node01:~$ sudo mount <IPaddress>:<path-name>  
/<user's target directory>
```

```
opc@node01:~$ sudo yum install nfs-utils
```

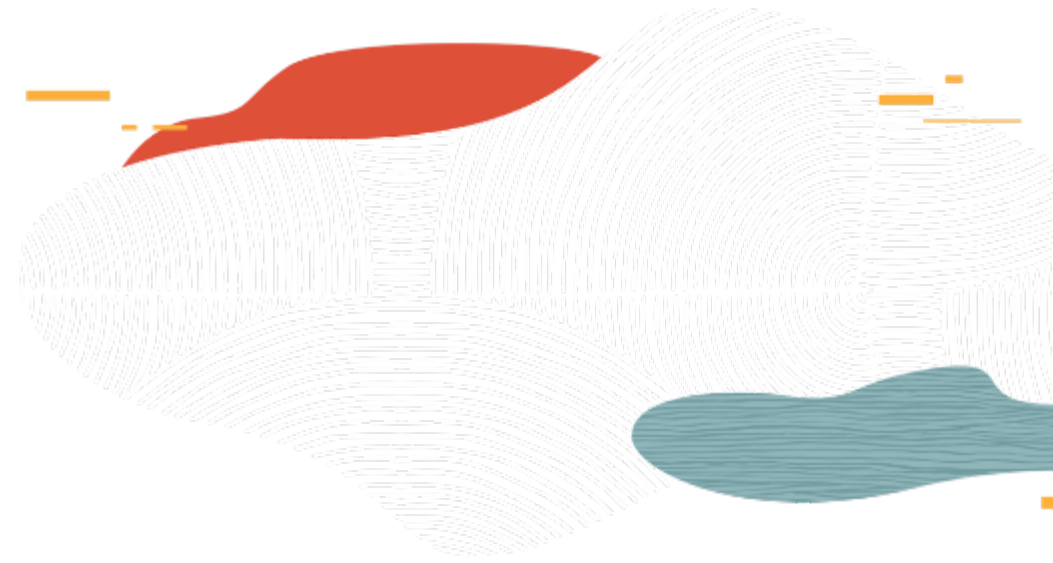
```
opc@node01:~$ sudo mkdir -p /mnt/nfs
```

```
opc@node01:~$ sudo mount 10.0.0.3:/fss-shared  
/mnt/nfs
```

NOTE: We recommend not to pass mount options to achieve best performance with File Storage Service. This approach leaves it to the client and server to negotiate the window size for Read & Write operations.

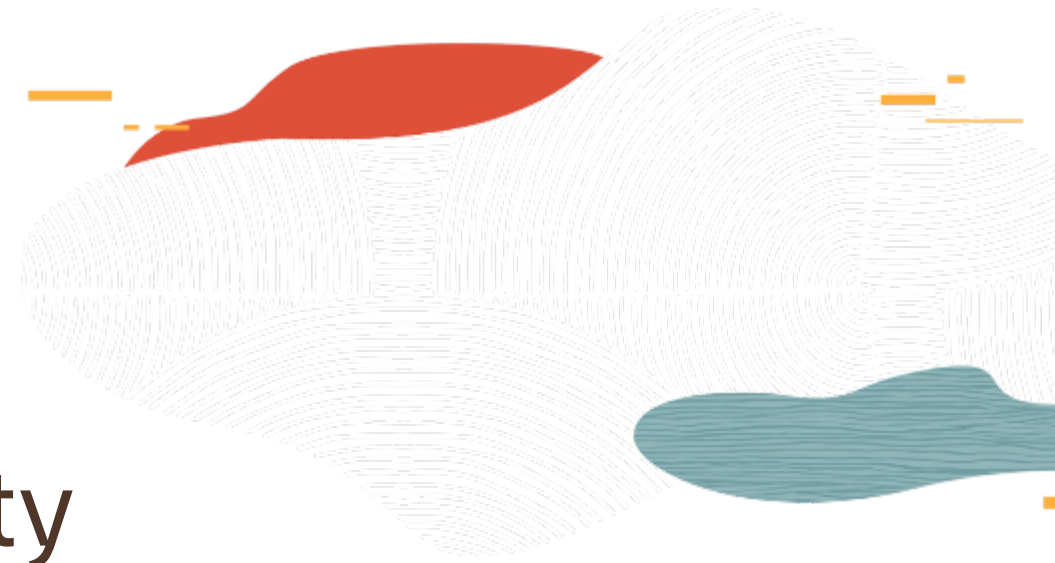
ORACLE

File Storage Service Demo



ORACLE

File Storage Service Security



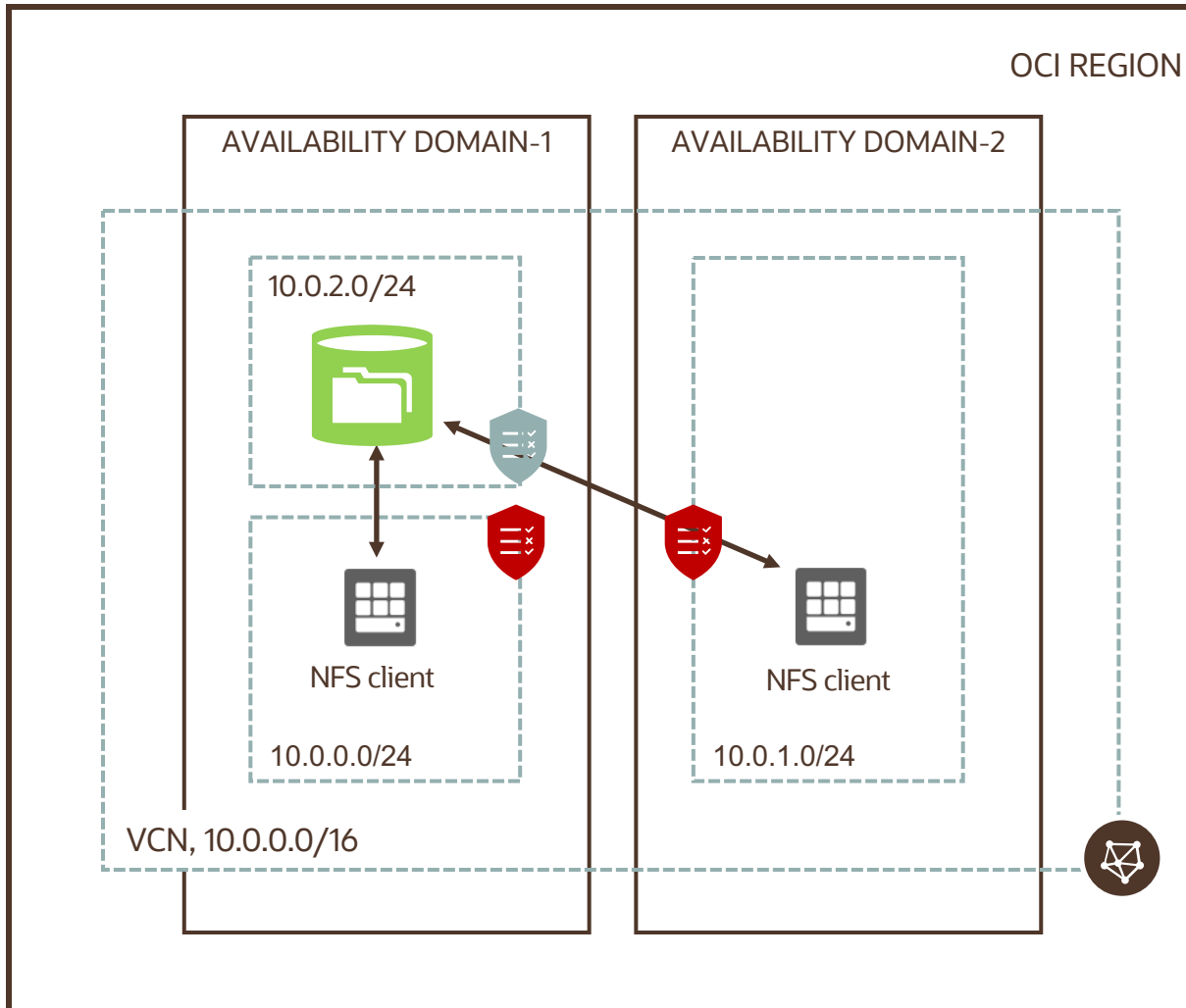
Security

Four distinct and separate layers of security with its own authorization entities and methods to consider when using FSS

Security layer	Uses these..	To control actions like these..
IAM Service	OCI users, policies	Creating instances (NFS clients) and FSS VCNs. Creating, listing, and associating file systems and mount targets
Security Lists	CIDR blocks	Connecting the NFS client instance to the mount target
Export Options	Export options, CIDR blocks	Applying access control per-file system based on source IP CIDR blocks that bridges the Security Lists layer and the NFS v.3 Unix Security layer
NFS v3. Unix Security	Unix users	Mounting file systems ¹ , reading the writing files, file access security

¹When mounting file systems, don't use mount options such as nolock, rsize, or wsize. These options cause issues with performance and file locking

Security Lists



Security List can be used as a virtual firewall to prevent NFS clients from mounting an FSS mount target (even in the same subnet). FSS needs -

- Stateful ingress TCP ports 111, 2048 – 2050
- Stateful ingress UDP ports 111 and 2048
- Opening these ports enables traffic from Solaris, Linux, and Windows NFS clients

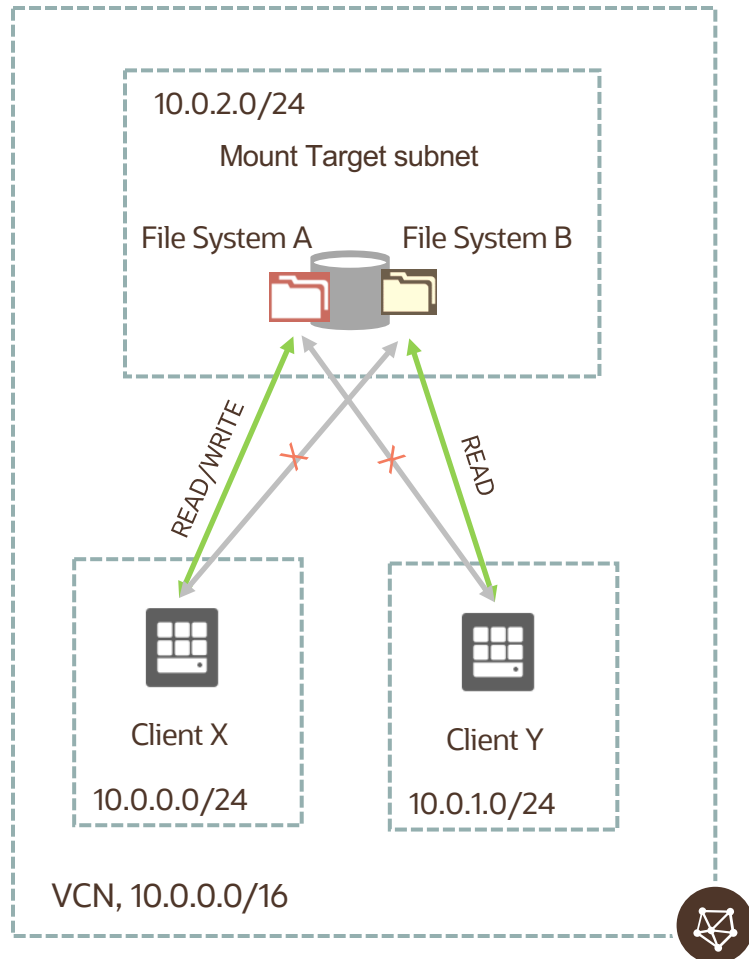
Type	Source CIDR	Protocol	Source Port	Dest Port
Ingress	10.0.0.0/24 ¹	TCP	All	2048-2050
Ingress	10.0.0.0/24	TCP	All	111
Ingress	10.0.0.0/24	UDP	All	2048
Ingress	10.0.0.0/24	UDP	All	111

¹ For all subnets within VCN (e.g. 10.0.1.0/24) to access File System, change destination CIDR to 10.0.0.0/16; all rules stateful

Export Option

- Security List is all or nothing approach – the client either can or cannot access the mount target, and therefore all file systems associated with it
- In a multi-tenant environment, using NFS export option, you can limit clients' ability to connect to the file system and view or write data
- Export controls how NFS clients access file systems; info stored in an export includes the file system OCID, export path, and client access options
- When you create file system and associated mount target, the NFS export options for that file system are set to allow full access for all NFS clients :
 - Source: 0.0.0.0/0 (All)
 - Require Privileged Source Port: False
 - Access: Read_Write
 - Identity Squash: None

Export Option



- Client X, assigned to 10.0.0.0/24, requires Read/Write access to file system A, but not file system B
- Client Y, assigned to 10.0.1.0/24, requires Read access to file system B, but no access to file system A
- Both file systems A and B are associated to a single mount target

```
oci fs export update --export-id <FS_A_export_ID> --export-options '[{"source":"10.0.0.0/24","require-privileged-source-port":"true","access":"READ_WRITE","identity-squash":"NONE","anonymous-uid":"65534","anonymous-gid":"65534"}]'
```

```
oci fs export update --export-id <FS_B_export_ID> --export-options '[{"source":"10.0.1.0/24","require-privileged-source-port":"true","access":"READ_ONLY","identity-squash":"NONE","anonymous-uid":"65534","anonymous-gid":"65534"}]'
```

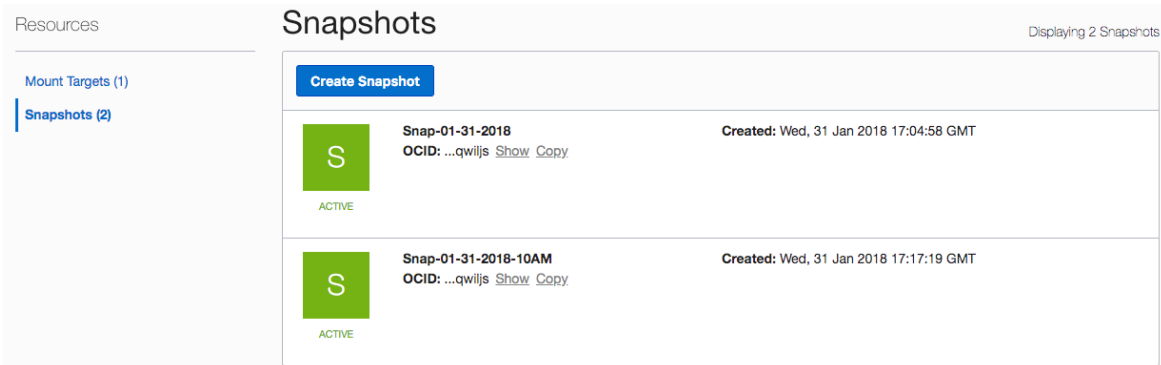


ORACLE

File Storage Service Snapshots

File Storage Service Snapshot

- Snapshots provide a read-only, space efficient, point-in-time backup of a file system
- Snapshots are created under the root folder of file system, in a hidden directory named `.snapshot`
- You can take up to 10,000 snapshots per file system
- You can restore a file within the snapshot, or an entire snapshot using the `cp` or `rsync` command –
`cp -r .snapshot/snapshot_name/* destination_directory_name`
- If nothing has changed within the target file system and you take a snapshot, it does not consume any additional storage





Resources Snapshots Displaying 2 Snapshots

[Mount Targets \(1\)](#)

[Snapshots \(2\)](#)

[Create Snapshot](#)

	Snap-01-31-2018 OCID: ...qwijls Show Copy	Created: Wed, 31 Jan 2018 17:04:58 GMT
	Snap-01-31-2018-10AM OCID: ...qwijls Show Copy	Created: Wed, 31 Jan 2018 17:17:19 GMT

```
[opc@node01 fs-shared]$ cd .snapshot/
[opc@node01 .snapshot]$ ls -la
total 4
drwxr-xr-x. 8 root root 6 Jan  4 21:58 .
drwxr-xr-x. 7 root root 6 Jan  4 21:58 ..
drwxr-xr-x. 4 opc  opc  4 Dec 14 20:00 snapshot-dec14
drwxr-xr-x. 5 opc  opc  5 Dec 14 20:06 snapshot-dec14-2PM
drwxr-xr-x. 8 opc  opc  8 Dec 18 19:23 snapshot-dec18
drwxr-xr-x. 7 root root 6 Dec 19 21:02 snapshot-dec19
drwxr-xr-x. 7 root root 6 Dec 20 16:45 snapshot-dec20
drwxr-xr-x. 9 root root 8 Dec 20 14:44 snapshot-test
[opc@node01 .snapshot]$
```

Summary

- OCI File Storage Service provides a fully managed, elastic, durable, distributed, enterprise-grade network file system
- FSS supports NFS v3, snapshots and default data-at-rest encryption
- FSS is highly scalable (Exabytes) and performant
- FSS supports four distinct and separate layers of security with its own authorization entities and methods

Oracle Cloud always free tier:

oracle.com/cloud/free/

OCI training and certification:

<https://www.oracle.com/cloud/iaas/training/>

<https://www.oracle.com/cloud/iaas/training/certification.html>

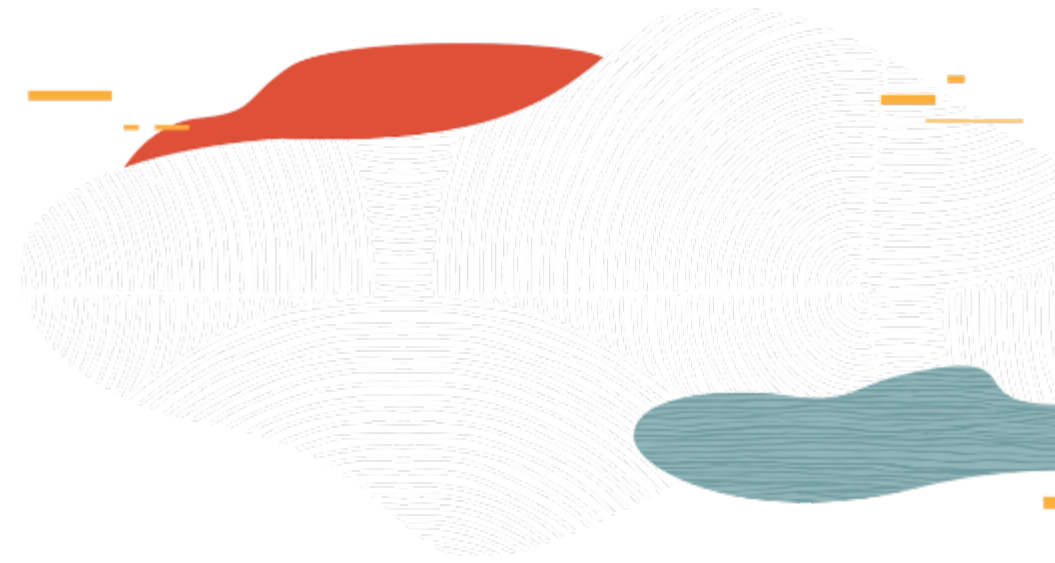
education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:

ocitraining.qcloudable.com/provider/oracle

Oracle learning library videos on YouTube:

youtube.com/user/OracleLearning



Thank you

