SAOUG
CONFERENCE 2025

PURESTORAGE®

Guardians of the Data Protecting Oracle databases and backups from Ransomware and Malicious Intent

HELLO
AFRICA

Ron Ekins

Director, Field Solutions Architecture
EMEA & LATAM

Outsurance In the House Party

Oracle ACE Director

Ron Ekins
Director Field Solution Architecture, EMEA & LATAM

- **Email: ron@purestorage.com**
- **X: @RonEkins**
- **BlueSky: @ronekins.com**
- **Blog: https://ronekins.com**
- **GitHub: https://github.com/raekins**

ORACLE | Partner

Oracle ACE Director

PURESTORAGE®

Positioned Highest in Execution, Furthest in Vision

2025 Gartner® Magic Quadrant™ for Enterprise Storage Platforms

Figure 1: Magic Quadrant for Enterprise Storage Platforms

Gartner

Oracle ACE

The Oracle ACE Program

600+ technical experts helping peers globally

- The Oracle ACE Program recognizes and rewards community members for their technical and community contributions to the Oracle community
- 3 membership levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com

aceprogram_ww@oracle.com Facebook.com/OracleACEs @oracleace Oracle ACE Program Group

Oracle ACE

ACE Member Benefits

Key Benefits

Cool **swag***, Digital awards for social media, Oracle **CloudWorld pass***, & more

Direct Access to Product Management

Multiple **direct communication channels** to product management and fellow ACEs

Exclusive Content

Exclusive **monthly virtual meetings** with product development teams + engaging guest speakers

Networking

In-person & virtual networking opportunities for ACEs to **connect with product development** and each other.

Cloud Account

$5k USD Cloud account*

Travel Support

ACE Directors are eligible for travel support to give presentations or lead workshops at conferences globally

* for Pro and Director levels

Agenda

What are malware and ransomware

Think Defence-in-Depth

Protection from ransomware and malicious intent

What else ?

PURESTORAGE®

What are Malware and Ransomware ?

What is malware ?

- **Malware** is malicious software, which - if able to run - can cause harm in many ways, including:
- causing a device to become locked or unusable
- stealing, deleting or encrypting data
- taking control of your devices to attack other organisations
- obtaining credentials which allow access to your organisation's systems or services that you use
- using services that may cost you money (e.g. premium rate phone calls).
- 'mining' cryptocurrency

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

National Cyber Security Centre

What is ransomware?

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it).

The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware.

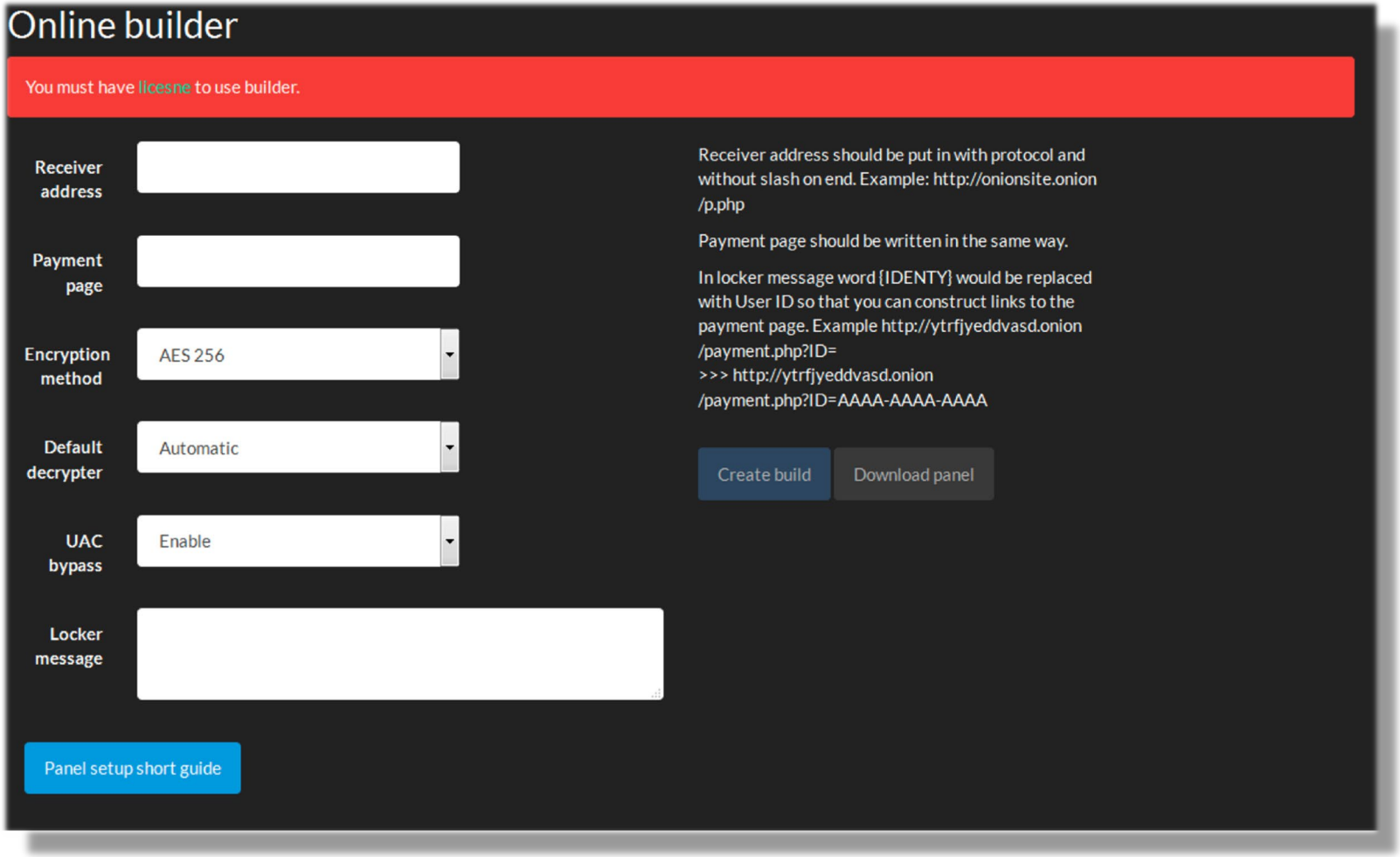
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

National Cyber Security Centre

RaaS Kits

Ransomware-as-a-Service

- RaaS kits readily available to build your own ransomware
- Come with instruction, only requires average computer skills.
- Classic model is user takes 80%, kit author takes 20%.
- Different price ranges – different amounts of configurability.



Modern Day ‘Blue Screen of Death

Deutsche Bahn

Train timetable during

WCry (WannaCry) incident

No longer limited to production databases.

Hackers are now hunting for your backups

Hackers spend days on your network **before** encrypting data

Time is spent looking for backup copies

Ransomware Attacks

Dwell Time Dropping

- Ransomware attacks accelerating
- Dwell Time falling
  - 416 Days in 2011
  - 24 Days in 2021
  - 21 Days in 2022
  - 10 Days in 2023
  - 7 Days 2024
  - ? Days 2025
- Shortest dwell time 7hrs
- More sophisticated attacks is now driving up average dwell time

- *Attack dwell time is defined as when a threat actor remains undetected within a targeted network or endpoint.*
- *Dwell time starts immediately after an initial malware infection has taken place and continues until the malware has been completely removed from a device.*

 https://www.sophos.com/en-us/press/press-releases/2023/08/dwell-time-time-start-attack-when-its-detected-shrinks-8-days-first

Backups are our last line of Defence

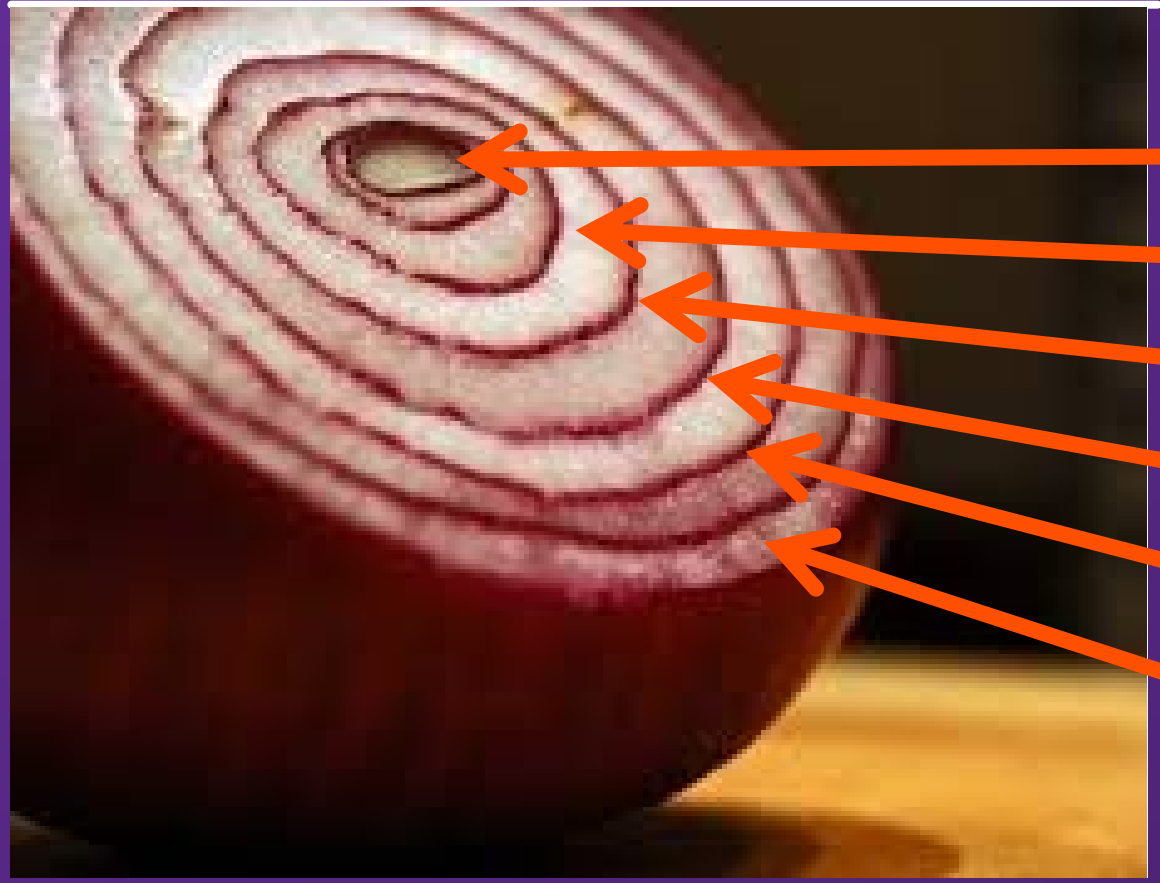
- If your data is encrypted, your only recourse is to restore from your backups.
  - Or Pay and Pray, and pay again and again…

PURESTORAGE®

So what can we do?

Source sample text

Think Defence in Depth



- Data security
- Application security
- Host security
- Network security
- Physical security
- Policies, procedures and awareness

Defence in Depth (1)

Policies, procedures, and awareness

Physical Security

Network Security

- Starts with employees and contractors
- Site / premises security
- Needs to now include remote access / working from home

Defence in Depth (2)

Host Security

- Hardened servers

Application Security

- Secure applications

Data security

- Know where all your data is

Implement a SIEM (Security Information and Event Management) solution such as Splunk

PURESTORAGE®

Protecting our database

From human error, malware or malicious intent

Oracle Automatic Storage Management (ASM)

Most attacks encrypt file systems

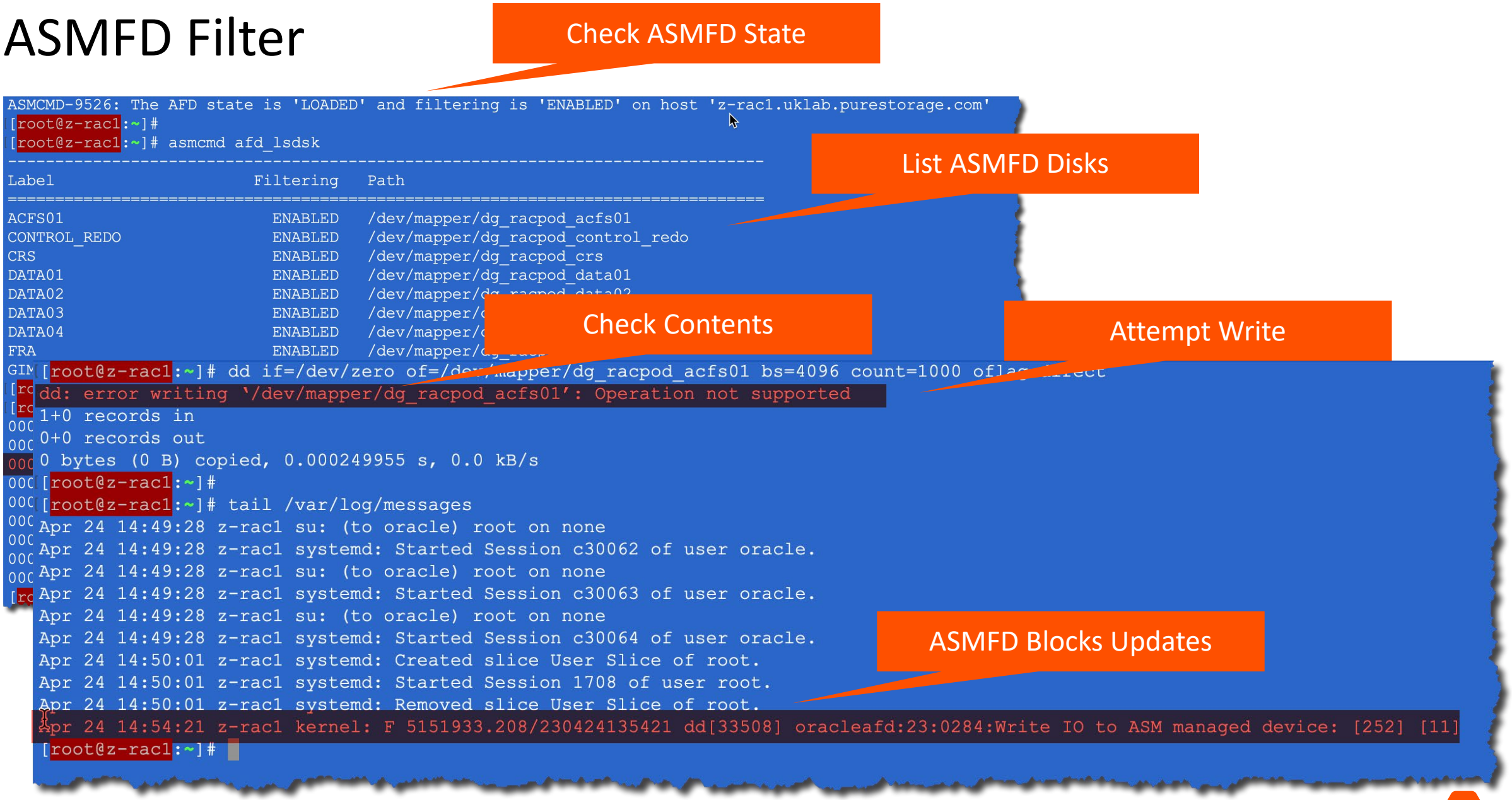
ASM uses raw block storage, it’s harder for malware and intruders to discover

Encrypting a raw file system is a lot more complex than a traditional file system .

Oracle ASM Filter Driver (ASMFD) & ASMLib V3

Limits access to ASM disk to Oracle database calls

ASMFD Filter



Confirm Block device OK

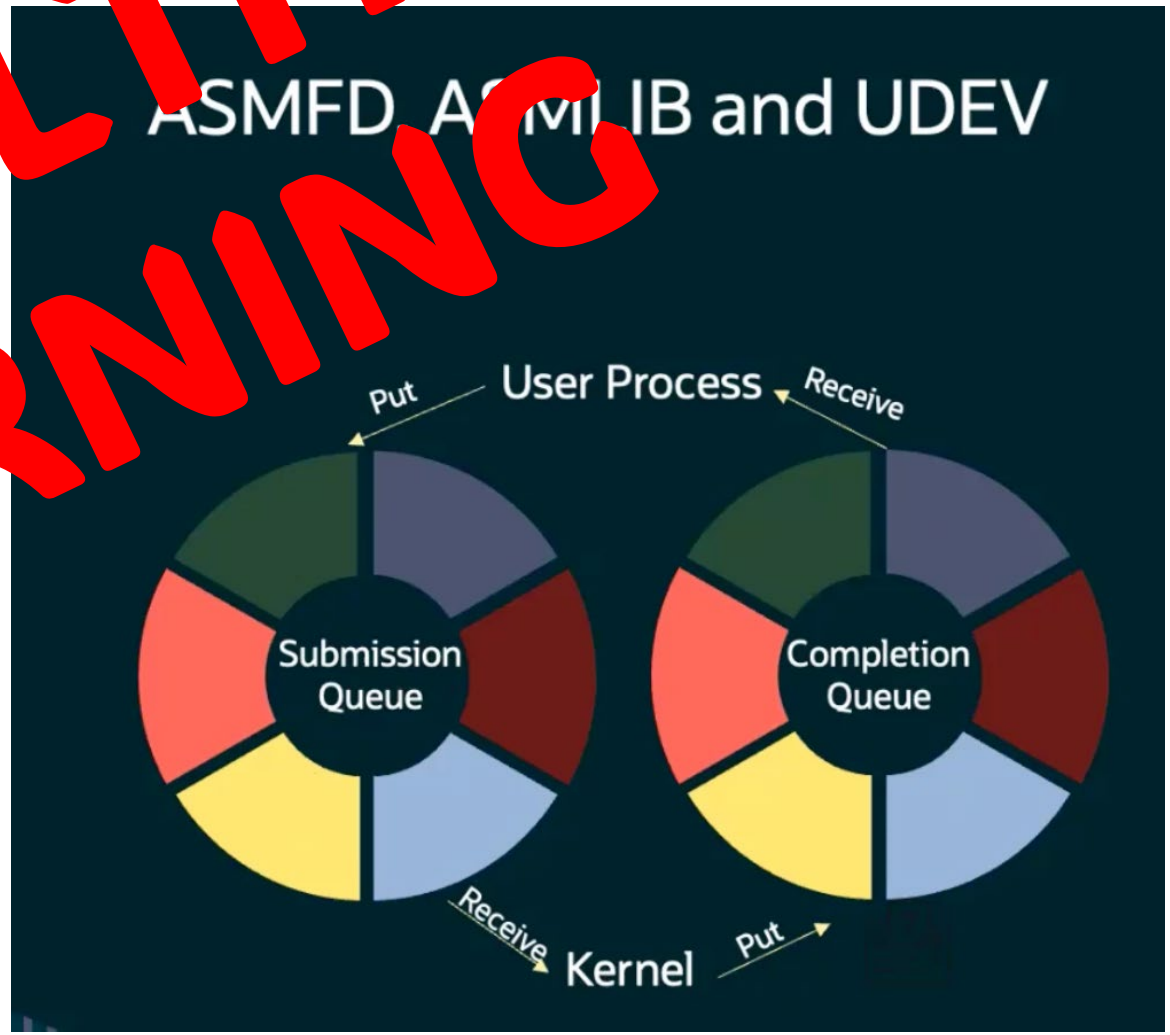
Kfed read /dev/mapper/dg_racpod_acfs01

```
kfbh.type:                            1 ; 0x002: KFBTYP_DISKHEAD
kfbh.datfmt:                          2 ; 0x003: 0x02
kfbh.block.blk:                       0 ; 0x004: blk=0
kfbh.block.obj:              2147483648 ; 0x008: disk=0
kfbh.check:                  2321497126 ; 0x00c: 0x8a5f3c26
kfbh.fcn.base:                  2845340 ; 0x010: 0x002b6a9c
kfbh.fcn.wrap:                        0 ; 0x014: 0x00000000
kfbh.spare1:                          0 ; 0x018: 0x00000000
kfbh.spare2:                          0 ; 0x01c: 0x00000000
kfdhdb.driver.provstr:   ORCLDISKACFS01 ; 0x000: length=14
kfdhdb.driver.reserved[0]:   1397113665 ; 0x008: 0x53464341
kfdhdb.driver.reserved[1]:         12592 ; 0x00c: 0x00003130
kfdhdb.driver.reserved[2]:            0 ; 0x010: 0x00000000
kfdhdb.driver.reserved[3]:            0 ; 0x014: 0x00000000
kfdhdb.driver.reserved[4]:            0 ; 0x018: 0x00000000
kfdhdb.driver.reserved[5]:            0 ; 0x01c: 0x00000000
kfdhdb.compat:                318767104 ; 0x020: 0x13000000
kfdhdb.dsknum:                        0 ; 0x024: 0x0000
kfdhdb.grptyp:                        1 ; 0x026: KFDGTP_EXTERNAL
```

ASMFD, ASMLIB & UDEV

- Latest Linux Kernel using io_uring
  - Impacts ASMFD IO Filtering
- Updates to ASMFD and ASMLIB to adapt to this change in i/o layer
- ASM Disks configured to use udev continue to function without any changes
- ASMFD Filtering is disabled in 12.24+ by default, prior releases need to be done manualy.
  - Soft-filtering can be disabled by "afdtool -filter disable" or "asmcmd afd_filter -d"

HEALTH WARNING



Migrate to ASMLib v3 for Database Protection

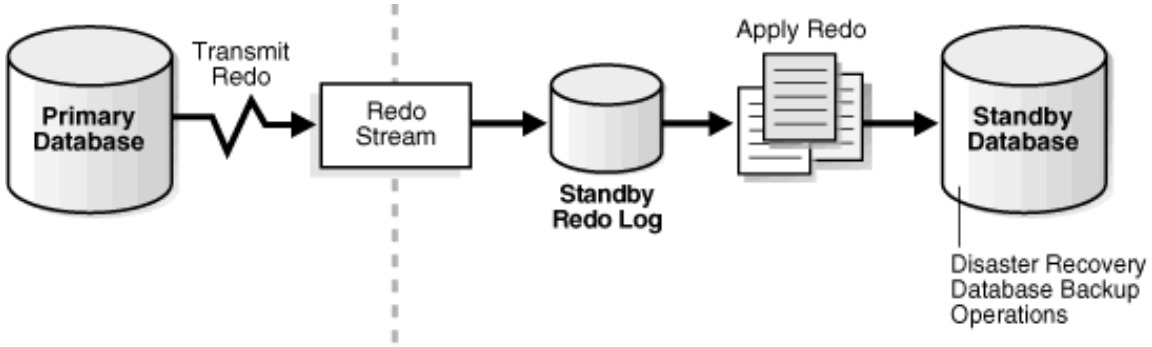
Another line of defence

Oracle Data Guard

Ransomware may not impact other Data Centre's

File system encryption not be replicated

Fail over to Standby database in event of disaster



Finally utilise Primary Storage Snapshots

Use primary Storage Snapshots to provide instant point-in-time recovery

Snapshot Database and Application binaries.

Nothing is faster than a pure meta-data operation

Automate Primary Storage Snapshots

With REST APIs

- Most modern infrastructure and applications supports REST interfaces
- Call REST interfaces using preferred language, utilities and DevOps technologies.
  - Python, PowerShell, Java…
  - Bash, Curl…
  - Terraform, Ansible..

  And PL/SQL

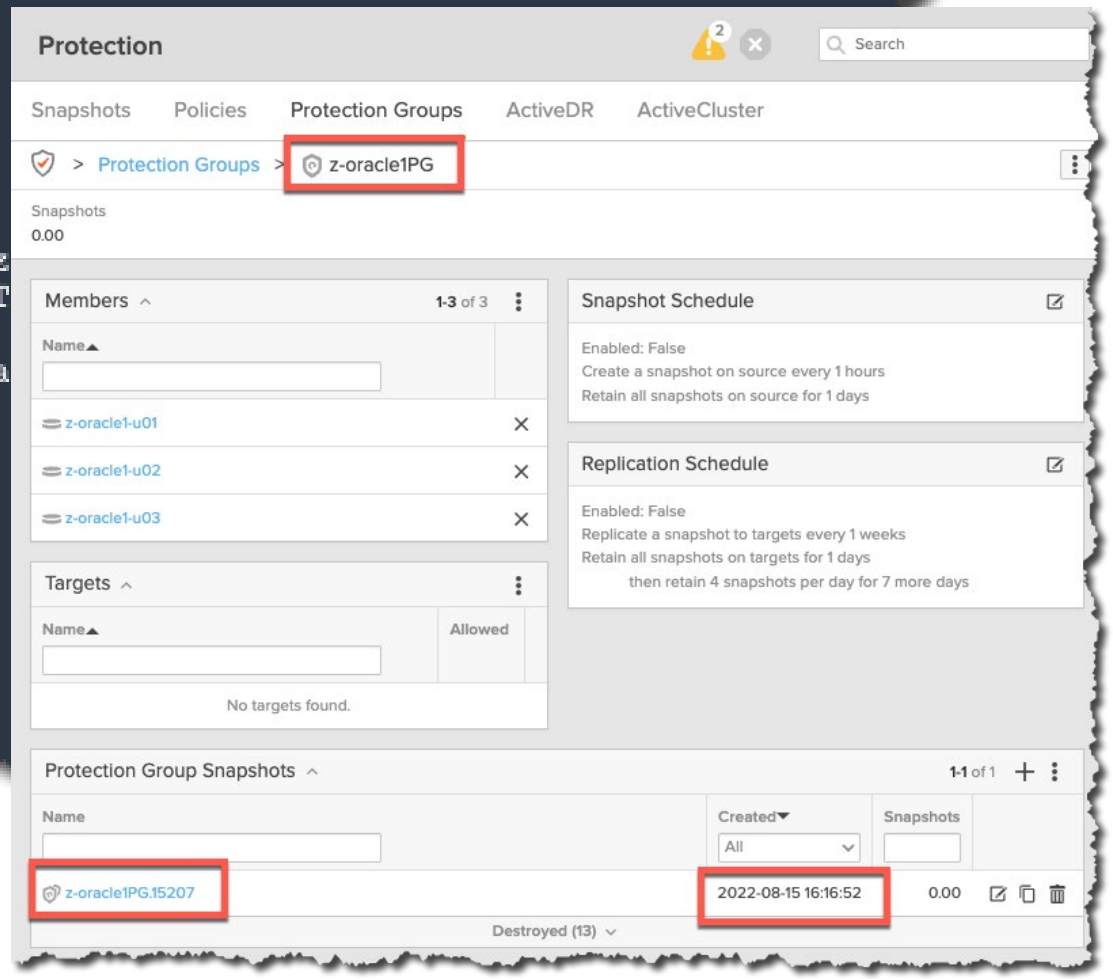
Use UTL_HTTP from with database

```
dbms_output.put_line('Create FlashArray Session');
dbms_output.put_line('-----------------------------------------------');

l_path := p_url || '/api/1.19/auth/session';
l_body := '{"api_token":"' || p_token ||'"}';

-- Prepare for Create session
l_http_request := UTL_HTTP.begin_request(l_path, 'POST' );

-- set Headers
UTL_HTTP.set_header(l_http_request, 'user-agent', 'mozilla/4.0');
UTL_HTTP.set_header(l_http_request, 'content-type', 'application/json');
UTL_HTTP.set_header(l_http_request, 'Content-Length', length(l_body));

-- set Body of request
UTL_HTTP.write_text(l_http_request, l_body);

-- get Response
l_http_response := UTL_HTTP.get_response(l_http_request);
dbms_output.put_line('Response status code: ' || l_http_response.status_code);

-- Loop through the response.
BEGIN
  LOOP
    UTL_HTTP.read_text(l_http_response, l_text, 32766);
    dbms_output.put_line ('Logon: ' || l_text);
  END LOOP;
EXCEPTION
  WHEN UTL_HTTP.end_of_body THEN
   dbms_output.put_line ('>');
END;

-- Loop through HTTP headers
FOR i IN 1..UTL_HTTP.GET_HEADER_COUNT(l_http_response) LOOP
  UTL_HTTP.GET_HEADER(l_http_response, i, l_name, l_value);
  -- DBMS_OUTPUT.PUT_LINE(l_name || ': ' || l_value);
  IF l_name = 'Set-Cookie' THEN
    l_cookie := l_value;
  END IF;
END LOOP;
```

```
dbms_output.put_line('>');
dbms_output.put_line('Perform Protection Group Snapshot of ' || p_pgroup);
dbms_output.put_line('-----------------------------------------------');

l_path := p_url || '/api/1.19/pgroup';
l_body := '{"snap":"true","source": ["' || p_pgroup ||'" ]}';

dbms_output.put_line('>' || l_path);
dbms_output.put_line('' || l_body);

-- Make a HTTP request and get the response.
l_http_request := UTL_HTTP.begin_request(l_path, 'POST' );

-- set Headers
UTL_HTTP.set_header(l_http_request, 'user-agent', 'mozilla/4.0');
UTL_HTTP.set_header(l_http_request, 'content-type', 'application/json');
UTL_HTTP.set_header(l_http_request, 'Content-Length', length(l_body));

-- set Body of request
UTL_HTTP.write_text(l_http_request, l_body);

-- get Response
l_http_response := UTL_HTTP.get_response(l_http_request);
dbms_output.put_line('Response status code: ' || l_http_response.status_code);

-- Loop through the response.
BEGIN
  LOOP
    UTL_HTTP.read_text(l_http_response, l_text, 32766);
    dbms_output.put_line (l_text);
  END LOOP;
EXCEPTION
  WHEN UTL_HTTP.end_of_body THEN
    UTL_HTTP.end_response(l_http_response);
END;
```

Automate Storage Snapshots

```
SQL> exec fa_snapshot('https://z-m20-a.uklab.purestorage.com','5d8ad02f-547d-fc24-bb51-
fa0d2b0de973','z-oracle1PG');
Create FlashArray Session
------------------------------------------------
Response status code: 200
Logon: {"username": "pureuser"}
>
Session Cookie:
session=.eJwtzMEKgzAQhOFXKXPOoWqQ1JcJi7sBwSSySQ5FfHdjKcz
LFpAqfT1x3BIMytbjiVfrJdiZA3_c6qZgh1Ucz2GYyI7cN46My6AV0UT
bja4CnRg
pmo; Expires=Mon, 15-Aug-2022 15:46:52 GMT; HttpOnly; Pa
>
Perform Protection Group Snapshot of z-oracle1PG
------------------------------------------------
>https://z-m20-a.uklab.purestorage.com/api/1.19/pgroup
{"snap":"true","source": ["z-oracle1PG" ]}
Response status code: 200
[{"name": "z-oracle1PG.15207", "source": "z-oracle1PG",

PL/SQL procedure successfully completed.
```



https://github.com/raekins/Oracle-HTTP/

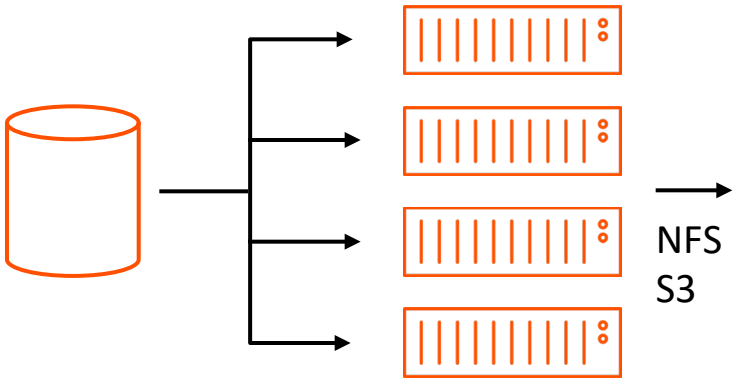
PURESTORAGE®

Protecting our data and backups

From accidental or RMAN policy deletion

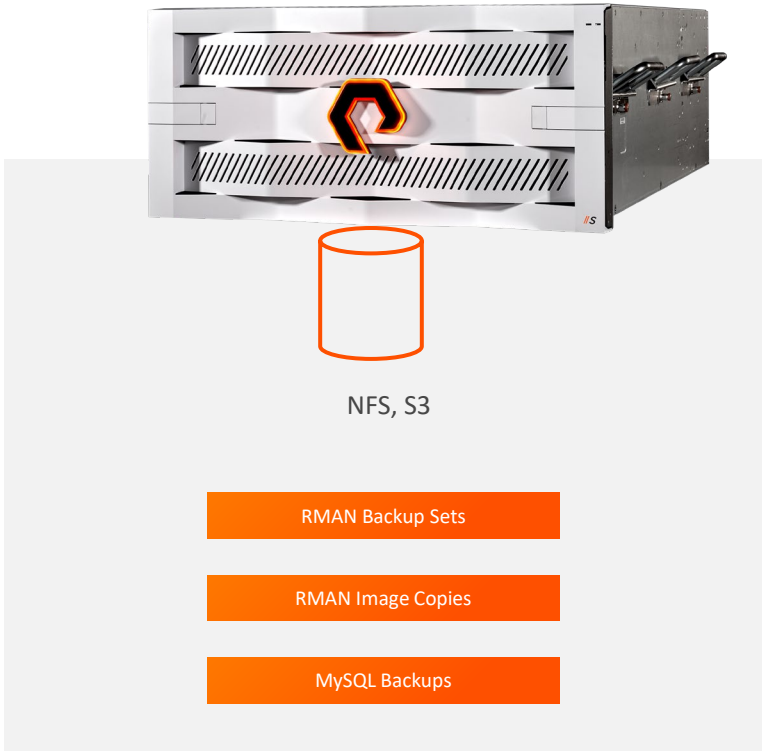
Database Protection – The 3:2:1+ Rule

Perform Off-array backup



Any Primary Storage

Database Servers



Database Backups

03 Create one primary backup and two copies of your data

02 Save your backups to two different types of media

01 Keep at least one backup file offsite

\+ + Make sure they're immutable and protected

Replicate to a secondary array or Cloud

AutoMounter Setup

Autofs setup

Install autofs

$ sudo yum install autofs

Create Automounter Map

$ sudo vi /etc/auto.master.d/fbnfs.autofs

```
[oracle@z-rac1 ~]$ cat /etc/auto.master.d/fbnfs.autofs
/mnt/orabkup    /etc/auto.fbnfs  --timeout=180
```

Timeout default is 300 seconds (5 minutes) inactivity

Create Map File

$ sudo vi /etc/auto.fbnfs

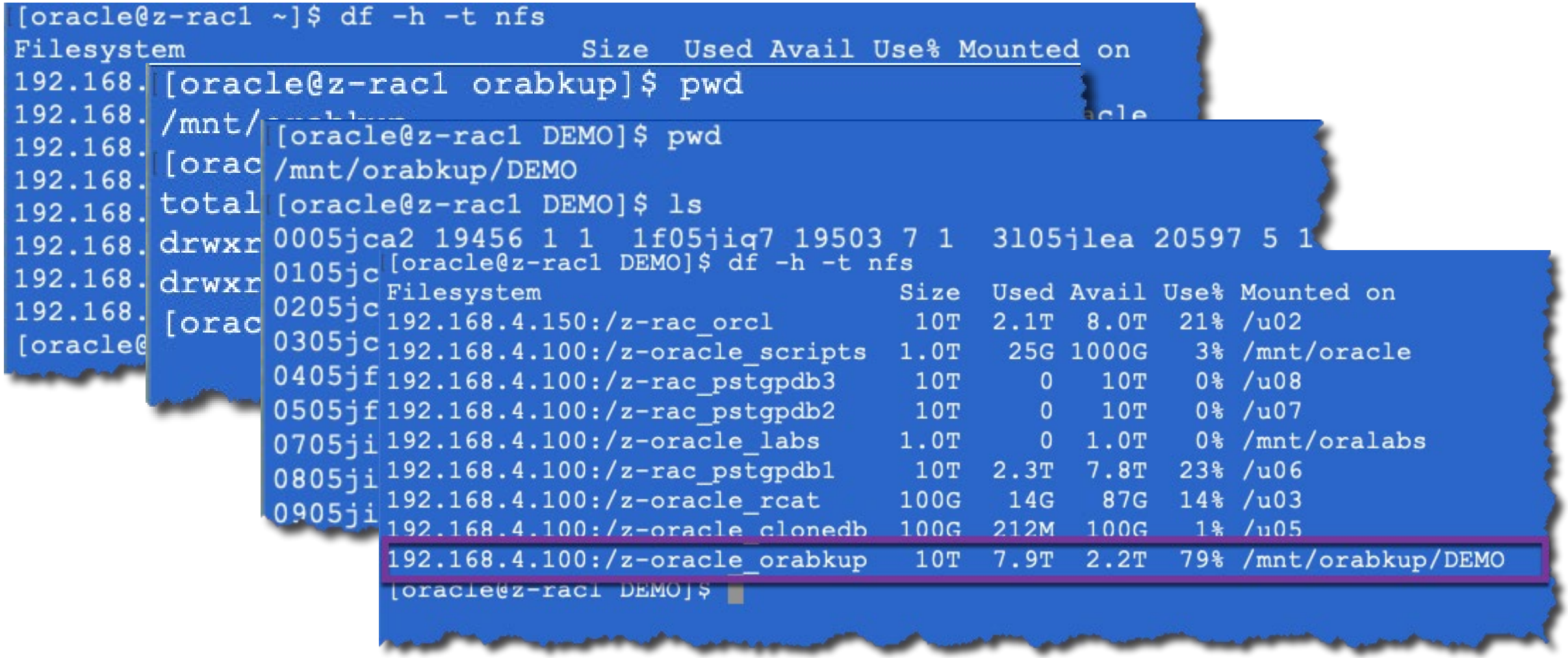
```
[oracle@z-rac1 ~]$ cat /etc/auto.fbnfs
DEMO -fstype=nfs,rw,soft,intr 192.168.4.100:/z-oracle_orabkup
ORCL -fstype=nfs,rw,soft,intr 192.168.4.100:/z-oracle_orabkup1
```

Start autofs Service

$ sudo systemctl enable --now autofs Created symlink from /etc/systemd/system/multi-user.target.wants/autofs.service to /usr/lib/systemd/system/autofs.service.

RMAN NFS mount hidden

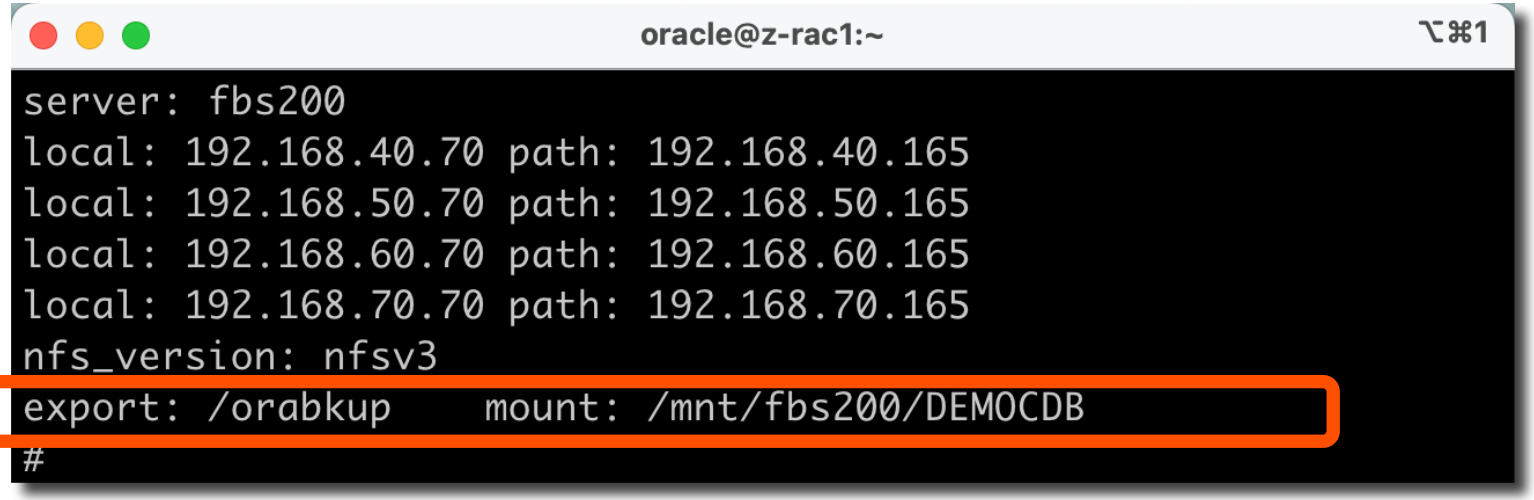
AutoFS mounts on backup location on-demand

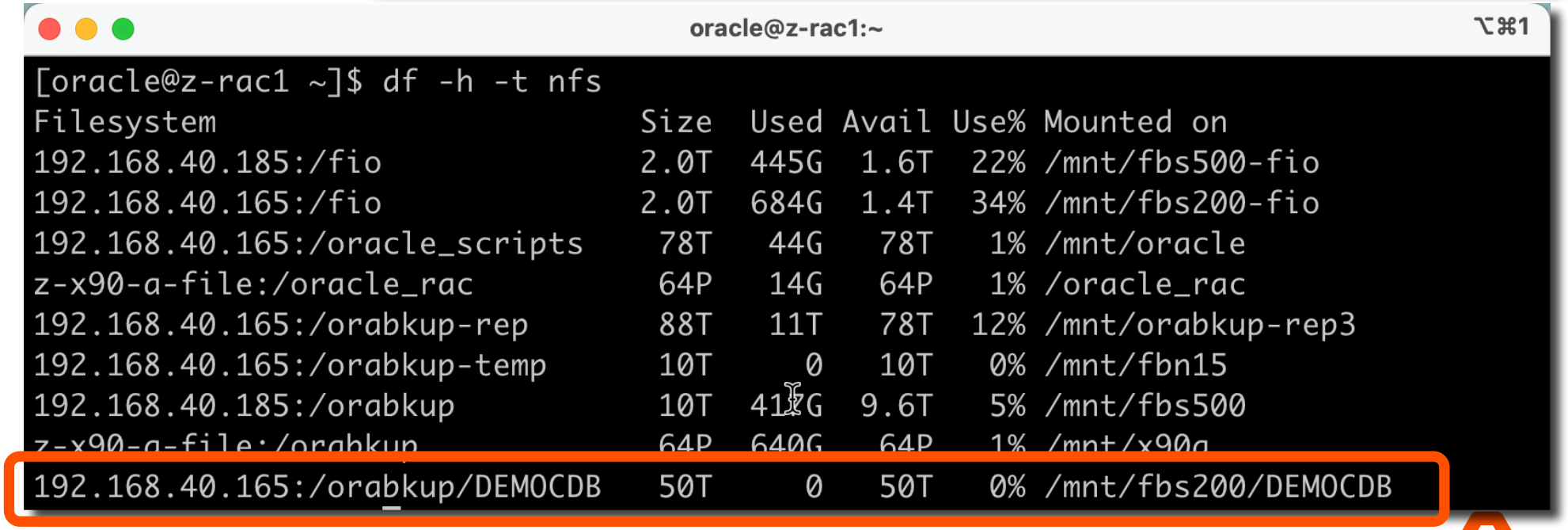


RMAN Backup location ‘/mnt/orabkup/DEMO’

We can also use Oracle dNFS

- Oracle dNFS dynamically mounts the NFS export using the *oranfstab* file
- Configure */etc/fstab* to provide backup path.





Performing RMAN Backup

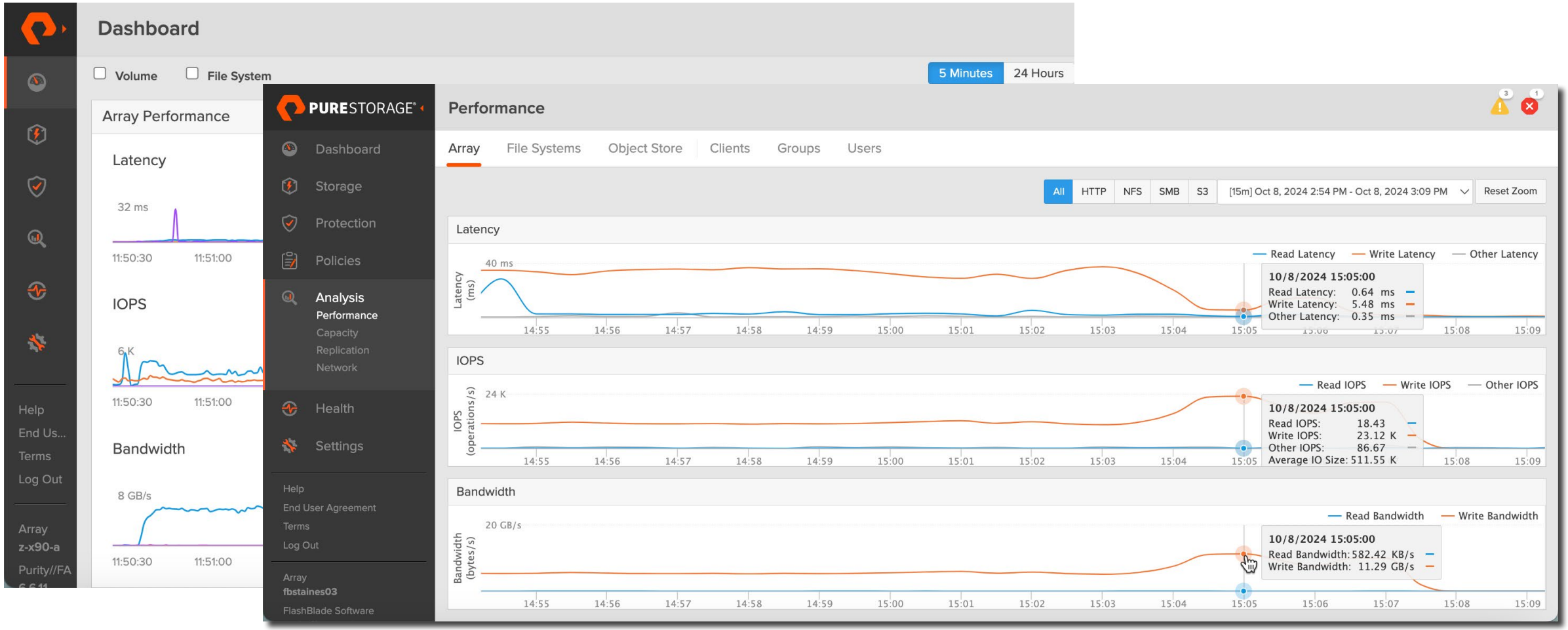
```
channel ORA_DISK_50: datafile copy complete, elapsed time: 00:00:53
channel ORA_DISK_50: starting datafile copy
input datafile file number=00042 name=+DATA/DEMOCDB/21C46BA6D08E9210E0633970E10AE121/DATAFILE/soe.300.1179324533
backing up blocks 3145729 through 3670016
output file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-36_hv372asd tag=FBS200
channel ORA_DISK_36: datafile copy complete, elapsed time: 00:00:24
channel ORA_DISK_36: starting datafile copy
input datafile file number=00042 name=+DATA/DEMOCDB/21C46BA6D08E9210E0633970E10AE121/DATAFILE/soe.300.1179324533
backing up blocks 3670017 through 3932160
output file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-34_ht372asd tag=FBS200
channel ORA_DISK_48: datafile copy complete, elapsed time: 00:00:46
channel ORA_DISK_48: starting datafile copy
input datafile file number=00043 name=+DATA/DEMOCDB/21C46BA6D08E9210E0633970E10AE121/DATAFILE/soe.299.1179324545
backing up blocks 524289 through 1048576
output file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-33_hs372asc tag=FBS200
channel ORA_DISK_55: datafile copy complete, elapsed time: 00:00:49
channel ORA_DISK_55: starting datafile copy
input datafile file number=00043 name=+DATA/DEMOCDB/21C46BA6D08E9210E0633970E10AE121/DATAFILE/soe.299.1179324545
backing up blocks 1048577 through 1572864
output file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-33_hs372asc tag=FBS200
channel ORA_DISK_60: datafile copy complete, elapsed time: 00:00:49
channel ORA_DISK_60: starting datafile copy
input datafile file number=00043 name=+DATA/DEMOCDB/21C46BA6D08E9210E0633970E10AE121/DATAFILE/soe.299.1179324545
backing up blocks 1572865 through 2097152
```


We can see Backup using v$dnfs_files view

```
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-63_le3726kq      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-65_li3726lb      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-66_lk3726mg      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-66_lk3726mg      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-67_lm3726mn      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-67_lm3726mn      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-68_lo3726mn      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-68_lo3726mn      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-69_lq3726mo      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-69_lq3726mo      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-70_ls3726ms      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-70_ls3726ms      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-71_lu3726n0      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-71_lu3726n0      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-72_m03726n3      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-72_m03726n3      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-73_m23726n5      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-73_m23726n5      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-74_m43726n6      30,720
/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-74_m43726n6      30,720
```

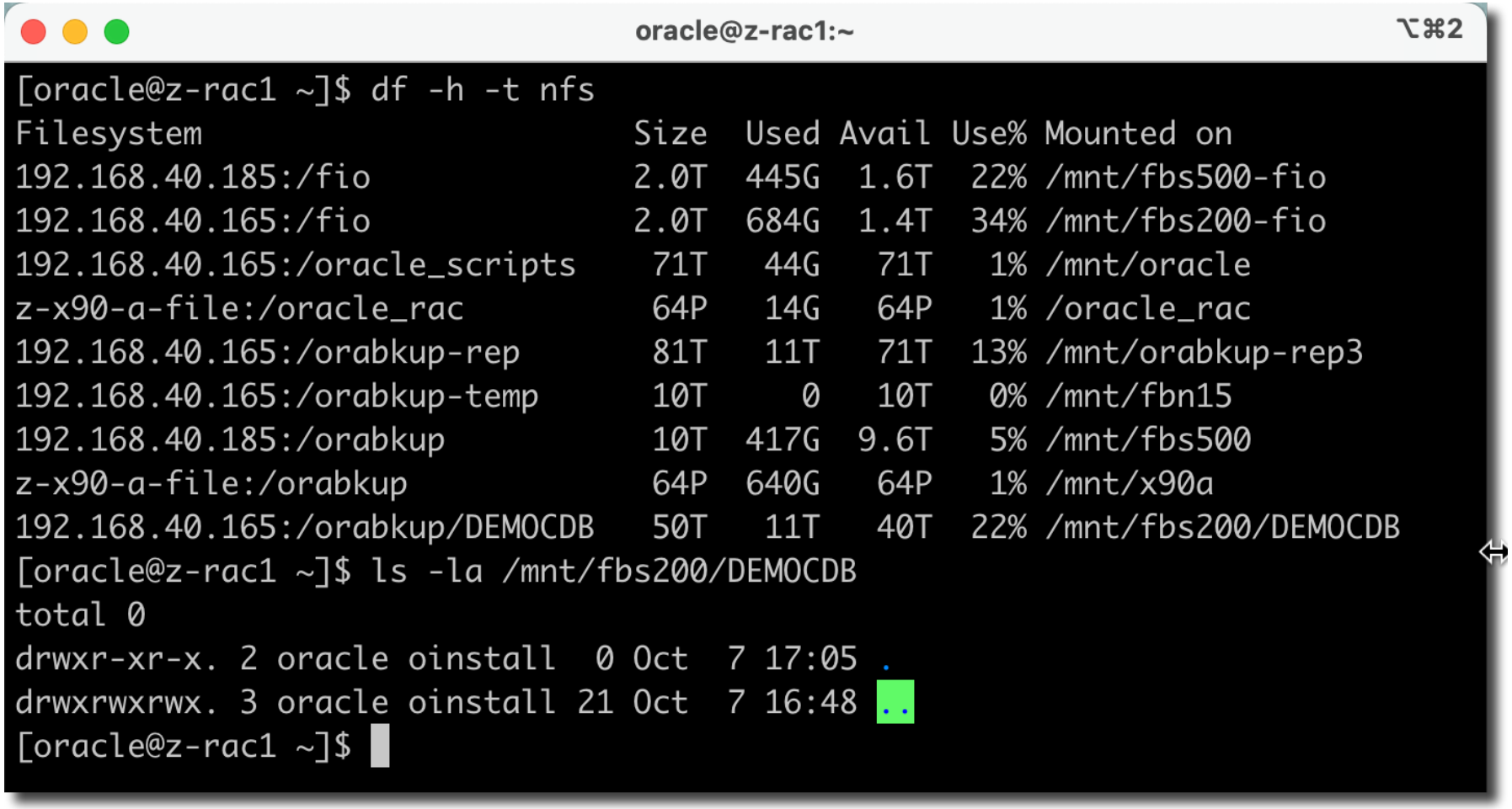
Check Storage Platform Activity

Block READ & FILE (NFS) WRITES



Backups Hidden from Operating System

- RMAN Backup files are not visible from the OS, only usage.
- Oracle or other users can't accidentally delete RMAN backups.



Backups can still be manged by RMAN

```
RMAN>
List of Datafile Copies
=======================

Key     File S C
------- ---- - --
27037   2    U 0
        Name: /m
        Tag: FBS
        Containe

27038   15   U 0
        Name: /m
        Tag: FBS
        Containe

27039   16   U 0
        Name: /m
        Tag: FBS
        Containe

27040   17   U 0
        Name: /m
        Tag: FBS200
        Container ID: 3, PDB Name: DEMOPDB
```

```
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-15_fe372a95 RECID=1187 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-16_ff372a96 RECID=1188 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-17_fg372a96 RECID=1189 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-19_fi372a96 RECID=1191 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-21_fk372a96 RECID=1193 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-22_fl372a96 RECID=1194 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-23_fm372a96 RECID=1195 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-25_fo372a97 RECID=1197 STAMP=1181821223
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-27_fq372a97 RECID=1199 STAMP=1181821223
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-2_fd372a94 RECID=1186 STAMP=1181821221
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-18_fh372a96 RECID=1190 STAMP=1181821222
deleted datafile copy
datafile copy file name=/mnt/fbs200/DEMOCDB/data_D-DEMOCDB_I-364614626_TS-SOE_FNO-20_fj372a96 RECID=1192 STAMP=1181821222
deleted datafile copy
```

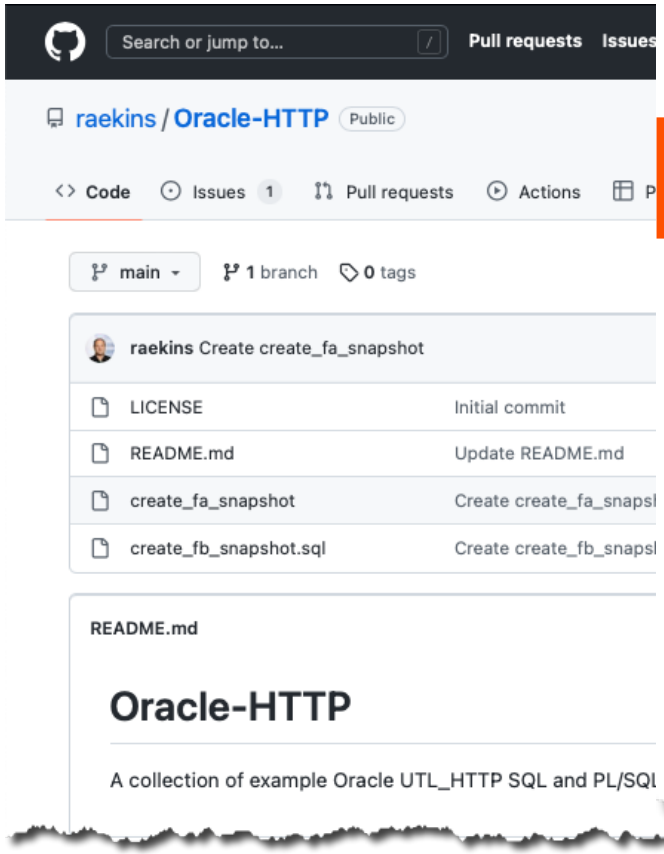

Utilise NFS Storage Snapshots

Take NFS file system immutable snapshots of RMAN backups.

Read-Only snapshots stop accidental or policy based deletion.

Perform File System snapshot Using SQL

Oracle UTL_HTTP




```
BEGIN
  UTL_HTTP.set_wallet('&p_wallet_d','&p_wallet_p');

  -- If using HTTPS, open a wallet containing the trusted root certificate.
  IF p_wallet_path IS NOT NULL AND p_wallet_password IS NOT NULL THEN
    UTL_HTTP.set_wallet('file:' || p_wallet_path, p_wallet_password);
  END IF;

  dbms_output.put_line('Create FlashBlade Session');
  dbms_output.put_line('-----------------------------------------------');

  l_path := p_url || '/api/login';

  -- Make a HTTP request and get the resp
  l_http_request  := UTL_HTTP.begin_requ

  UTL_HTTP.set_header(r     => l_http_re
                      name  => 'api-toke
                      value => p_token);

  UTL_HTTP.set_header(r     => l_http_req
                      name  => 'User-Agen
                      value => 'OracleDB/

  l_http_response := UTL_HTTP.get_respons
  dbms_output.put_line('Response status c
```

```
dbms_output.put_line('>');
dbms_output.put_line('Perform FileSystem Snapshot of ' || p_filesystem);

l_path := p_url || '/api/1.12/file-system-snapshots?sources=' || p_filesystem || chr(38) || 'send=false';
dbms_output.put_line('>' || l_path);

-- Make a HTTP request and get the response.
l_http_request  := UTL_HTTP.begin_request(url => l_path, method => 'POST' );

UTL_HTTP.set_header(r     => l_http_request,
                    name  => 'User-agent',
                    value => 'OracleDB/19c');

UTL_HTTP.set_header(r     => l_http_request,
                    name  => 'x-auth-token',
                    value => l_xauth_token);

l_http_response := UTL_HTTP.get_response(l_http_request);

dbms_output.put_line('Response status code: '||l_http_response.status_code);
```

https://github.com/raekins/Oracle-HTTP/

Automate File System Snapshots

```
SQL> exec fb_snapshot('https://fbstaines02.uklab.purestorage.com','T-da03a759-bb3f-4995-9c6c-
fee48d7c1a98','ora-test');
Create FlashBlade Session
------------------------------------------------
Response status code: 200
Logon: {"username":"pureuser"}
>
x-auth-token: 75c16f38-f628-4888-b796-41663d1561a2
>
Perform FileSystem Snapshot of ora-test
------------------------------------------------
>https://fbstaines02.uklab.purestorage.com/api/1.12/file-system-snapshot
test&send=false
Response status code: 200
{"items":[{"name":"ora-
test.2022_08_10_13_56","suffix":"2022_08_10_13_56","created":16601361960
{"name":null,"id":null,"resource_type":null,"location":null,"is_local":n
ll},"destroyed":false,"source_destroyed":null,"time_remaining":null,"id"
7e2c-64aa8bb6505c","owner":{"name":"ora-test","id":"e8d16880-fe19-6224-a
0f729f298e32","resource_type":"
file-systems"},"owner_destroyed":false,"source":"ora-test","source_id":"
0f729f298e32","source_is_local":true,"source_location":{"name":"fbstaine
6d81-433f-bb
31-5fc33e76fa5f","resource_type":"arrays"},"source_display_name":"ora-te
>
>
List FileSystem Snapshots of ora-test
------------------------------------------------
>https://fbstaines02.uklab.purestorage.com/api/1.12/file-system-snapshot
sort=created&names_or_sources=ora-test
Response status code: 200
{"total":
{"name":null,"suffix":null,"created":null,"policy":null,"destroyed":null
,"time_remaining":null,"id":null,"owner":null,"owner_destroyed":null,"so
null,"source_is_local":null,"source_location":null,"source_display_name"
:{"total_item_count":1,"continuation_token":null},"items":[{"name":"ora-
test.2022_08_10_13_56","suffix":
"2022_08_10_13_56","created":1660136196000,"policy":
{"name":null,"id":null,"resource_type":null,"location":null,"is_local":n
,"destroyed":false,"source_destroyed":false,"time_re
maining":null,"id":"b05be6f6-7771-e708-7e2c-64aa8bb6505c","owner":{"name
test","id":"e8d16880-fe19-6224-a443-0f729f298e32","resource_type":"file-
systems"},"owner_destroyed":false,"source":"ora-t
est","source_id":"e8d16880-fe19-6224-a443-
0f729f298e32","source_is_local":true,"source_location":{"name":"fbstaines02","id":"66992c13-
6d81-433f-bb31-5fc33e76fa5f","resource_type":"arrays"},"source_dis
play_name":"ora-test"}]}

PL/SQL procedure successfully completed.
```

Check File System Snapshot

From the OS we can now see the the database procedure has created a FlashBlade file system snapshot in the .snapshot directory

```
# ls -al /mnt/ora-test/.snapshot
total 0
drwxr-xr-x. 1 root root 0 Aug 10 13:56 .
drwxrwxrwx. 2 root root 0 Aug 10 12:09 ..
drwxrwxrwx. 2 root root 0 Aug 10 12:09 ora-test.2022_08_10_13_56
```

From the FlashBlade we can also see the file system snapshot.

File System Snapshots

RMAN Catalog Snapshot

RMAN> catalog start with '<snapshot directory>' noprompt;

```
RMAN Catalog snapshot: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552

Recovery Manager: Release 19.0.0.0.0 - Production on Tue Jun 8 09:35:53 2021
Version 19.10.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

connected to target database: DEMO (DBID=3784643325)
connected to recovery catalog database

RMAN>
searching for all files that match the pattern /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552

List of Files Unknown to the Database
=====================================
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/df00alat_17839_1_1
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/dg00alat_17840_1_1
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/dh00alb4_17841_1_1
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/di00alb4_17842_1_1
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/dj00alb4_17843_1_1
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/dk00alb4_17844_1_1
File Name: /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.08-JUN-2021-093552/dl00alb5_17845_1_1
```

RMAN Validate Snapshot

RMAN> restore database validate

```
channel ORA_DISK_34: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/n700an53_18151_1_1
channel ORA_DISK_35: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/n800an54_18152_1_1
channel ORA_DISK_36: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/n900an54_18153_1_1
channel ORA_DISK_37: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nf00an5b_18159_1_1
channel ORA_DISK_38: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nj00an5j_18163_1_1
channel ORA_DISK_39: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/ni00an5h_18162_1_1
channel ORA_DISK_40: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nl00an5o_18165_1_1
channel ORA_DISK_41: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nk00an5n_18164_1_1
channel ORA_DISK_42: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nh00an5f_18161_1_1
channel ORA_DISK_43: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/ng00an5d_18160_1_1
channel ORA_DISK_44: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/ne00an5b_18158_1_1
channel ORA_DISK_45: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nm00an5q_18166_1_1
channel ORA_DISK_23: piece handle=/mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/na00an55_18154_1_1 tag=TAG20210601T15132
channel ORA_DISK_23: restored backup piece 1
channel ORA_DISK_23: validation complete, elapsed time: 00:00:02
channel ORA_DISK_24: piece handle=/mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nb00an57_18155_1_1 tag=TAG20210601T15132
channel ORA_DISK_24: restored backup piece 1
channel ORA_DISK_24: validation complete, elapsed time: 00:00:02
channel ORA_DISK_40: piece handle=/mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nl00an5o_18165_1_1 tag=TAG20210601T151323
channel ORA_DISK_40: restored backup piece 1
channel ORA_DISK_40: validation complete, elapsed time: 00:00:01
channel ORA_DISK_45: piece handle=/mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nm00an5q_18166_1_1 tag=TAG20210601T151323
channel ORA_DISK_45: restored backup piece 1
channel ORA_DISK_45: validation complete, elapsed time: 00:00:01
channel ORA_DISK_25: piece handle=/mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/nd00an5a_18157_1_1 tag=TAG20210601T151323
channel ORA_DISK_25: restored backup piece 1
```

RMAN Restore Snapshot

RMAN> restore database

```
allocated channel: ORA_DISK_61
channel ORA_DISK_61: SID=368 instance=DEMO1 device type=DISK
allocated channel: ORA_DISK_62
channel ORA_DISK_62: SID=487 instance=DEMO1 device type=DISK
allocated channel: ORA_DISK_63
channel ORA_DISK_63: SID=612 instance=DEMO1 device type=DISK
allocated channel: ORA_DISK_64
channel ORA_DISK_64: SID=732 instance=DEMO1 device type=DISK

channel ORA_DISK_1: starting datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup set
channel ORA_DISK_1: restoring datafile 00020 to +DATA/DEMO/A5C6810E4B040548E0533970E10A590E/DATAFILE/soe.367.1040576831
channel ORA_DISK_1: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/ma00an4p_18122_1_1
channel ORA_DISK_2: starting datafile backup set restore
channel ORA_DISK_2: specifying datafile(s) to restore from backup set
channel ORA_DISK_2: restoring datafile 00021 to +DATA/DEMO/A5C6810E4B040548E0533970E10A590E/DATAFILE/soe.371.1040576863
channel ORA_DISK_2: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/mb00an4p_18123_1_1
channel ORA_DISK_3: starting datafile backup set restore
channel ORA_DISK_3: specifying datafile(s) to restore from backup set
channel ORA_DISK_3: restoring datafile 00022 to +DATA/DEMO/A5C6810E4B040548E0533970E10A590E/DATAFILE/soe.374.1040576893
channel ORA_DISK_3: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/mc00an4p_18124_1_1
channel ORA_DISK_4: starting datafile backup set restore
channel ORA_DISK_4: specifying datafile(s) to restore from backup set
channel ORA_DISK_4: restoring datafile 00023 to +DATA/DEMO/A5C6810E4B040548E0533970E10A590E/DATAFILE/soe.373.1040576927
channel ORA_DISK_4: reading from backup piece /mnt/orabkup/DEMO/.snapshot/z-oracle_orabkup.07-JUN-2021-161447/md00an4p_18125_1_1
```


PURESTORAGE®

SCHRODINGER'S BACKUP

The condition of any backup in unknow until a restore is attempted.


Are you ready
for a
Ransomware
Attack ?

Understand business impact and requirements

Do you have a Service Level Agreement with the business ?

Know how long a system restore takes

Understand any inter-system dependences

Peer review procedures and run-books

Get someone else to test your process

Utilise SafeMode Storage Snapshots

Take Primary Storage immutable snapshots
Take NFS file system immutable snapshots of RMAN backups.

Read-Only immutable snapshots prevent accidental, malicious or policy based deletion.

NG/MAX

737 NG
737-8 MAX
Cockpit Companion

This manual is the property of: _____

Phone: _____

Document, simulate incidents and practice

Finally, remember protection needs a Team

Data Defence-in-Depth

We all need to constantly review and reduce our exposure to malware and other threats.

Adopt a multi-layered approach to data protection, give ourselves the best possible protection

Network, Storage, Linux Admins, Application Developers, SREs and DBAs…