OCI Security Audits

CIS benchmarks and SELinux

SKILLBUILDERS

Applying the CIS benchmarks

- The Centre for Internet Security
  - Publishes benchmarks for numerous environments
  - If you pass the benchmarks, you are probably OK
- Two that all DBAs will likely be using are:
  - CIS Oracle Database 19c Benchmark v1.1.0 - 12-16-2022
  - CIS Oracle Linux 8 Benchmark v2.0.0 - 03-29-2022
- OCI: the Vulnerability Scan Service
  - Generates reports for Compute Instances
  - DB Systems you must do yourself

SELinux is a de facto standard

- You won't pass the benchmarks without SELinux
  - Enabled by default on a Compute Instance
  - But not on a DB System
- Enabling SELinux
  - Use the dbcli utility
  - Straightforward, but does need a reboot

To conclude

- OCI has some nice facilities
  - The Vulnerability Scan Service checks CVEs
  - Apply the CIS benchmarks
  - But not on DB System nodes ☹
- SELinux is a basic requirement
  - Enabled by default on Compute instances
  - Requires configuration on a DB System