Oracle Deployment Isolation in a virtualized environment

INAIL Architecture Proposal

DIREZIONE CENTRALE PER L'ORGANIZZAZIONE DIGITALE

Author: Claudio Fini

Mail: c.fini@inail.it

Table of Contents

INTRODUCTION

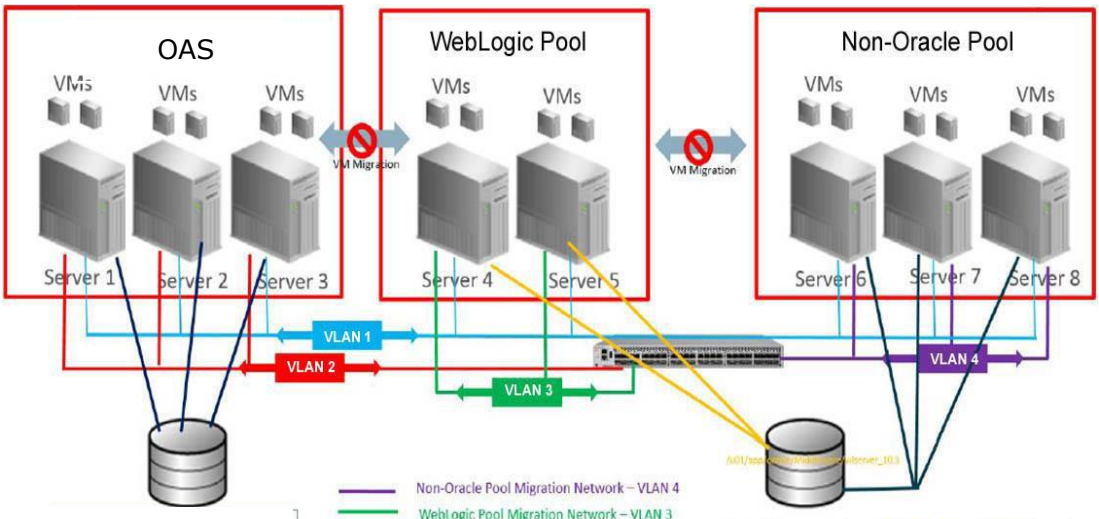
The purpose of this document is to demonstrate the physical network and physical storage constraints employed by Inail company to ensure Oracle software are isolated on specific servers in a virtualized environment (Vmware, Nutanix etc…).

ARCHITECTURE DIAGRAM

Esempio 1

The following diagram illustrates the virtualized environment on which Oracle programs will be deployed. There are several Oracle programs (Oracle Analitycs Server; Web Center Content; Web Logic Server; Web Logic server Multitenant; SOA Suite for Oracle Middleware; Unified Business Process Management Suite; Enterprise Identity Service Suite, Oracle Identity Manager Connector factor) which are deployed in separate resource pools. A third resource pool is shown and severs in this pool do not host VMs running Oracle programs. It also notes the separate storage device for Oracle and Non-Oracle pools and restricts VM migration to respective Pools.

Figure 1. Logical Design



Dedicated storage device for OAS exposed through LUN masking

vMotion VLAN id will be dedicated to clusters that host Oracle products.

Each pool will have different ID as well.
Will be possible to move the VMs among the Weblogic dedicated clusters. Is not possible vMotion between a Weblogic cluster and a not Weblogic cluster because the dedicated VLAN is not present on other clusters (in any case the storage segregation it would prevent it too)

The same concept can be applied to Oracle Analitycs Server and all the other products listed above.

ISOLATION DESCRIPTION

Physical Hardware Isolation

Here we describe how the physical hardware, network and storage will be architected to prevent and limit VM migration across non-Oracle and Oracle ESXi Clusters.

Network Isolation

Network isolation will be obtained through isolated migration network for each Oracle ESXi cluster. Each migration network of each Oracle ESXi Cluster doesn't have a gateway, so that communication between migration network of non-Oracle ESXi cluster and migration network of Oracle ESXi cluster is forbidden.

In conclusion, network isolation will be obtained using **dedicated VLAN**.

Storage Access Restrictions

In our infrastructure every LUN will be zoned, so it will be visible to one specific VMware cluster only. But the boot LUNs that will be visible to its own host only.

Lun Masking on storage array to grant access of a single LUN to ESXi hosts in a single cluster only.

VM and Storage Migration Restriction

VM and Storage migration will be restricted in our virtualized environment through the two following techniques:

a) Dedicated and **isolated VLAN** by lack of gateway for dedicated migration Network of Oracle ESXi Clusters
b) Dedicated and exclusive **LUNs** for Oracle and non-Oracle ESXi Clusters

VALIDATION AND QUANTIFICATION

VM and Storage Migration Network

Here we report an example of the command to show the **VLAN** configuration:

"*sh vlan id* 2831"

This is a future architecture we will provide the network information in the event of an audit.

Storage Access Restriction

Storage Access Restriction for DELL VMAX/PowerMax Storage

"`symaccess -sid xxx -type stor list -devs xxxx`"

The following output of Command Line Interface shows that the LUN named 01521 is assigned to specific Storage Group.

```
cseadmin@localhost:~> symaccess -sid 671 -type stor list -devs 01521

Symmetrix ID          : 000296700671


Storage Group Name
--------------------------------
SG_ASLPRI02
```

"**`symaccess -sid xxx list assign -devs xxxx`**"

The following output of Command Line Interface shows that the LUN named 01521 can be accessed only by the authorized host wwn.

```
cseadmin@localhost:~> symaccess -sid 671  list assign -devs 01521

Symmetrix ID          : 000296700671

Sym
Dev     Identifier        Type   Dir:Port
------  ----------------  -----  ----------------
01521   100028924aafe8c0  FIBRE  FA-3D:011,FA-5D:024
        100028924aaff814  FIBRE  FA-3D:011,FA-5D:024
```

"symaccess -sid xxx -type init list -wwn xxxxxxxxxxx"

The following output of Command Line Interface shows that host wwn belong to specific host group

```
cseadmin@localhost:~> symaccess -sid 671 -type init list -wwn 100028924aafe8c0

Symmetrix ID          : 000296700671


Initiator Group Name
--------------------------------
IG_ASLPRI02
```

Storage Access Restriction for HPE Nimble Storage

"vol --info xxx (LUN_NAME) **--pool** xxx (POOL_NAME)"

The following output of Command Line Interface shows that the LUN named **MDSNOPRODWIN01-01** can be accessed only by the authorized host wwn (initiator).

Nimble OS **$ vol --info MDSNOPRODWIN01-01 --pool sp-santuario**

```
Name: MDSNOPRODWIN01-01
Serial number: 2c559cc3a723d0186c9ce9002d9c0604
Target name: 56:c9:ce:90:5a:52:14:00
Description:
Owned by: HPENIMB
Size (MiB): 8388608
Pool: sp-santuario
Move to pool: N/A
Move aborting: N/A
Move data migrated: N/A
Move data remaining: N/A
Move start time: N/A
Move estimated completion time: N/A
Folder: N/A
Performance policy: default
Block size (bytes): 4096
Reserve: 0%
Limit: 100%
```

```
Snapshot count: 48
Volume mapped usage (MiB): 139050
Volume compression: 1.82X
Uncompressed snapshot usage including pending deletes (MiB): 22333
Snapshot compression: 2.32X
Read only: No
Multi-initiator: No
Thinly-provisioned: Yes
Cache pinned: N/A
Pinned cache size (MiB): N/A
Upstream cache pinned: No
Caching enabled: N/A
Cache policy: N/A
State: online
Online: Yes
Offline reason: N/A
Clone: No
Parent volume: N/A
Base snapshot: N/A
Volume collection: MDSNOPRODWIN01-Collection-Sant-Aci
Number of connections: 12
        iSCSI: 0
        FC: 12
Created: Feb  7 2023 15:09:04
Last configuration change: Feb  7 2023 15:09:05
Access Control List:
        Apply to: volume & snapshot
        Initiator Group: MDSNOPRODWIN01
        Access Protocol: fc
        LUN: 1
Connected Initiators:
Initiator: AIL-WLD-SYN02-ESX09_A (10:00:26:c5:21:20:00:44)
        Target FC Interface: (Sant-nimble-9995 : A : fc3a.1) (56:c9:ce:90:5a:52:14:05)
        ALUA: active/optimized
        PR Key: 0x0
        Target FC Interface: (Sant-nimble-9995 : B : fc3a.1) (56:c9:ce:90:5a:52:14:0d)
        ALUA: standby
        PR Key: 0x0
Initiator: AIL-WLD-SYN02-ESX09_B (10:00:26:c5:21:20:00:46)
        Target FC Interface: (Sant-nimble-9995 : A : fc1a.1) (56:c9:ce:90:5a:52:14:01)
```

```
        ALUA: active/optimized
        PR Key: 0x0
        Target FC Interface: (Sant-nimble-9995 : B : fc1a.1) (56:c9:ce:90:5a:52:14:09)
        ALUA: standby
        PR Key: 0x0
Initiator: AIL-WLD-SYN02-ESX10_A (10:00:26:c5:21:20:00:48)
        Target FC Interface: (Sant-nimble-9995 : A : fc3a.1) (56:c9:ce:90:5a:52:14:05)
        ALUA: active/optimized
        PR Key: 0x0
        Target FC Interface: (Sant-nimble-9995 : B : fc3a.1) (56:c9:ce:90:5a:52:14:0d)
        ALUA: standby
        PR Key: 0x0
Initiator: AIL-WLD-SYN02-ESX10_B (10:00:26:c5:21:20:00:4a)
        Target FC Interface: (Sant-nimble-9995 : A : fc1a.1) (56:c9:ce:90:5a:52:14:01)
        ALUA: active/optimized
        PR Key: 0x0
        Target FC Interface: (Sant-nimble-9995 : B : fc1a.1) (56:c9:ce:90:5a:52:14:09)
        ALUA: standby
        PR Key: 0x0
Initiator: SIL-WLD-SYN02-ESX09_B (10:00:9a:92:49:a0:00:4a)
        Target FC Interface: (Sant-nimble-9995 : A : fc1a.1) (56:c9:ce:90:5a:52:14:01)
        ALUA: active/optimized
        PR Key: 0x0
        Target FC Interface: (Sant-nimble-9995 : B : fc1a.1) (56:c9:ce:90:5a:52:14:09)
        ALUA: standby
        PR Key: 0x0
Initiator: SIL-WLD-SYN02-ESX10_B (10:00:9a:92:49:a0:00:4e)
        Target FC Interface: (Sant-nimble-9995 : A : fc1a.1) (56:c9:ce:90:5a:52:14:01)
        ALUA: active/optimized
        PR Key: 0x0
        Target FC Interface: (Sant-nimble-9995 : B : fc1a.1) (56:c9:ce:90:5a:52:14:09)
        ALUA: standby
        PR Key: 0x0
Agent Type: none
Online Snapshots:
Application identifier:
Dedupe Enabled: Yes
Previously Deduped: Yes
Application Category: Other
Encryption cipher: none
```

```
IOPS Limit: unlimited

Throughput Limit (MiB/s): unlimited

Nimble OS $
```

This command output is only for example, in the future architecture we will provide the right information in the event of an audit.