
ORACLE®

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 Training Materials – Usage Agreement

Use of this Site (“Site”) or Materials constitutes agreement with the following terms and conditions:

1. Oracle Corporation (“Oracle”) is pleased to allow its business partner (“Partner”) to download and copy the information, documents, and the online training courses (collectively, “Materials") found on this Site. The use of the Materials is restricted to the non-commercial, internal training of the Partner’s employees only. The Materials may not be used for training, promotion, or sales to customers or other partners or third parties.

2. All the Materials are trademarks of Oracle and are proprietary information of Oracle. Partner or other third party at no time has any right to resell, redistribute or create derivative works from the Materials.

3. Oracle disclaims any warranties or representations as to the accuracy or completeness of any Materials. Materials are provided "as is" without warranty of any kind, either express or implied, including without limitation warranties of merchantability, fitness for a particular purpose, and non-infringement.

4. Under no circumstances shall Oracle or the Oracle Authorized Boot Camp Training Partner be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this Site of Materials. As a condition of use of the Materials, Partner agrees to indemnify Oracle from and against any and all actions, claims, losses, damages, liabilities and expenses (including reasonable attorneys' fees) arising out of Partner’s use of the Materials.

5. Reference materials including but not limited to those identified in the Boot Camp manifest can not be redistributed in any format without Oracle written consent.

ORACLE VM

ORACLE

Oracle VM 3 Protecting the VM Installation

Presenter's Name
Presenter's Title

ORACLE PARTNERNETWORK

Specialized. Recognized by Oracle.
Preferred by Customers.

Protecting Data:
Backup and Recovery Discussion

Backup Approaches – Option 1

Treat VMs as if they are physical machines

- Useful if VM cannot be suspended/shutdown before copy
- Backup agent/client is installed directly in VM guest - backup process similar to bare-metal deployment
- VM guest independently communicates directly with backup server
- Similar OS provisioning methods as bare metal/physical machines - imaging or scripted
- Drawback is typically decreased performance during backup/restore operations

Backup Approaches – Option 2

Treat VMs as files

- Useful if VM can be suspended/shutdown or in quiescent state before copy
- Backup/restore files via standard command line file management utilities, cp, tar, etc
- Backup can take a while to complete as usually an exact copy of VM image files stored elsewhere
- Drawback is that unchanged data will be unnecessarily duplicated in copy

Backup Approaches – Option 2

Treat VMs as files

- Note that there are some upcoming features with OCFS2 to allow snapshots, but at an image file level… think of them like hard links with copy-on-write support.
- For more information, do a Google search for OCFS2 and reflink.

Backup Approaches – Option 3

Volume (LUN) snapshots and clones

- Storage vendor snapshot functionality required – e.g., NetApp FlexClone/Snapshots
- Snapshot only takes a few seconds - snapshot points to original source data - no copy necessary
- VM can typically remain online - although VM flushes dirty pages to disk before snapshot taken

Backup Approaches – Option 3

Volume (LUN) snapshots and clones

- Oracle VM Server and Oracle VM Manager will be including Linux host based snapshot features in a future release
  - Independent of storage vendor
  - File backed snapshots via reflink on OCFS2
  - Possibly LVM snapshotting

Backup Approaches – Option 4

Built in backup tools

- Storage vendor software communicates with hypervisor and/or VM guest application
- For example, NetApp Oracle Backup and Recovery - NetApp appliance places VM guest database into “hot backup” state, takes volume snapshot, and then places database back into normal state. Access NetApp Snapshot copies via existing Oracle Recovery Manager (RMAN) software to recover data.
- http://www.netapp.com/us/solutions/applications/oracle/oracle-backup-recovery.html

Backup Approaches – Option 4

Built in backup tools

- In a future release of Oracle VM Manager, we plan to include a storage manager API for storage vendors where you can perform operations such as snapshots from the OVM Manager console.

Virtualization and Security Considerations

Areas of Consideration

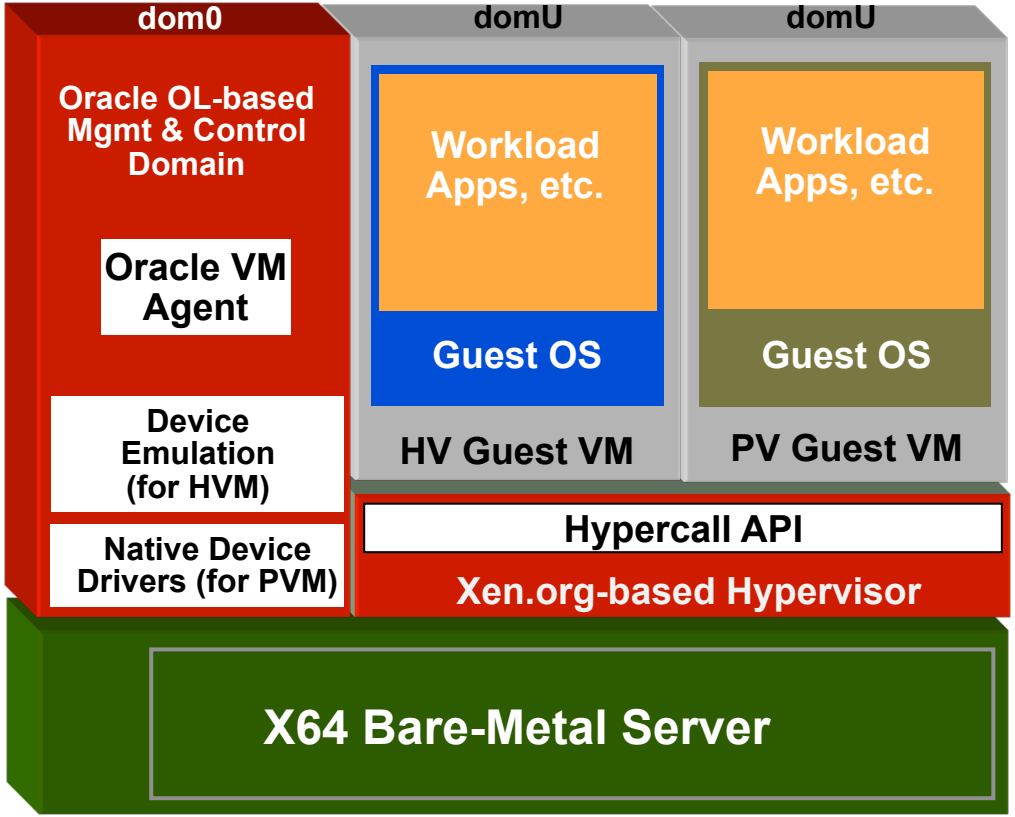
- Hypervisor's Role in Security
- Dom0's Role in Security
- Guest VM Security Considerations

Hypervisor Role in Security

Anatomy of Xen

Key Concept: Dom0

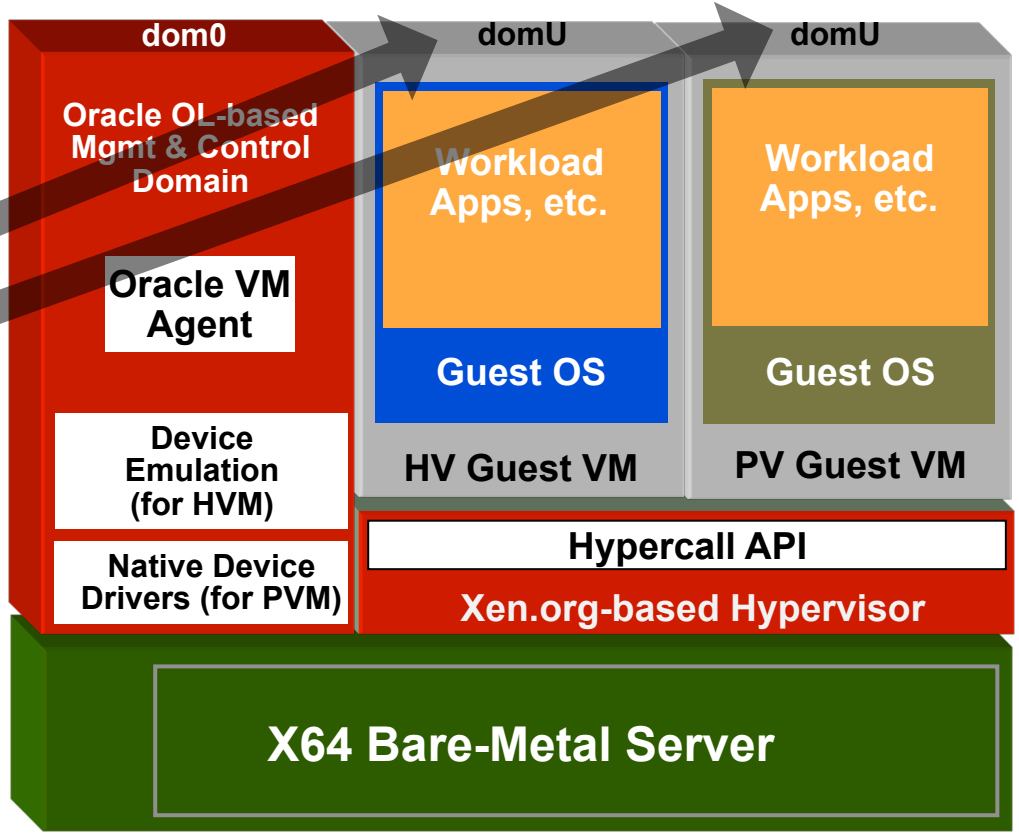
- **"Dom0"** is a privileged management and control domain containing…
  - A thin control kernel based on Oracle Linux (including UEK features)
  - Open / native Linux device drivers
  - Oracle VM Manager agent
  - Device emulation code to support non-PV guests (e.g. Windows)
- **Dom0 should *not* contain extra services or applications, as a best practice**
  - **Minimize performance & security risks**
  - **Minimize code size**



 |

Key Concept: DomU

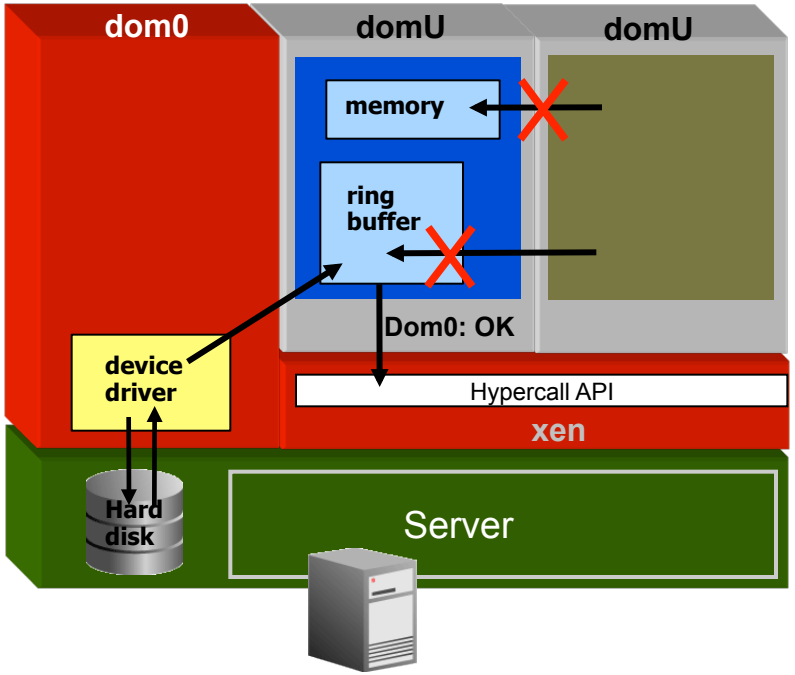
- **"DomU"** is an unprivileged guest domain that hosts a virtual machine on the server
  - Run any normal server workload
  - One domU is not aware of another



 |

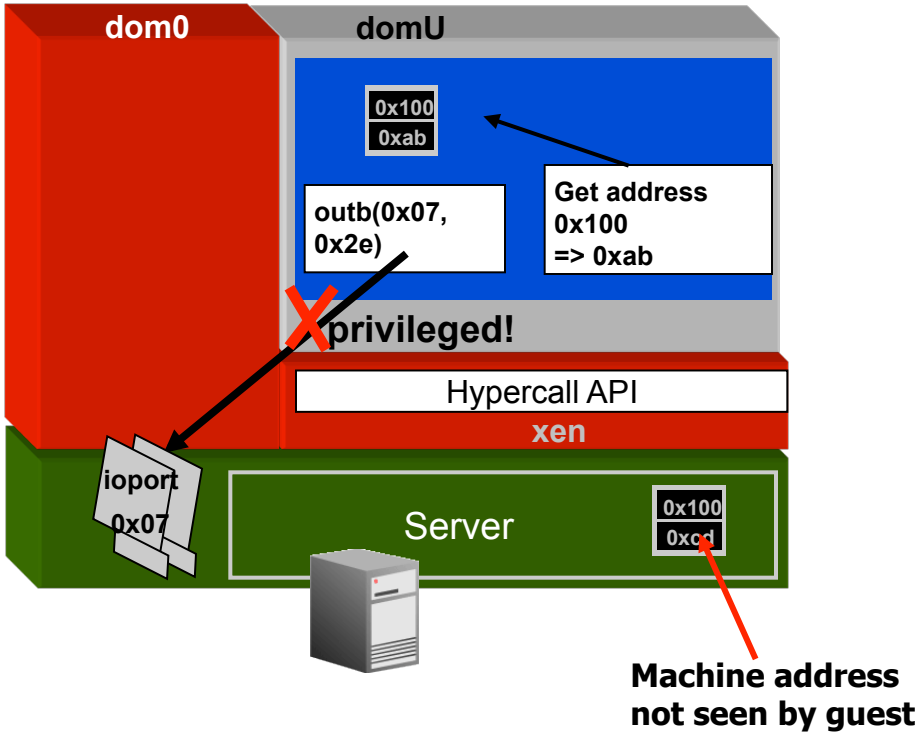
Guest-Guest Protection

- Memory access: protected by explicit sharing
- I/O isolation: hypervisor prohibits device access
- Point-to-point communication: access granted from one domain to another does not give access to all



Guest-Hypervisor Isolation

- Privileged operations are trapped
- Guest physical addresses are not machine addresses
- Narrow hypercall interface with aggressive checking



Hypervisor Security Considerations

- Control physical access: includes physical console (keyboard/serial), ipmi, sol, remote access cards (e.g. DRAC, ilo)
- Disable unnecessary boot devices: USB, PXE, virtual devices can be disabled if not needed
- TPM can be used for signed BIOS, bootloader, hypervisor and dom0, modifications to any of these will fail to boot and protect the system

More Hypervisor Security Considerations

- Stay current: use ULN to stay on top of CVE reports and fixes before exploits are developed
- Use trusted guest kernels
- Use only essential components (e.g. disable debugger from grub.conf if not debugging)
- Label-based security: an optional component to xen to allow fine grained access control to resources, enforced by hypervisor

Dom0 Role in security

Domain-0 Security

- Dom0 is very highly privileged
  - Able to create or destroy domains
  - Can request from hypervisor read-write access to guest memory for setup of console, debugger, etc.
  - Controls all I/O
  - Network accessible: for guest control, migration
- A compromised dom0 is more dangerous than a single compromised Linux host
- Most security considerations involve controlling access to dom0

Controlling Domain-0 Access

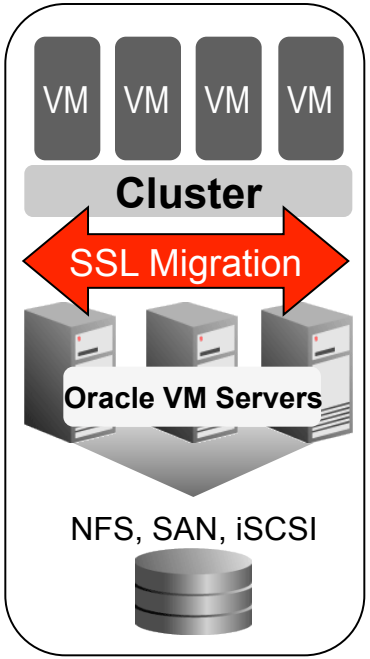
- Use same approach as for bare metal Linux security
- Stay up-to-date on patches!
- Control critical configuration files
- Small footprint: run fewest services possible, install minimal set of packages (Oracle VM)
- Use native (or commercial) logging and audit facilities
- Live migration can be used to keep guests running

Control Network Access to ovs-agent Service

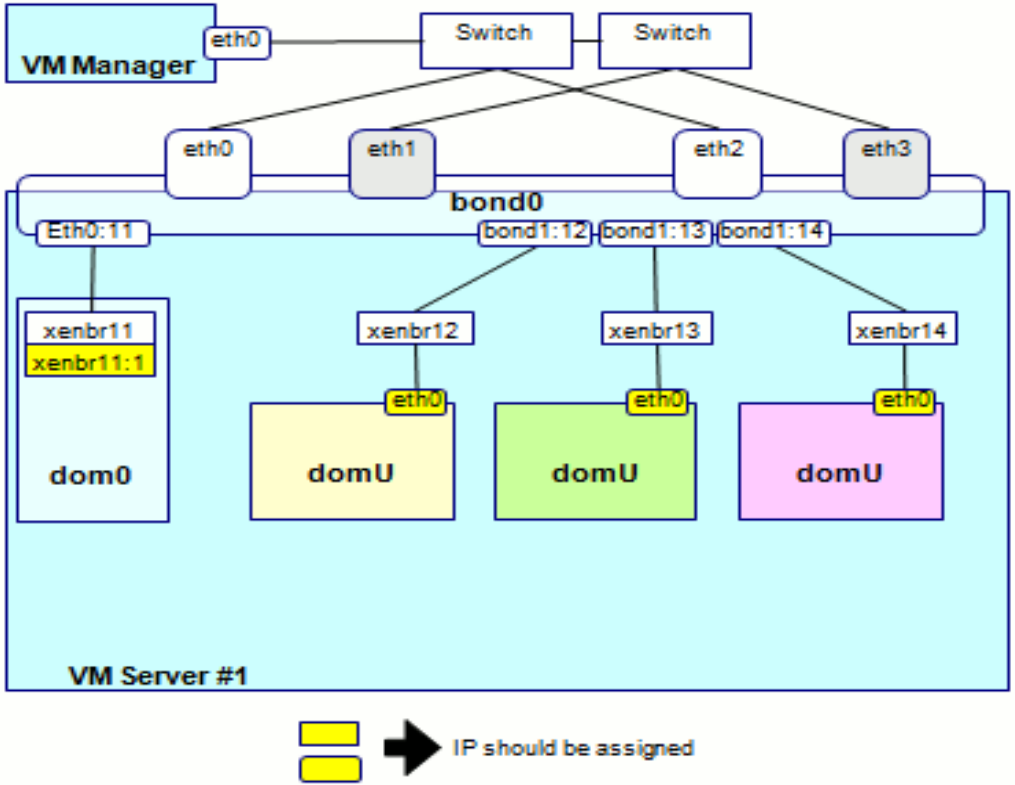
```
[root@xxxxx # service ovs-agent configure
;network access control by ip --
;rules := if addr.match(allow) and not addr.match(deny): return True
;pattern items delimited by comma and could be
;219.142.73.50   #single ip
;219.142.73.*    #range
;219.142.73.0/24 #range in CIDR format
;default to allow all, deny none
allow=*
allow=
now allow=*
deny=
deny=
now deny=
…
would you like to modify password to communicate with agent (local)?[y/N]
```

Dom0 Network Access

- Firewalling: use iptables to control individual services
- Isolate traffic: private networks can be used to make sensitive network loads (live migration) invisible to the public network
- Oracle VM uses SSL for live migration and agent communication, so public net can be used
- Use VLANs to separate guests from each other, or even from dom0



Bonding Network with VLAN Tagging



 |

Overview:
Effects on Guest OS Security

Virtualized Guest OS Considerations

- Set up security as if hypervisor were not present
  - Do not rely on hypervisor for security, configure network, devices, file system, etc. just like bare metal
- VLANs, bonding, multipathing can still be used in-guest
  - But take a logical approach: in-guest VLAN tag may conflict with bridge, bonded virtual interface might not have two physical paths, etc.
- Separate Ethernet bridges can be used for each guest to prevent any traffic flow

Security Advantages for the Guest OS

- Virtual hardware is constant
  - Required driver updates for physical devices affect dom0 but do not affect the guest; use live migration for full uptime
  - Rarely a need to upgrade an existing guest OS for new hardware support: eliminates instabilities and security holes due to OS patches
- "Gold images" change infrequently: reduces costly testing and validation, even when switching physical hardware vendors

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®