An Oracle White Paper
April 2012

Network Isolation in Private Database Clouds

Executive Overview

Cloud computing is emerging as an important IT strategy as enterprises strive to deliver more services to users across the network. Cloud computing is an architectural model that leverages standardization and consolidation to allow effective and safe sharing of pooled resources. However, sharing resources brings new challenges and considerations. There are several types of resources and operations that must be isolated between different tenants of a cloud.

This paper will focus on the options and features that can be used to provide network isolation in an Oracle Private Database Cloud configuration.

Different types of network isolation

In a cloud configuration tenants share the same underlying physical infrastructure. Without network isolation, tenants could intentionally or unintentionally consume a large part of the network, intrusively see data on the network that does not belong to them, or invoke side-channel tenant attacks. A proper network design that includes resource control and security ensures these issues are mitigated.

Cloud Providers typically want network isolation for resource management or network security. In most cases, these Cloud Providers choose to combine both as a means to satisfy tenant requirements.

Network Traffic Isolation

In a Cloud environment there may be cases where certain user traffic needs to be isolated on its own network. For example, traffic isolation can be used to provide an initial layer of security, higher bandwidth for specific tenants, implement specialized chargeback policies, or to support tiered networks. Other examples include isolating network traffic for LAN based backups, ftp, or replication traffic. In this paper we will focus on isolating database Sql*Net network traffic.

Network Security Isolation

Networks in a consolidated environment must ensure database traffic is secure and authenticated against trusted clients. Network security is built on top of network isolated traffic, and can be implemented using encryption (SQL*Net, TLS/SSL, or https) or authentication; i.e., allow or deny database service access using validation rules.

The following sections will cover the two different types of network isolation.

Network Traffic Isolation

Monitoring and controlling both physical and virtual network resources are key to understanding how bandwidth is being consumed. Cloud Providers must be able to:

- Identify bottlenecks to prevent network congestion and avoid downtime
- Establish network service-level agreements (SLAs) and meet network quality of service (QoS) goals
- Understand network traffic trends and consumption in order to charge for network-related services
- Gather security information that could help prevent denial of service attacks (DoS)

The first aspect of network traffic isolation is the creation of segmented networks. This can be done physically, or logically. In physical network isolation, network interface cards will be dedicated to a specific application or group of applications, and thus physical segmentation is provided between networks.

Logical network isolation uses software such as VLANs, network interface virtualization (vNICs), or multiple logical listening endpoints to partition physical network resources. Traffic for multiple applications share the same physical interfaces, but each application sees only the network traffic and resources assigned to it, and cannot see traffic or resources assigned to other applications.

The second aspect of network traffic isolation is resource control or Quality of Service management (QoS). This needs to be in place to monitor and manage network traffic, and ensure that tenants consume only their fair-share of network bandwidth. Network resource management is generally applied at the vNIC level, i.e., currently, there is no network governor that provides class of service (CoS) at the application or tenant level. Since vNICs are a tool for creating logical network isolation, network resource QoS is most practical with logical network isolation environments.
In this section, we will describe how network traffic bandwidth and network resource management are handled differently between the Private Cloud architectures.

Network Traffic Isolation in Database Cloud Configurations

In Database Cloud configurations, there can be multiple Oracle 11g Real Application Clusters (RAC) databases or a single RAC database to support multiple applications. Both implementations consist of one or more application specific RAC services, where these RAC services are typically serviced by a single database listener. The basic RAC configuration consists of a private network used for RAC Cache Fusion traffic and public network to carry all database client traffic. The database listener process listens on a well-known port for this public network traffic.

To provide public network traffic isolation in this scenario, Cloud Providers have three options: add extra network adapters; implement 802.1q VLAN tagging to create additional logical network interfaces (from physical interfaces); or create multiple database listeners. The first option has the advantages of increased network bandwidth with each additional network card, with the downside of extra cost. The second option is a cost-effective approach if the configuration is not already network bandwidth limited. In both cases, an additional VIP and secondary database listeners that listen on that VIP address must be created to support the isolated user traffic.

The third option is to setup logical networks to create multiple database listeners from a single (physical or logical) network, with each listener listening on a separate port and network.

Network resource management in this configuration is maintained and handled at the network switch layer. Figure 1, below describes the network topology in the Database Cloud configurations. This configuration consists of three nodes in the Cloud Pool, with private interconnect links as well four NICs, bonded, to form two separate public networks, representing isolated paths.

Note: clients that access the default listener can leverage SCAN addressing. However, SCAN exists only for the default listener, thus clients using the secondary networks (listeners) must use connection methods available prior to 11gR2, such as the tnsnames.ora address list or EZConnect method.

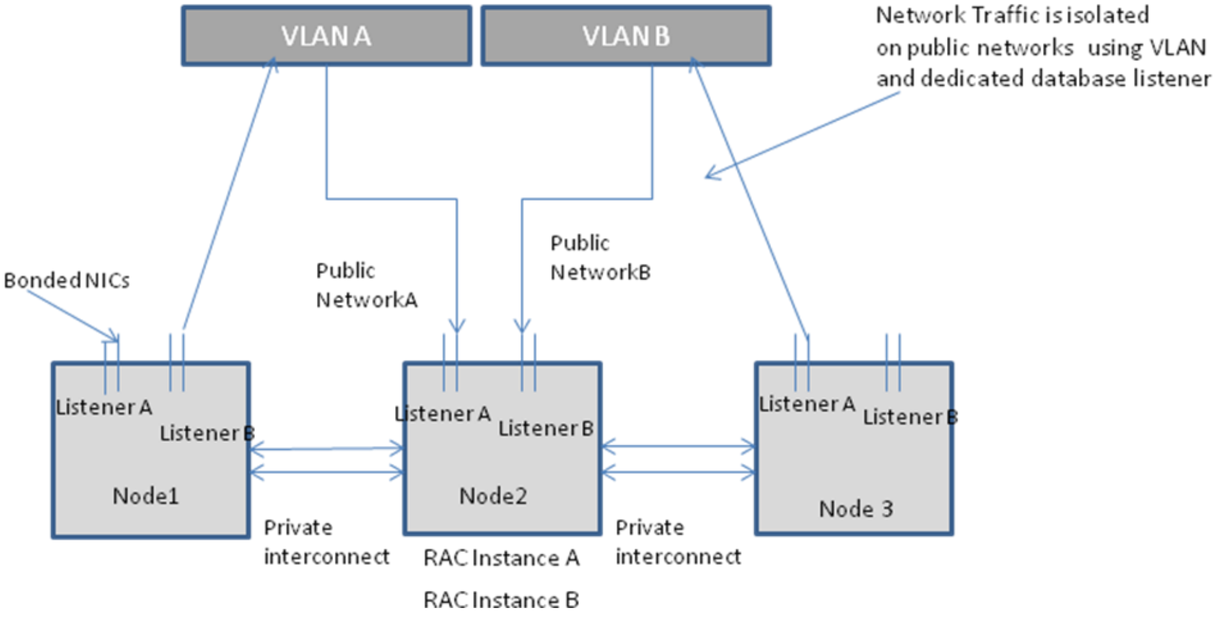


Figure1. Network topology in DB Cloud Configurations

Network Traffic Isolation in Hypervisor-based Cloud environments

In a hypervisor-based virtualized environment, the host server includes one or more network interfaces. These physical network interfaces (pNICs) can be bonded and presented as multiple virtual network interfaces (vNICs) to guest OSes (VMs). However, each vNIC interface is assigned a unique IP and MAC address, thus each vNIC is logically distinct. The hypervisor's driver domain (dom0) controls all packet ingress/egress guest traffic through a bridge. This bridge effectively acts as a layer 2 switch, passing packets accordingly and appropriately keeping network traffic isolated and secure.

Additionally, VLAN tagging can be defined in the host server to further isolate network traffic. Packets sent by a vNIC on a VLAN cannot be seen by vNICs on other VLANs. Furthermore, broadcast and multicast packets sent from one vNIC on a VLAN will be distributed only to the vNICs on the same VLAN.

The hypervisor via dom0, also has the capability to manage network Quality of Service (QoS) on a per-VM basis, thereby placing resource controls on network bandwidth. For added network isolation, VMs can have dedicated physical network interfaces; however, this reduces the core benefits of virtualization.

Figure 2 below describes the network topology in a hypervisor-based cloud configuration. This configuration consists of three nodes in the server pool. Each host server has five bonded NICs to form four separate public networks and one private network. Dom0 (the driver domain) has a single bonded vNIC dedicated for Live Migration and other host network activities. The host server also houses three user domains (Dom1-3) each created with two vNICs connected into two different VLANs, representing isolated paths

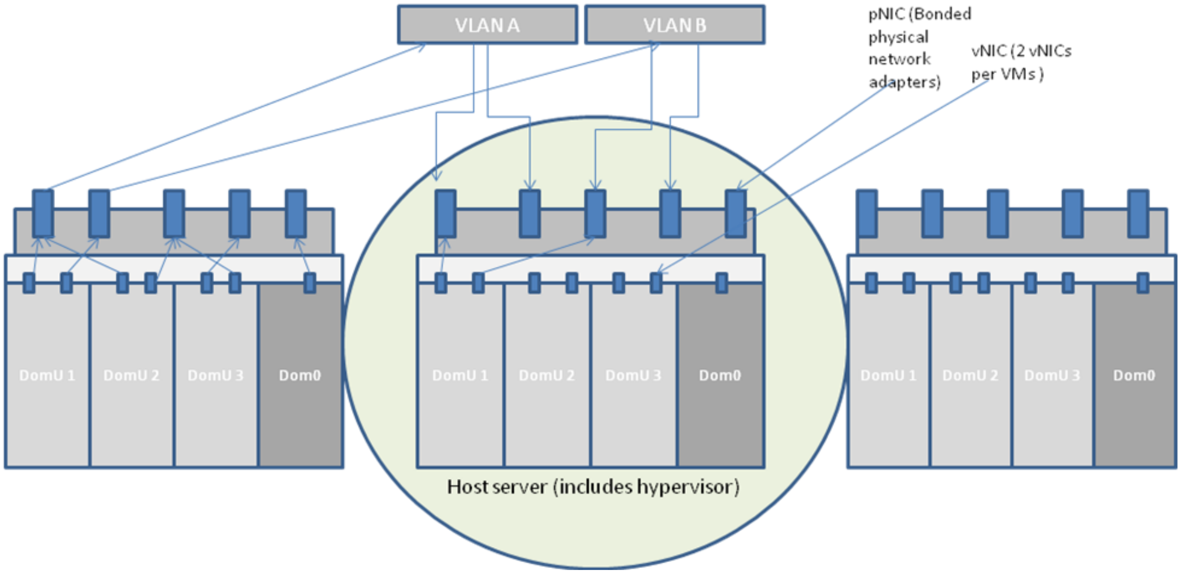


Figure2. Network topology in the Hypervisor-based Cloud configuration

Network Traffic Isolation in Solaris Zones-based Cloud environments

Solaris 11 (S11) introduces several networking enhancements. These features provide full network virtualization, fine-grained network resource management and monitoring, and increased performance to leverage modern servers and NICs. These S11 capabilities and features are available on bare-metal systems as well as in virtualized Zone configurations.

This section will discuss Solaris 11 network virtualization in Solaris Zones configurations. Solaris Zones act as completely isolated virtual environments within a single operating system instance.
There are two types of zones: global and non-global. Global Zones are analogous to dom0 described in previous section; Non-global zones (local zones) are provisioned from Global Zones, analogous to user domains. Global zones present system resources to non-global zones.

Similar to hypervisor-based virtualization, when a zone is provisioned one or more vNICs are presented and the IP stack is enabled. The IP and MAC addresses are configured on the logical interface (vNIC). Routing policies and network security can be hardened in these zones when the zones are provisioned. This closes potential security holes when the network is administered by the local zone's root user.

S11 provides the capability to set bandwidth limits for specific NIC ports or vNICs; this effectively configures the link speed of vNICs that are assigned to zones, ensuring that one interface does not exceed its expected use of the network, and negatively impact other traffic. Bandwidth can also be assigned to vNICs to make certain that each vNIC will have a minimum bandwidth available, regardless of the bandwidth usage of other virtual machines sharing the same physical NIC. Note that bandwidth limits should be assigned with some care to ensure that the sum of the vNIC bandwidths reasonably matches the physical bandwidth of the underlying physical NIC.

Network resource control is further managed by assigning CPU resources to a NIC port or vNIC, such that greater CPU resources are allocated to high priority and high bandwidth traffic while more limited resources are assigned to low priority traffic. This capability functions in conformity with Oracle Solaris Zones and CPU pools. If a CPU pool is assigned to a zone, then vNICs defined for that zone will inherit the same pool, and CPU resource limits placed on the vNIC will be from that CPU pool.

Figure 3 describes the network topology in Solaris 11 Zones configurations. This configuration consists of three nodes in the server pool. The Global Zone has three bonded NICs to form two separate public networks and one for the private interconnect. The Global Zone also has two local zones with three vNICs per zone, connected into two different VLANs, representing isolated paths.

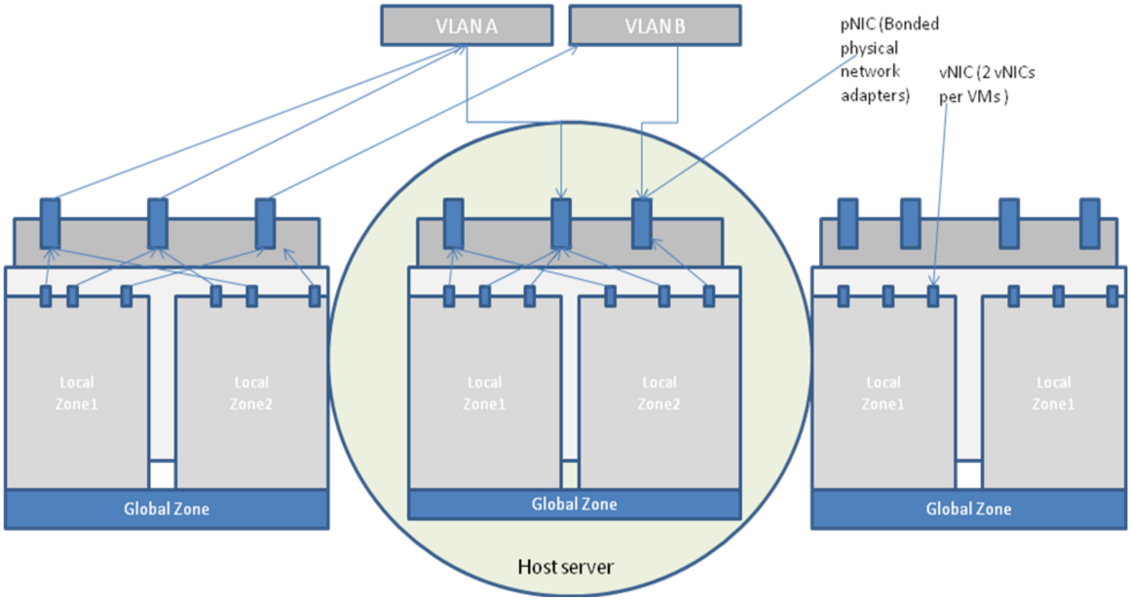


Figure3. Network topology in the S11 Zone-based Cloud configuration

The following table describes the features and technologies available to provide network traffic isolation.

FEATURES	ISOLATION CAPABILITY
Physical segmentation	Uses separate network interface cards to carry traffic for logically grouped applications. Note that all network traffic is still carried across the same set of enterprise switches and router, thus network convergence still exists. To have a completely isolated network, a silo'ed network with separate networks and routes needs to be in place. A completely isolated network is not recommended as it does not promote optimal sharing of cloud resources and adds significant management overhead.
vNICs	In virtualized environments, a physical NIC is divided into multiple virtual interfaces (vNICs) to create kernel isolated and dedicated network stacks. These physical network interfaces can be presented as vNICs and shared between one or more VMs. However, each vNIC interface is assigned a unique IP and MAC address, thus from a layer 2 perspective each vNIC is distinct. In Solaris 11 environments, vNICs can be created in both bare-metal and virtualized configurations.
VLAN (802.1q)	A virtual LAN (VLAN), as specified by the IEEE 802.1q standard, is a method for segregating network traffic within a bridged LAN infrastructure. VLANs allow two logically separated networks to use the same physical medium, while not allowing them to intercommunicate without a layer 3 device (router). This VLAN configuration is done at the switch and defines mapping between VLANs and ports. This configuration also allows Quality of Service to be implemented at the switch layer.

Note that some of the features listed above can be used together. For example, bonded vNICs can be VLAN tagged to provide greater isolation. Thus, in an environment with switches and routers that support VLANs, end–to-end traffic can be isolated, even though the traffic may be running on a shared physical link.

Network Security Isolation

With compliance mandates and regulatory requirements, network isolation along with network security have become essential elements of any cloud deployment. The technology used for network traffic isolation, discussed in the earlier section, does not cover issues with security breaches that stem from external networks, side-channel attacks, or regulatory concerns between tenants. In addition to network security, Cloud Providers must ensure that other aspects of security, such as OS and database security are also in place. As part of enterprise network security and 'secure by default' framework, customers generally have standardized on the following network security solutions:

- Network Firewall – Also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, and are often situated at the borders of networks as a way to filter potential security threats coming from untrusted sources. A DMZ is a firewall configuration. Incoming data packets are blocked unless they match the established and configurable rule sets. Network firewalls may be hardware devices, software such as soft switches, or a combination of the two.

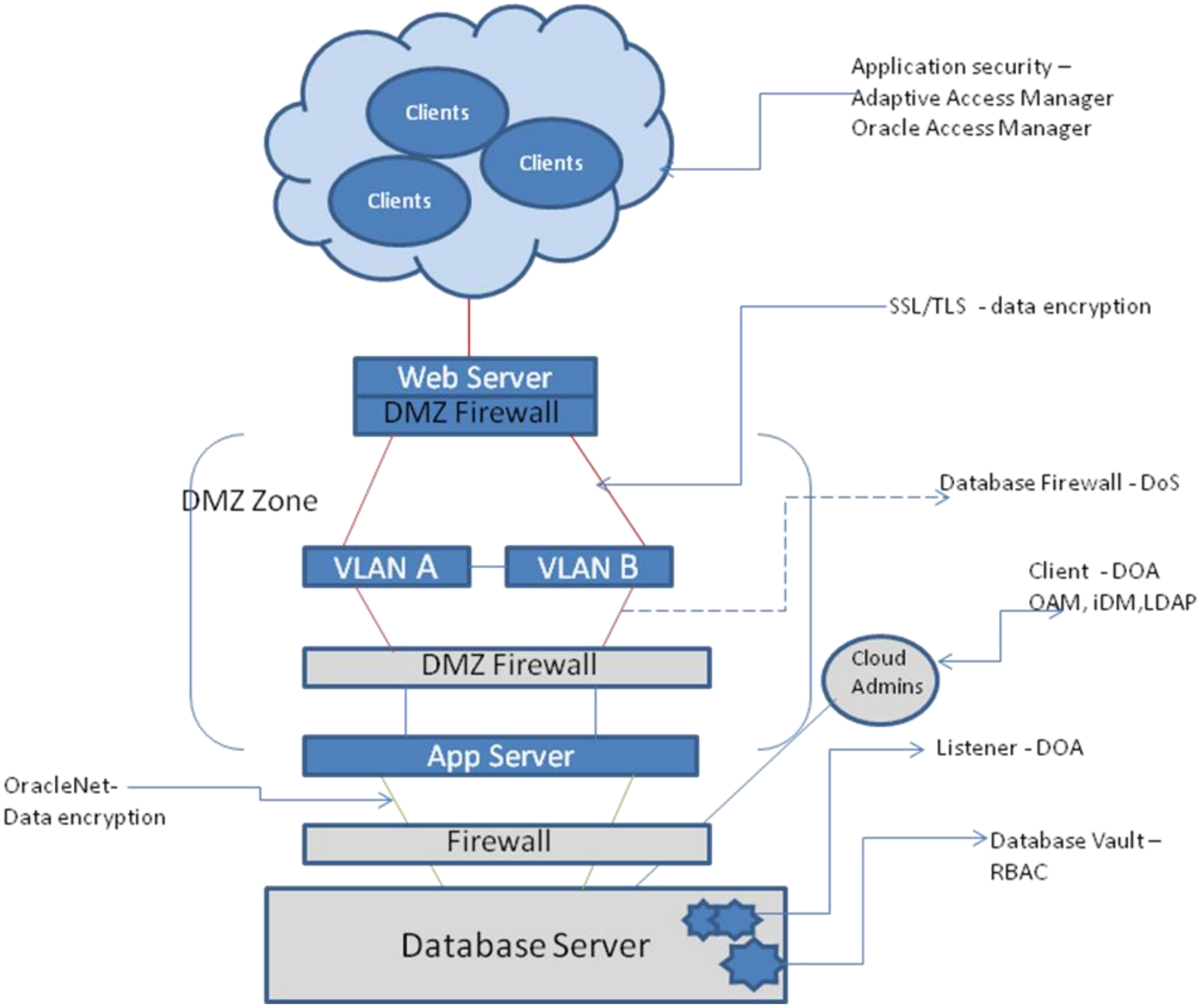
- VLAN Tagging - VLANs allow multiple logically separated networks to use the same physical medium, thus two separate VLANs cannot communicate with each other without a layer 3 device (router). This VLAN configuration is done at the switch and defines mapping between VLANs and ports. VLANs created over vNICs provide an extra layer of security and bandwidth control. Packets sent by a vNIC on a VLAN cannot be seen by vNICs on other VLANs, and broadcast and multicast packets sent from a vNIC on a VLAN will be distributed only to the vNICs on the same VLAN. Typically vNICs will be used in conjunction with VLANs. However, customers have fears of packet leaks from one VLAN to another (revealing sensitive information), or a specially crafted packet that is injected into another VLAN. There are features that mitigate this risk. For example, Solaris 11 ensures that VLAN tagging is performed in the global zone; i.e., the local zone's vNICs are not exposed to VLAN ids and headers and thus cannot send packets which contain VLAN headers. NIC classification also ensures that a zone will receive packets only from the VLAN it belongs to.

- Role Based Security – A sound network security architecture requires a solid "endpoint security" (client workstation and database server) design. On the client side, the workstation or mobile devices must have hardened user authentication. Additionally, application-based authorization and authentication ensures clients have only the required access to the application. On the database server, Role Based Security, or Role Based Access Control (RBAC), needs to be employed. Oracle Database Vault's RBAC approach extends the database's native "least privileges approach" to security by employing a fine grained authorization to database objects.

There are various tools and features offered by the Oracle stack that also provide a deeper level of network security. These network security solutions can be divided into three areas: features that validate data origin authentication (DOA), provide in-band data security, and prevent denial of service attacks (DoS). Many of these products work at different layers of the network path. Cloud Providers should determine which features make business sense based on existing architecture and standards. For example, it is generally considered a best practice to stop DoS attacks at the edge of the network, i.e., closest to the source of the attack.

The following table describes tools and features available to provide a secure cloud environment.

Feature	Capability
Oracle Adaptive Access Manager Oracle Identity Manager-LDAP	Application-based security ensures clients are authenticated and authorized. This can be integrated with LDAP. Clients are authenticated before connection to the server or database. This authentication / authorization can include RAC service. This authentication is essential for server-side and database access.
Oracle Database Firewall	An out-of-band SQL traffic monitor that provides real-time monitoring of SQL database activity on the network. Uses SQL grammar-based technology to block unauthorized transactions from reaching the database. Also, restricts access to the database based on client's source network location. This feature also provides mitigation and prevention of DoS attacks. Additionally, Oracle Database Firewall combined with 3rd party technologies such F5 BIG-IP Application Security Manager (ASM) provides two-tier, edge-of network protection and secure database traffic protection.
Oracle Advanced Security Option - Network Encryption	Supports authentication by using digital certificates over SSL in addition to the native encryption. Provides functionality to secure communications between clients and servers. SSL features can be implemented standalone or in combination with other Advanced Security authentication supported methods e.g., encryption provided by SSL in combination with the authentication provided by Kerberos. It is recommended to enable SSL encryption between clients and the App Server, in conjunction with Sql*Net encryption between the App Server and the DB Server.


Clients
Clients
Clients
Application security –
Adaptive Access Manager
Oracle Access Manager
SSL/TLS - data encryption
Web Server
DMZ Firewall
DMZ Zone
Database Firewall - DoS
VLAN A
VLAN B
Client - DOA
OAM, iDM,LDAP
DMZ Firewall
Cloud
Admins
App Server
Listener - DOA
OracleNet-
Data encryption
Firewall
Database Vault –
RBAC
Database Server

Use Case Scenario

ACME Cloud Incorporated plans to build a database cloud to support hundreds of internal applications used by several internal LOBs and external partners. ACME Cloud must isolate the network traffic of each LOB and external partner to provide resource isolation and monitoring, and to prevent any visibility among different clients. Additionally, several applications have specific security compliance requirements which require special consideration.

ACME Cloud has a standard policy in place to deploy a DMZ between the web server tier and the application server tier; and another DMZ between the application server and the database server tier. Additionally, VLANs are implemented throughout the network configuration.

In order to minimize the number of topologies deployed and still meet the compliance-related requirements, ACME Cloud decided to create two database cloud pools: one for internal LOBs and one for external partners. Both cloud pools were based on the Database Cloud architecture model. All middle tier, application tier and web servers were deployed on hypervisor-based virtualized environments.

- The LOB cloud pool was a four-node RAC cluster in which each LOB was represented as a schema in one database. Since there was no compliance regulated data in any of the LOB schemas, no encryption was implemented; however, Database Vault security realms were put into place. From a network isolation perspective, a bonded 10GBe network was used to support all the internal user traffic

- For the cloud pool hosting the external partners, a database was provisioned for each partner logically grouped based on purchased-tier support. This cloud pool has two quad GbE cards, totaling eight physical un-bonded or 4 bonded networks. All applications that require strong data security requirements are grouped together to run database traffic over a specific network interface, providing service-to-network-to-client routing. This traffic is Sql*Net encrypted between the WebLogic App Servers and the database servers using Oracle Advanced Security Option. The external partners can optionally implement SSL encryption between clients and the web servers. Additionally, there is a DMZ between the web servers and application servers. For the traffic that does not need data security, Oracle Database Vault realms and connect command rules are implemented to validate client authentication.

Conclusion

In consolidated, multi-tenant configurations such as Private Database Clouds, tenant isolation becomes a very important aspect of the architecture. Proper isolation enables the fair and secure use of the environment's shared resources. Without proper isolation, tenants may intentionally or unintentionally abuse shared resources or compromise security of their neighbors.

Physical and logical isolation techniques are available to provide varying degrees of isolation. The level of isolation to deploy will largely depend on individual tenant requirements and the relationships of the tenants being consolidated together. This paper addressed the technologies and techniques available to Database Cloud Providers to implement end-to-end isolation for networking traffic.

For More Information

TOPIC	URL
Database Consolidation onto Private Clouds	http://www.oracle.com/us/products/database/database-private-cloud-wp-360048.pdf
Best Practices for Database Consolidation in Private Clouds	http://www.oracle.com//technetwork/database/focus-areas/database-cloud/database-cons-best-practices-1561461.pdf
RAC Network Requirements	http://docs.oracle.com/cd/E11882_01/rac.112/e17264/preparing.htm#TDPRC123
Securing the 11gR2 Network	http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_network_secure.htm
SSL and Firewalls with 11gR2	http://docs.oracle.com/cd/E11882_01/network.112/e10746/asossl.htm#ASOAG9679
11gR2 Listener Security	http://docs.oracle.com/cd/E11882_01/network.112/e16543/guidelines.htm#DBSEG504
Customizing the 11gR2 Listener	http://docs.oracle.com/cd/E11882_01/network.112/e10836/listenercfg.htm#i483130
Configuring multiple 11gR2 Listeners	http://docs.oracle.com/cd/E11882_01/network.112/e10836/concepts.htm#NETAG178
Oracle Database Vault	http://docs.oracle.com/cd/E11882_01/server.112/e23090/dvintro.htm#DVADM001
Configuring Oracle VM Server Management on a VLAN	http://docs.oracle.com/cd/E26996_01/e18549/ch05s10s04.html
Oracle Solaris 11 Networking	http://www.oracle.com/technetwork/server-storage/solaris11/documentation/o11-137-s11-net-virt-mgmt-525114.pdf
Application Traffic Restriction on Solaris 11	http://www.oracle.com/technetwork/articles/servers-storage-admin/o11-095-s11-app-traffic-525038.html

ORACLE®

Oracle is committed to developing practices and products that help protect the environment

Network Isolation in Private Database Cloud
April 2012
Author: Nitin Vengurlekar
Contributing Authors: Burt Clouse, Raj Kammend

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together