An Oracle White Paper
July 2012

Security in Private Database Clouds

Executive Summary 3

Commonly Accepted Security Practices and Philosophies 4

Principal of Least Privilege 4

Defense-in-Depth 4

Private Database Cloud Security Issues and Threats 5

Tenant Security in Private Database Clouds 7

Enforcing Security in a Private Database Cloud 8

Three *A*'s: Authentication, Authorization, and Auditing 9

Compliance Regulations and Oracle Security Products 10

Conclusion 12

For More Information 13

Executive Summary

As Cloud Computing has evolved and matured, it has sparked growing interest from the enterprise market where economic pressures are challenging traditional IT operations. Many companies and governments are being faced with growing IT costs that originate from multiple sources such as legacy systems, software licensing, power consumption, and operating overhead. These growing costs are exacerbated by the inefficiencies in traditional IT organizations such as project-based funding, underutilization of resources, lengthy manual provisioning times, and organizational silos. Cloud Computing is focused on addressing these issues by reducing costs through better standardization, higher utilization, greater agility, and faster responsiveness of IT services.

However, a high-priority concern for many enterprises in embarking on a Private Cloud journey is security of the infrastructure itself and the information stored and processed by that infrastructure. Particularly for firms in domains with a high level of regulation and/or sensitive customer data, Cloud consolidation strategies and self service capabilities can pose significant challenges. Balancing rich mechanisms for identity and access management with convenience features such as single sign-on is a must for Cloud environments.

Securing information and software assets in the Cloud can be problematic, especially in public Cloud environments where the systems are not directly controlled by the data owners. Private Clouds reduce some of the risk because the environments are housed within an organization's walls, although the issue then becomes one of securing the critical data from other departments or sub-organizations.

Several deployment models are available for Private Database Clouds. This paper will be focused primarily on the security risks, mitigations and commonly accepted practices that apply to Database Consolidations in which multiple databases are consolidated on a single pool of resources, also known as a Cloud Pool. Please review the Private Database Cloud Overview for details on architecture and terminology.

Commonly Accepted Security Practices and Philosophies

Principal of Least Privilege

The principle of least privilege is the practice of limiting access to the minimal level, yet still allowing the application to function normally. For example, application owners and administrators should have access only to the data, applications, and systems and privileges necessary to perform their duties. This approach provides better stability and more predictable behavior; e.g., unauthorized users cannot purposely or accidently remove privileged files or stop critical processes. Additionally, least privileges also improves mean time to deploy applications, since fewer privileges or roles need to be implemented.

However, least privilege principle is one of the most difficult philosophies to implement. Organizations must have knowledge of the following to successfully implement least privilege principle:

1. Classification of data
2. Knowledge of where their sensitive data resides
3. Solid automation for user access lifecycle management

Although these philosophies apply to general application deployment, least privilege principle becomes even more important and relevant in the Cloud, as tenants will require certain level of security isolation.

Defense-in-Depth

Defense-in-depth is the practice of using controls at all layers of the information architecture. In Cloud architectures, the need to follow this philosophy is even more important. The areas of focus include hardware (physical access), operating system, hypervisor, virtual machines, storage, database, application servers, applications, networks, consumer portals, and the interfaces for Cloud automation and management. One of the primary architecture design goals should be to separate production from development environments. In a traditional architecture, this is done using distinct servers, storage systems, and network subnets. In Cloud architectures, using Cloud Pools is becoming an accepted method for achieving this goal. Cloud Pools can by separated by data sensitivity, line of business, and/or classification of users accessing it. A Cloud Pool is used to refer to a common set of resources shared by tenants. In this paper a Cloud Pool refers to an Oracle RAC Cluster.

Private Database Cloud Security Issues and Threats

With the convergence of technology that represents current Cloud initiatives come different threats. Complicating this is the fact that traditional perimeters of the infrastructure change in a Cloud environment, trust boundaries may be modified as well as the rate of change and level of scale one typically finds in a Cloud environment. Specifically, these contribute to the complexity of managing the Cloud infrastructure which in and of itself may be considered a risk. We can state that the velocity of change in a Cloud is proportional to the velocity of attack, i.e., as the rate of change increases the potential for threats manifesting themselves also increases. Such threats are typically linked to the management of the Cloud infrastructure. Most importantly, these are all manageable with current security and governance processes and controls. The following is a sampling of potential threats that one may encounter in a Cloud environment.

Side Channel infiltration

The multi-tenancy or proximity of systems in conjunction with an improperly secured Cloud environment may increase the risk to data or system corruption from adjacent systems and applications. Such threats can be addressed by utilizing a strong security architecture that implements a secure by default security policy, system hardening and strong compartmentalization.

Data leakage

As with existing IT systems, there is always the possibility of data leaking or being disclosed between tenants running on a Cloud system. The remedy here is to ensure that appropriate controls are put in place, such as data encryption or access control mechanisms. In a Cloud environment, we could further state that data leakage may be possible by leaving data remnants in memory or on disk after a de-provisioned database service. One approach to addressing this threat is to ensure a consistent data scrubbing process is implemented. Likewise, a Cloud environment must ensure that no data leakage can occur between different tenants. Depending upon the criticality of the data, one practical method of protecting remnant information is to physically isolate the deployments and restrict access to those deployment environments where the remnants may reside. This is no different from non-Cloud architectures.

Attack platform / threat amplification

An improperly secured Cloud environment can be a point from which various inter/intra system attacks can be launched to either co-tenants or external systems, thereby causing a potential cascading failure of multiple systems that are co-tenants. Threat amplification means that a problem propagates faster and farther through a Cloud environment than it would under alternate circumstances (i.e., in a non-Cloud environment). This also has the effect of potentially reducing a timely response to and recovery from the threat. This challenge can be addressed by ensuring that comprehensive and well managed security and governance processes are in place to detect, manage and correct threats before they go viral and spread.

Distributed Denial of Service (DDoS) attacks

A denial of service (DoS) attack is an incident in which a user or application becomes unavailable or non-serviceable because it is deprived of the resources necessary operate. A distributed denial-of-service (DDoS) is a large DOS attack comprised of a large number of compromised systems attack a single target. A DOS/DDoS involves a loss of service or business function, such as customer facing websites, email, or networks. DDoS attacks may be launched against a Cloud environment that can result in the loss of access to or exhaustion of some resources or services so that the systems underperform or become unusable. Such threats can be addressed by proper system resource monitoring and management, replication of systems and failover processes. A common DOS attack is the Buffer Overflow Attack. Note that DoS attacks generally do not usually result in the theft or loss of business data; however, it can cost the companies businesses and credibility.

Complexity

Complexity is an inherent and potential threat in any computing environment. As complexity grows, so do the security risks: more components mean more attack surfaces and more interactions among components. When a system environment includes a variety of configuration and components (e.g., multiple O/S versions to maintain, multiple vendors to track, etc.), the management of the components is more difficult.

Oracle's Private Database Cloud methodology reduces complexity by emphasizing a rationalized, standardized environment. With less variety to manage, each component can be given more detailed attention. Furthermore, when data stores are consolidated, their oversight is centralized, whereas in a silo'd environment there are more opportunities for data stores to fall outside of standard processes. Complexity can be further addressed through enforcement of strong security policies and procedures, along with standardized processes for provisioning users into the Cloud and decommissioning environments.

Tenant Security in Private Database Clouds

Security plays a critical role in shaping the details of Private Database Cloud architecture. Organizations must develop a clear understanding of security requirements, trust boundaries, and threat profiles. Database security includes a comprehensive approach for how, why, and by whom data is accessed. Further, organizations must understand how trust is established and propagated as well as how threats are mitigated across a Private Database Cloud environment. Organizations need to understand where and how security policy is defined, how access is managed, and how audit and compliance requirements are met given the distinct capabilities that providers and consumers have in a Private Database Cloud. Please review the following paper for details on the different Private Database Cloud Models.

Databases are at the core of Cloud environments because they generally contain the most sensitive and important information for both providers and consumers. As such, it is at the center of the defense-in-depth approach to security. If the database is locked down so only authorized access is permitted following least privilege, the risk of data loss or compromise is significantly reduced. Although this is not specific to Cloud environments, it becomes paramount in high consolidation density configurations, which is a typical configuration for Private Database Clouds.

The application's security Service Level Agreement (SLA) must be well defined before being migrated or provisioned into the Cloud. A security policy-based template can be used so that a consistent deployment strategy is used for the appropriate level of security SLA. For example, an application may have stringent security requirements, whereby its data cannot be co-mingled with other applications.

Multitenant Cloud security has always been a primary concern for any Cloud deployment. There are significant challenges that involve ensuring a good balance between maintaining corporate compliance and leveraging the cost benefits of a shared infrastructure model. Creating heavily isolated configurations for specific applications to meet compliance reduces operational efficiency and diminishes the overall value of a Cloud. In order to meet this challenge, the Cloud architecture must include, at design time, security policies for database provisioning, de-provisioning, and data access control.

Three approaches can be taken when provisioning databases to meet appropriate level of security SLA:

- Provision a separate schema and use Oracle Tablespace Encryption (TDE).
- Provision a separate database in the same Cloud Pool to host the application.
- Build a Cloud Pool specifically for applications that hold compliance regulated data by type.

Enforcing Security in a Private Database Cloud

Cloud providers must ensure that all aspects of security, such as infrastructure, O/S and database security are in place. The following table describes security scenarios and how each impacts Private Database Cloud deployments.

Security Isolation use case	**Security handling**
How can I prevent the Cloud DBA from accessing and viewing my data?	Database Vault using Realms should be used to protect application and schema data from unauthorized access. This will prevent access to user data from other tenants as well as DBAs.
How do I provide security isolation in my consolidated configuration?	Minimize access to the database server; i.e., Sql*Net Pipe only access. It is recommended to allow only Cloud DBAs have physical access to the database server. For those users who need server access, implement named user accounts for DBAs with sudo access for privileged commands. To further harden the system configuration, role based access control (RBAC) should be considered.
I have customer sensitive data. How can I ensure that I meet compliance regulations?	Transparent Data Encryption (TDE) addresses encryption requirements associated with public and private data privacy and security mandates such as PCI. PCI-DSS, PII, HIPPA dataset isolation can be handled in different ways, depending on security SLA defined or mandated by the business. Isolate customer sensitive datasets into their own set of tablespaces, and implement tablespace encryption.
Can I protect and secure my network traffic?	There are many different approaches to network data security, depending on what traffic needs to be secured and where that traffic is going. Oracle Database Firewall allows 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 as F5 BIG-IP Application Security Manager (ASM) provides two-tier, edge-of network protection and secures database traffic protection. Oracle Advanced Security Option - Network Encryption supports authentication by using digital certificates over SSL in addition to the native encryption. This provides functionality to secure communication 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 Application Server, in conjunction with Sql*Net encryption between the App Server and the DB Server. The following paper covers Network Isolation and Security: http://www.oracle.com/technetwork/database/focus-areas/database-cloud/ntwk-isolation-pvt-db-cloud-1587225.pdf

Three *A*'s: Authentication, Authorization, and Auditing

Part of the defense in depth approach involves the three *A*s: authentication, authorization, and auditing. Oracle offers a variety of products and features that address these three *A*s at various points of user data access. Cloud providers should determine which features or products should be implemented based on business needs or existing architecture and standards. The following are enabling technologies and features for Oracle Database Security:

Product	**Description**	**Authentication/ Audit/ Authorization**
Oracle Database Vault	Enforce least privilege access for privileged database users Enforce who, where, when, and how data can be accessed using rules and factors Prevent application by-pass and enforce enterprise data governance Restrict administrators from viewing data in the databases they manage Prevent ad hoc changes to the database by administrators	Authorization, Authentication
Oracle Audit Vault	Consolidate database audit from heterogeneous sources into a secure warehouse Alert on suspicious activity in near real time and drill down to the source Centralized audit policy management Out of the box compliance reports	Audit
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.	Authorization, Authentication
Oracle Label Security	Classify data based on which customer it belongs to Classify users based on their privilege level Database automatically classifies data as it is inserted Database enforces row level access to data	Authorization
Oracle Secure Test Data Management	Make application data securely available in non-production environments Prevent application developers and testers from seeing sensitive data Referential integrity automatically preserved so applications continue to work Works with Oracle and non-Oracle databases	Authorization
Oracle Database Firewall	Monitor database activity to prevent SQL injections Highly accurate SQL grammar-based analysis minimizes costly false positives Flexible SQL enforcement options based on white lists and/or black lists Scalable architecture provides enterprise performance in all deployment modes	Authorization, Authentication
Oracle Advanced Security	Encrypt application data at rest with tablespace transparent data encryption Encrypt database traffic on the wire Manage encryption keys with built-in key management Strong authentication of database users for greater identity assurance	Authorization

Feature	Description	
Secure Application Roles	Roles that are activated through a password protected procedure, so only the application can be granted the role. This prevents users that have both an apps account and database account from getting past the application security controls	Authorization
Virtual Private Database (VPD)	Record level security that only returns the authorized records when a request is made. VPD adds a predicate based on the policy for that table	Authorization
Proxy authentication	When a user of an application logs in, the user's credentials are passed to the database to be kept in the lightweight session context for auditing and reporting purposes	Authorization
Standard Database auditing	Captures audit information including failed database login attempts	Audit

Compliance Regulations and Oracle Security Products

The following table lists the various compliance regulations and how the Oracle Products/Features map to address those regulation requirements:

Regulation	Impact	Oracle Products
HIPAA	The Health Insurance Portability and Accountability Act of 1996 requires that all patient healthcare information be protected when electronically stored, maintained, or transmitted to ensure privacy and confidentiality. It also mandates that each user be uniquely identified before being granted access to confidential information.	**Oracle Advanced Security (ASO), Oracle Data Masking, Oracle Database Vault and Oracle Audit Vault, TDE**
Sarbanes Oxley	Sarbanes-Oxley Act of 2002 (SOX) requires public companies to validate the accuracy and integrity of their financial management. SOX requires that businesses not only document and assess their internal controls but also control access to financial systems. Section 404 covers internal control activities & compliance risks that can be addressed by identity and access management (IAM) solutions.	**Oracle DB Vault, ASO**
Gramm-Leach-Bliley	It mandates privacy and the protection of customer records maintained by financial institutions. These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusion	**Oracle DB Vault, ASO,TDE**

PCI/DSS	The Payment Card Industry (PCI) Data Security Standard contains 12 requirements grouped into six areas: build and maintain a secure network, protect cardholder, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy.	**Oracle DB Vault, ASO,TDE**
European Union (EU) **PIPEDA** **Data Protection Directive**	This directive outlines individuals' rights concerning their personal data. It is described as a stringent data privacy initiative, and the guidelines to ensure that data is transferred outside the EU only when it is adequately protected have extraterritorial implications for businesses.	**Oracle DB Vault, ASO,TDE**
California SB 1386	California SB 1386 requires companies to report security breaches involving private consumer information. Personal information is defined as Social Security number, driver's license or California ID card number, account number, or credit or debit card number in combination with a required security code, access code, or password that permits Access to an individual's financial account.	**ASO, TDE**
Massachusetts data protection law, 201 CMR 17.00	Massachusetts 201 CMR 17.00 mandates that "every person who owns, licenses, stores or maintains personal information about a resident of the Commonwealth [of Massachusetts] requires all persons and businesses with personal information to have an adequate protective system in place to prevent unauthorized access to personal information, firewall and malware protection for the computer systems, as well as encryption for all data containing personal information transmitted through the public network or wirelessly.	**Oracle DB Vault, Audit vault, Oracle Firewall**

Conclusion

Private Database Cloud architectures can provide significant benefits to an organization as long they are implemented and managed effectively and securely. In consolidated, multi-tenant configurations such as Private Database Clouds, tenant isolation becomes a very important aspect of the architecture. Without proper isolation, tenants may intentionally or unintentionally abuse shared resources or compromise security of their neighbors. Proper isolation enables the fair and secure use of the environment's shared resources.

Oracle's database security offerings allow organizations to standardize on a Cloud-based architecture for better utilization and improved efficiency, while providing an opportunity to identify, evaluate, and group data based on sensitivity and compliance requirements. The resulting environment allows for an efficient and consistent protection of data with better security and less complexity. The key benefits of these attributes are the faster certification of compliance by auditors as the tools that provide important information are available instantly and reliably.

For More Information

TOPIC	URL
Database Consolidation onto Private Clouds	http://www.oracle.com/us/products/database/database-private-cloud-wp-360048.pdf
Sustainable Compliance for PCI Standards	http://www.oracle.com/us/products/database/security-pci-dss-wp-078843.pdf
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
Oracle Database Vault	http://docs.oracle.com/cd/E11882_01/server.112/e23090/dvintro.htm#DVADM001
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

Security in Private Database Clouds
July 2012

Author: Nitin Vengurlekar
Contributing Authors: Burt Clouse, Raj Kammend, Tim Read, Troy Anthony, Steve Enevold, Joel Weise

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

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

Hardware and Software, Engineered to Work Together