Security guidelines for Oracle Database @Azure landing zone accelerator

This article explores specific design elements and provides targeted recommendations for Oracle Database@Azure workload security.

Overview

Most databases store sensitive data. To have a secure architecture in which to land these workloads, implementing security only at the database level isn't sufficient. Defense in depth is a comprehensive approach to security that involves implementing multiple layers of defense mechanisms to protect data. Instead of relying on a single security measure at a specific level, such as, for example, focusing on network security mechanisms, the defense in depth strategy employs a combination of different layer security measures to create a robust security posture. Defense-in-depth approach can be architected for Oracle workloads through strong authentication and authorization framework, hardened network security and encryption of data at rest and in-transit.

To learn more about Oracle Exadata security refer to Overview of Oracle Exadata Security and Security Features of Oracle Exadata Database Machine.

Design Considerations

Exadata Resource layered security

Exadata Database Service on Dedicated Infrastructure (ExaDB-D) are resources deployed in Azure vNet and as such a multi-layer approach for security is pertinent. Implementing security only at the database level isn't sufficient and layered security approach is recommended, in the section below we will address different areas where security should be addressed to ensure your data and databases are secured.

When deploying ExaDB-D there are two types of controls, the APIs to manage the infrastructure, these are local to Azure and executed based on the user/principal's permissions. The other type are DB management APIs that are executed in Oracle Cloud Infrastructure (OCI) and will have their own set of credentials and permissions that will be set up as part of the initial onboarding process.

Exadata network security

Exadata Database on dedicated infrastructure (ExaDB-D for short) is deployed in the customer vNet using virtual interfaces in the proper subnets. The ExaDB-D system consists of multiple database servers and storage servers, running Oracle Linux.

The Exadata Cloud Infrastructure utilizes different default ports for various operation, please review the below table for key ports that are used, for the full list and explanation please review the Oracle document here.

Protocol	Port Number	Service Name	Comments	Application
TCP	22	SSH	Management port for Linux Virtual Machines	SSH
TCP	443	HTTPS	Management Server (MS) on Exadata Storage Servers	Requests from ExaCLI and/or RESTful API calls. PDU Web interface
UDP or TCP	53	DNS	Database servers, Exadata Storage Servers	DNS (Domain Name System)
TCP	1521	Oracle Database listener	Client access to database servers	Client applications

The layered approach to network security consists of:

- control-plane security.
- vNet (data-plane) access security.
- ExaDB-D server access security.

To secure the control-plane it is important to use the principle of least privilege and to utilize Entra ID to manage the proper permissions and group access to the infrastructure and APIs controlling ExaDB-D. For data-plane and vNet access, it is important to allow only specific networks to access the data by limiting the sources IP range, allow only ports needed for secure communication, prevent any access

from and to the internet and use NAT in case it is required. Always encrypt data in transit (SSL). To secure ExaDB-D server access, utilize *SELinux* and *cellwall* service which enables firewall service on the servers.

Following the best practices of the shared responsibility matrix to secure the network traffic related to ExaDB-D:

- The control-plane, APIs to manage the ExaDB-D infrastructure in Azure or the Oracle databases in OCI, is encrypted in transit over SSL.
- The data-plane security, connectivity to the database itself and data operations, is the responsibility of the customer and should follow the least privileges permission model, encryption at rest and in transit and periodic rotation of encryption keys.

Exadata encryption and keys security

Exadata uses Oracle Cloud Infrastructure Vault (OCI Vault) to store and manage keys, you can choose to use managed keys or to bring your own encryption key the vault.

To note, in case you bring your own encryption key, the rotation of the key is managed by the user and is not automated by OCI Vault.

Vulnerability Scanning Overview

Oracle Cloud Infrastructure Vulnerability Scanning Service helps improve your security posture by routinely checking hosts and container images for potential vulnerabilities. The service gives developers, operations, and security administrators comprehensive visibility into misconfigured or vulnerable resources, and generates reports with metrics and details about these vulnerabilities including remediation information.

The Vulnerability Scanning service identifies vulnerabilities in the following resources:

- Compute instances (also known as hosts)
- Container Registry images

Design Recommendations

- Secure the Control Plane using the principle of least privilege and use Microsoft Entra ID to manage the proper permissions and group access to the infrastructure and APIs controlling ExaDB-D.

- Secure the data-plane and vNet access by limiting the sources IP range, allowing only ports needed for secure communication, preventing access from/to the internet (use NAT in case it is required), and always encrypt data in transit (SSL).
- Follow a shared responsibility matrix to secure the network traffic related to ExaDB-D.
- Use OCI Vault to store and manage encryption keys. If yoy decide to bring your own keys then set up a strict process for key rotation.
- Use the Vulnerability Scanning capabilities provided by Oracle to detect security issues such as ports that are unintentionally left open, OS packages that require updates and patches to address vulnerabilities and OS configurations that hackers might exploit and other vulnerabilities.