

Oracle Cloud Infrastructure Classic and Platform Cloud Services Security

ORACLE WHITE PAPER | NOVEMBER 2017





Disclaimer

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®



Table of Contents

Disclaimer	1
Table of Contents	
1. Introduction	1
2. Oracle Cloud Services: Built for Trust	4
3. Customer and Oracle Security Responsibilities	6
4. Oracle Cloud Infrastructure Security	8
5. Shared Identity and Access Management	14
6. Service-Specific Security	18
7. Oracle's Approach to Engineering Secure Cloud Services	39
8. Conclusion	40



Global spending on IaaS is expected to reach almost US\$16.5 billion in 2015, an increase of 32.8 percent from 2014, with a compound annual growth rate (CAGR) from 2014 to 2019 forecast at 29.1 percent, according to Gartner's latest forecast. [<http://www.gartner.com/newsroom/id/3055225>]

SUSAN MOORE
GARTNER

1. Introduction

The global spending on Infrastructure as a Service (IaaS) is growing rapidly. Still, many Chief Information Officers (CIOs) hesitate to fully embrace cloud infrastructure and platform services. Their uncertainty stems mainly from the anxiety over the security of their systems and data. CIOs want to build scalable hybrid cloud solutions while taking the necessary steps to secure their data across their enterprises. With the right security solutions and processes, even the most demanding enterprises can move to the cloud with confidence.

Oracle Cloud was developed to offer secure infrastructure and platform services that are used by Oracle customers to run their mission-critical enterprise workloads and store their data. Why are Oracle customers choosing Oracle Cloud solutions? The answer is simple. Oracle customers get a unique value from Oracle that isn't offered by other vendors:

- » Oracle offers the most complete portfolio of integrated infrastructure and platform services with depth and breadth of functionality.
- » Oracle Cloud offers a hybrid cloud, allowing easy management and monitoring of services from on-premises as well as easy migration of workloads.
- » Oracle Cloud solutions were built using standards-based technologies that customers are familiar with.

This white paper focuses on shared and service-specific security capabilities of the following services: Oracle Cloud Infrastructure Compute Classic, Oracle Cloud Infrastructure Object Storage Classic, Oracle Cloud Infrastructure Networking Classic, Oracle Management Cloud, Oracle Java Cloud Service, and Oracle Database Cloud Service – Enterprise Edition.

For a comprehensive list of the available Oracle Cloud services, go to <https://www.oracle.com/cloud>.

Oracle Cloud customers primarily want these security capabilities from Oracle:

- » **Control:** Security mechanisms to control who can access data and under which conditions

- 
- » **Auditing:** Ability to audit resources to maintain their security configuration
 - » **Visibility:** Logs providing visibility into accounts and resources
 - » **Assurance:** Ability to independently verify how data is being stored, accessed, and protected against unauthorized access and modification
 - » **Security:** Services that are designed, coded, tested, deployed, and managed securely
 - » **Out-of-the-box integration with existing Oracle technologies:** Seamless integration with existing Oracle solutions such as identity and access management

Security is a top priority for Oracle Cloud solutions. Oracle's vision is to create the most secure and trusted public cloud infrastructure and platform services for enterprises and government organizations. Oracle's mission is to build secure public cloud infrastructure and platform services where there is greater trust – where Oracle customers have effective and manageable security to run their workloads with more confidence, and build scalable and trusted secure cloud solutions.

Oracle has a strong security culture and formal security policies, and Oracle's products have been used by enterprises and government organizations over the last three decades for mission-critical applications across the world.

Oracle's security philosophy is built around the following approaches:

- » Oracle's preventive strategy is based on defense-in-depth. Oracle believes that there is a need to drive down the perimeter and add security controls closer to the data.
- » In addition to having a defense-in-depth preventive strategy, Oracle continues to develop strong and effective processes for breach detection, incident response, and effective remediation.
- » Oracle is working to define security and trust models which work well for cloud computing. For example, Oracle believes that the traditional administrator model based on the powerful, full-privileged administrator concept should be replaced with a model that places more power with the customer. Oracle should manage only the infrastructure objects, and doesn't have any channels to access customer data.

Oracle employs some of the world's foremost security experts in information, database, application, infrastructure, and network security. Since its founding, Oracle has been a driving force in developing secure applications and systems. At Oracle, we apply this experience to the development of our comprehensive cloud offerings.



Used by organizations worldwide, from large enterprises and the most demanding governments to small enterprises, Oracle Cloud offers a comprehensive IaaS and Platform as a Service (PaaS) portfolio that includes services such as Compute, Storage, Networking, Database, Java, Process, Mobile, Data Management, and Business Analytics. All of Oracle's IaaS and PaaS services share a common set of security capabilities such as identity and access management.



2. Oracle Cloud Services: Built for Trust

Oracle's mission is to bring its leading enterprise technology and business applications software to customers, anywhere in the world, through the Internet. Oracle Cloud is a broad set of industry standards-based, integrated services that provide customers with subscription-based access to Oracle platform services, application services, and social services, all completely managed, hosted, and supported by Oracle.

Oracle Cloud Infrastructure as a Service (IaaS) offers a set of core infrastructure capabilities like elastic compute and storage to provide customers the ability to run any workload in the cloud. The core of Oracle Cloud IaaS provides three primary functions on which customers can build and manage virtual environments, applications, and associated configurations.

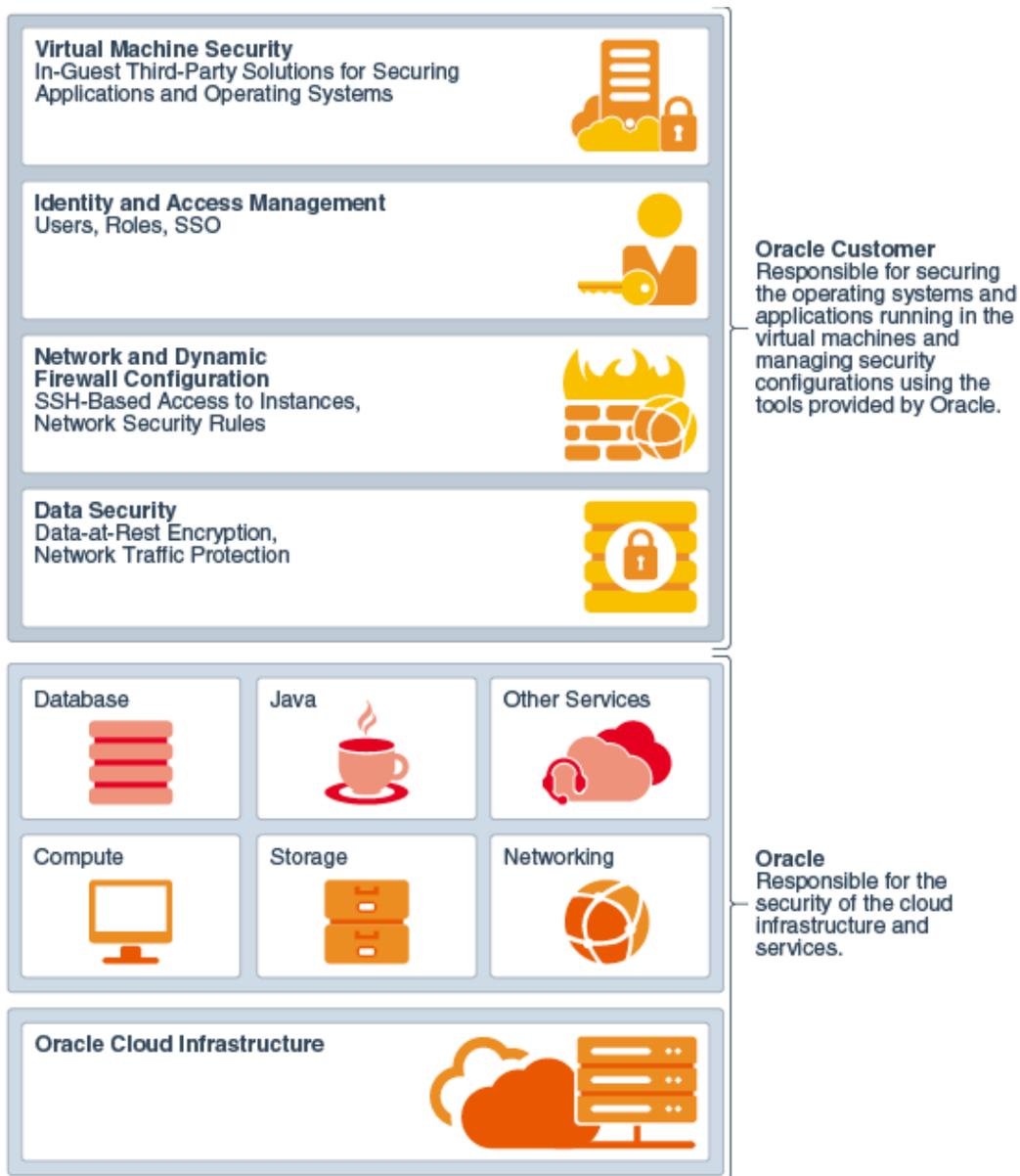
- » Oracle Cloud Infrastructure Compute Classic provides flexible and scalable computing, block storage, and networking services on Oracle Cloud. Customers can choose between a multitenant elastic compute and a dedicated compute service. The latter provides a compute environment provisioned on isolated computing resources. The compute zones are completely dedicated to a customer, with complete network isolation. Customers can get access to Oracle Cloud Infrastructure Compute Classic through a Representational State Transfer (REST) API, a command-line interface (CLI), and a web-based UI.
- » Oracle Cloud Infrastructure Object Storage Classic is a cost-effective, remote backup and archiving solution for enterprise data and applications. Customers can access Oracle Cloud Infrastructure Object Storage Classic by using the industry-standard OpenStack Swift-compatible REST API, NFSv4 via the Oracle Cloud Infrastructure Storage Software Appliance, programmatically via the Java API, or other certified third-party applications. Customers can also monitor key storage metrics and manage users and roles by using a web-based graphical console. For enhanced security, customers can use the client-side encryption features of the software appliance and Java library to encrypt every object with a unique symmetric key before uploading and storing the object in the cloud service.
- » Oracle Cloud Infrastructure Networking Classic offers two VPN solutions. A site-to-site VPN for dedicated compute enables customers to connect their data centers to Oracle Cloud over an IPsec tunnel. The second VPN solution is offered via Corente Cloud Services Exchange, which uses a distributed virtual appliance located at the network edge. In addition to VPN solutions, Oracle customers can use Oracle's FastConnect solution that provides a private, high bandwidth connection between customer data centers and Oracle Cloud, offering more predictable network performance. FastConnect also provides a predetermined path for data transfer, unlike the Internet, thus offering better security because the data will never leave trusted boundaries.



Oracle Cloud Platform as a Service (PaaS) helps enterprise IT and independent software vendor (ISV) developers rapidly build and deploy rich applications, or extend Oracle Cloud Software as a Service (SaaS) applications using an enterprise-grade cloud platform based on the industry's best database and application server. Oracle Cloud PaaS includes multiple database enterprise cloud services, which offer database functionality based on Oracle Database and Oracle Exadata Database Machine. Powered by Oracle WebLogic Server, Oracle Java Cloud Service provides a platform on top of Oracle's enterprise-grade cloud infrastructure for developing and deploying new or existing Java EE applications. For a comprehensive list of the available Oracle Cloud services, go to <https://www.oracle.com/cloud>.

3. Customer and Oracle Security Responsibilities

As a customer, the services that you use determine the configuration work you must perform as part of your security responsibilities. Oracle Cloud infrastructure and platform services operate under a shared responsibility model, where Oracle is responsible for the security of the underlying cloud infrastructure, and you are responsible for securing your workloads as well as platform services such as Oracle Database and Oracle WebLogic Server. The following figure shows the shared security responsibilities.





As with all Oracle Cloud services, you should protect your Oracle Cloud Services access credentials and set up individual user accounts. You are responsible for managing and reviewing access for your own employee accounts as well as for all activities that occur under their accounts.

Oracle Cloud Services that fall into the category of IaaS, such as Oracle Cloud Infrastructure Compute Classic and Oracle Cloud Infrastructure Object Storage Classic, are completely under customer control and require you to perform all of the necessary security configuration and management tasks. For example, for Oracle Cloud Infrastructure Compute Classic, you are solely responsible for configuring, operating, maintaining, and securing the operating systems and other associated software of your cloud services including your applications. You are solely responsible for maintaining appropriate security, protection, archiving, and backup of your content, which may include the use of application or in-guest encryption technologies to protect your content from unauthorized access. You have full control of when patches are applied. For Oracle Cloud Infrastructure Object Storage Classic, you are responsible for encrypting your data on the client side before storing it in Oracle Cloud Infrastructure Object Storage Classic.

Oracle Cloud services that fall into the category of PaaS, such as Oracle Database Cloud Service and Oracle Java Cloud Service, are completely under customer control and require you to perform all of the necessary security configuration and management tasks. For example, for Oracle Database Cloud Service, you are responsible for backup, recovery, patching, and scaling by using Oracle-provided cloud tooling. You are also responsible for defining network security policies at the virtual machine level as well as database access control policies because you have full-privileged access to your virtual machine instances and your database instances that run on your virtual machine. Customer data is encrypted by default in tablespaces.

For Oracle Java Cloud Service, customers are responsible for backup, recovery, patching, and scaling by using Oracle-provided cloud tooling. For the non-virtual image version of the Oracle Java Cloud Service, Oracle provides automated backups.

Oracle is responsible for protecting the global infrastructure that runs all of the services offered in Oracle Cloud. This infrastructure consists of the hardware, software, networking, and facilities that run Oracle Cloud services. In the following sections, we will discuss Oracle's infrastructure and service-specific security capabilities in more detail.



4. Oracle Cloud Infrastructure Security

Oracle's Cloud infrastructure is used to provision a variety of SaaS, PaaS, and IaaS services. The Oracle Cloud infrastructure includes facilities, network, hardware, and operational software that support the provisioning of these services. The cloud infrastructure was developed to offer secure infrastructure and platform services that are used by Oracle customers to run their mission-critical enterprise workloads and store their data. You can be assured that you are building scalable enterprise cloud solutions using Oracle's compute, storage, networking, and platform services that run on top of some of the most secure cloud infrastructure in the world.

4.1 Physical Security Safeguards

Oracle provides secured computing facilities for both office locations and production cloud infrastructures. Oracle's data centers are state of the art, using innovative engineering approaches. The exterior perimeter of each data center has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned guard stations, all of which help defend against non-entrance attack points. Authorized staff must pass a two-factor authentication to access data centers. Oracle only provides data center access and information to employees and contractors who have a legitimate business need for these privileges. All physical access to data centers by Oracle employees is logged and audited routinely. Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management.

4.2 Oracle Cloud Services Access for Oracle Employees

Access to cloud systems is controlled by restricting access to authorized personnel. Oracle uses a secured VPN tunnel using multifactor authentication for employee access and enforces access policies on infrastructure components and cloud management systems used to operate the Oracle Cloud environment. System access controls include system authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined users. All operator actions including key strokes are logged in a way that Oracle can perform audits and forensics.

Network and operating system accounts for Oracle employees are reviewed to ensure appropriate employee access levels. In the event of employee terminations, Oracle takes prompt actions to terminate network, telephone, and physical access.



4.3 Background Checks

Oracle conducts criminal background checks, as permitted by law, as part of preemployment screening practices for new employees in the United States. Oracle's ability to conduct background checks outside the United States is subject to local legislation and local Oracle policy.

4.4 Measures to Minimize Employee Risks

Measures to minimize risks associated with human error, theft, fraud, and misuse of facilities include personnel screening, confidentiality agreements, and security awareness education and training with enforcement of disciplinary actions. Oracle employees are required to maintain the confidentiality of customer data. Oracle employees are required to sign a confidentiality agreement and comply with company policies concerning protection of confidential information (Code of Ethics and Business Conduct, Oracle Acceptable Use Policy for Company Resources, and the Information Protection Policy) as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.

4.5 Oracle Corporate Network Segregation

The Oracle Cloud production network is segregated from the Oracle corporate network and requires a separate set of credentials for logical access. Oracle Cloud developers and administrators on the corporate network who need to access Oracle Cloud components in order to maintain them must explicitly request access credentials. All requests are reviewed and approved by the applicable service owner.

4.6 Secure Network Architecture

The Oracle Cloud network provides significant protection against traditional network security issues such as distributed denial of service (DDoS) attacks, man-in-the-middle attacks, IP spoofing, and port scanning.

Oracle uses network protection devices, including firewalls, to monitor and control network communications at the external boundary of the network and at internal boundaries within the network. These network boundary devices employ traffic flow policies, or access control lists (ACLs), that enforce the flow of traffic. Firewalls are deployed in a layered approach to perform packet inspection with security policies configured to filter the packets based on protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types. Oracle Cloud services use network vulnerability assessment tools to identify security threats and vulnerabilities. Formal procedures are in place to assess, validate, prioritize, and remediate identified problems. Oracle subscribes to vulnerability notification systems to stay apprised of security incidents, advisories, and



other related information. Oracle takes action on the notification of a threat or risk after it's confirmed that a valid risk exists, that the recommended changes are applicable to service environments, and the changes will not otherwise adversely affect the services.

DDoS protection/mitigation is delivered primarily through a certified firewall appliance with dedicated DOS protection enabled. Devices are scaled to support large amounts of traffic and maintain a connection. This provides layer 3-7 attack prevention capabilities. Whether the attack is volumetric, trying to overload connections per second capacity, or falsifying legitimate connections, trying to exhaust memory, the proxy nature of the load balancer environment allows inspection and a response for each connection to either absorb or drop as appropriate. These devices are designed to actively terminate each session for protocol inspection, content examination, and web application (layer 7) firewall. These devices also provide technologies such as SYN cookie encryption, high capacity connection tables, pattern matching, flow validation, Internet Control Message Protocol (ICMP) flood limiting, and strict TCP forwarding.

Oracle Cloud Services uses Network Intrusion Detection Systems (NIDS) to protect the environment. NIDS sensors are deployed in either Intrusion Prevention Mode (IPS) or Intrusion Detection Mode (IDS) on the network, to monitor and block suspicious network traffic from reaching the internal network. NIDS alerts are routed to a centralized monitoring system that is managed by the security operations teams 24 hours, 365 days a year.

4.7 Encrypted Access to Oracle Cloud Services

Customer access to the system is mostly through the Internet. The industry-standard Transport Layer Security (TLS) protocol is used for Oracle Cloud Service access. TLS connections are negotiated for at least 128-bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be used for connecting to web-enabled programs. The list of certified browsers for each version of an Oracle program can be found on the Cloud Customer Support Portal designated by Oracle for the specific service ordered (for example, the My Oracle Support portal). In some cases, a third-party site used with cloud services that aren't under the control of Oracle may force a non-encrypted connection. In other cases, a third-party site that the customer wants to integrate with the cloud service may not accept an encrypted connection. For cloud services where non-encrypted connections with the third-party site are permitted



by Oracle, Oracle will enable these connections in addition to their encrypted counterparts, if applicable.

Customers can also access Oracle Cloud services via SSH or using an IPsec-enabled VPN service.

4.8 Platform Hardening and Monitoring

Oracle employs standardized system hardening practices across Oracle Cloud systems in order to protect these systems from potential attacks. The platform hardening practices include restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, logging, and alerting.

4.9 Security Incident Response

Oracle evaluates and responds to incidents that create suspicions of unauthorized access to or handling of customer data whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contractors.

Staff operators provide 24 hour, 365 days coverage to detect and manage security incidents. Upon notification, Oracle's Global Information Security (GIS) organization defines escalation paths and response teams to address those incidents, depending on the type of activity. GIS will work with the customer, the appropriate technical teams, and law enforcement, when necessary, to respond to the incident. The goal of the incident response team is to restore the confidentiality, integrity, and availability of the customer's environment, and to establish root causes and remediation steps. Operations staff has documented procedures to identify and address incidents where handling of data may have been unauthorized, including prompt and reasonable reporting, escalation procedures, and chain-of-custody practices.

4.10 Malware Prevention

An effective malware attack can lead to account compromise and data theft. The Oracle Cloud operations team uses a variety of methods to prevent, detect, and eradicate malware. Oracle deploys antivirus/malware software on relevant systems used by Oracle Cloud Services. Viruses and malware that are detected are removed (or quarantined) automatically. Virus and malware definitions are updated frequently, and applicable client systems are configured to perform definition updates and real-time scans. Oracle's Global Desktop Strategy (GDS) organization keeps antivirus/malware products and Windows Server Update Service (WSUS) servers up to date with virus and malware definitions and security updates. GDS may notify the user community of any credible virus or malware threats and when WSUS security updates are available.



4.11 Internal Oversight by Executives

The Oracle Security Oversight Committee (OSOC), consisting of Oracle senior executives, reviews and approves Oracle's security and privacy policies and programs. Global Information Security (GIS) is the corporate organization that is responsible for security oversight and enforcement, at the corporate level. GIS is also responsible for the development and management of information security policies and strategies, information security assessments, and training and awareness. GIS is the primary contact for security incident response, providing the overall direction for incident prevention, identification, investigation, and resolution.

Oracle's Chief Privacy Officer provides oversight and management of privacy-related regulatory issues. Oracle's Business Audit and Assessment organization is responsible to Oracle's Board of Directors to audit the compliance of all these functions and to report the audit results.

4.12 Data Disposal

When services are terminated or at a customer's request, Oracle will delete environments or data in a manner designed to ensure that they can't reasonably be accessed or read, unless there is a legal obligation imposed on Oracle which prevents Oracle from deleting all or part of the environments or data.

4.13 Physical Media in Transit

Designated Oracle personnel handle media and prepare it for transportation according to defined procedures and only as required. Digital media is logged, encrypted, securely transported, and as necessary for backup, archived in a vault by a third-party off-site vendor. Vendors are contractually obligated to comply with Oracle-defined terms for media protection.

4.14 Data Privacy

Oracle's Data Processing Agreement for Oracle Cloud Services (Data Processing Agreement) and the Oracle Services Privacy Policy describe Oracle's treatment of data that resides on Oracle systems (including personally identifiable information (PII)) to which Oracle may be provided access in connection with the provisioning of most cloud services. The Data Processing Agreement specifically describes Oracle's and the customer's respective roles for the processing and control of personal data that the customer provides to Oracle as part of the cloud services.



These documents are available at:

- » Data Processing Agreement for Oracle Cloud Services
<http://www.oracle.com/dataprocessingagreement>
- » Oracle Services Privacy Policy
<http://www.oracle.com/us/legal/privacy/services-privacy-policy-078833.html>

4.15 Third Party Audit Reports

Audit reports of Oracle Cloud Services are periodically published by Oracle's third-party auditors, although reports may not be available for all services or at all times. Customers may request a copy of the current published audit report available for a particular Oracle Cloud service. These reports are confidential, may be used solely by the customer to evaluate the design and operating effectiveness of defined controls applicable to Oracle Cloud Services and are provided "AS-IS" without any warranty.



5. Shared Identity and Access Management

Oracle Cloud offers a shared identity and access management solution used by all Oracle Cloud services including PaaS and IaaS services. Identity is a core feature that Oracle customers rely on to provide secure access to Oracle's PaaS and IaaS services. The Oracle Cloud feature that brings users, services, and applications together in a secure manner is shared identity.

5.1 Identity Domain, Users, and Roles

A tenant in Oracle Cloud represents a customer who has subscribed to one or more services from Oracle Cloud. Typically there is a one-to-one correspondence between an Oracle Cloud tenant and an Oracle customer. An identity domain in Oracle Cloud represents the namespace assigned for a tenant. An identity domain is used to identify and associate the assets of a tenant and thereby enable isolation of data assets and transactions of a tenant from that of other tenants. A tenant's assets include subscribed services and data assets including security artifacts such as users, groups, tokens, cookies, and policies. An Oracle customer can be associated with more than one Oracle Cloud identity domain.

Oracle's shared cloud identity management solution controls the authentication and authorization of the users who can sign in to a service in Oracle Cloud and which features they can access in relation to the service. An Oracle Cloud service account is a unique customer account that can have multiple cloud services of different service types. For example, you can have three different services, such as Java, Database, and Infrastructure as a Service (IaaS) as part of a single Oracle Cloud service account. Every Oracle Cloud service belongs to an identity domain. Multiple services can be associated with a single identity domain to share user definitions and authentication. Users in an identity domain can be granted different levels of access to each service associated with the domain. When you sign up for an Oracle Cloud service account, Oracle Cloud creates an identity domain specific to you. When your users log in to an Oracle Cloud service through the service account, the cloud identity management controls the user authentication and controls which features of the service they can access.

Access management within an identity domain depends on users and their roles. Users with administrative roles manage local cloud identities and their rights.



There are two types of users in an identity domain to manage:

- » **Standard users:** Add user accounts, import a batch of user accounts, assign roles to users, modify user accounts, reset passwords, and remove user accounts.
- » **SFTP users:** Set passwords for secure FTP (SFTP) user accounts. SFTP user accounts are used to sign in to an SFTP server to perform FTP operations related to Oracle Cloud services.

There are two types of roles in an identity domain to manage:

- » **Predefined roles:** View a list of all the predefined roles created by Oracle Cloud and link to a list of users assigned to the role you select
- » **Custom roles:** View, add, and remove roles that you created for customized access to your Oracle Cloud services

When a service account is activated, Oracle Cloud assigns the following roles to a customer automatically:

- » **Account administrator:** The account administrator role is at the service instance level. It gives a user several responsibilities to manage one or more Oracle Cloud services. An account administrator is responsible for managing an Oracle Cloud account through the cloud user interface (UI). The account administrator has business oversight responsibilities for service instances across one or more identity domains. The account administrator can nominate service administrators and identity domain administrators for services the account administrator buys. The account administrator can view metrics for individual service instances.
- » **Identity domain administrator:** The identity domain administrator manages users and their roles. The identity domain administrator's view is limited to the users and roles in the identity domains that they were assigned to manage. The identity domain administrator sees all the roles at the domain and service levels. An identity domain administrator is a "super administrator" for an identity domain and for all of the services within the domain. An identity domain administrator can delegate to other identity domain administrators as well as manage roles assigned to service administrators. Identity domain administrators can perform administrative responsibilities for the whole identity domain.
- » **Service administrator:** A service administrator is a "super administrator" for a particular service instance. Service administrators can assign additional service administrators to roles as well as manage other roles associated with the service. However, service administrators can't create users or roles.



5.2 Passwords

Passwords are required to access all user accounts. You specify the password when you create the account, and you can change it at any time from the cloud UI.

5.3 Single Sign-On Using SAML 2.0

You can federate your corporate identity and your identity domain and thereby achieve single sign-on (SSO) between on-premises and Oracle Cloud. The SSO service enables users to log in to one domain and access another domain without logging in again. Oracle Cloud uses the open standard Security Assertion Markup Language (SAML) 2.0 to implement single sign-on for browser-based access. The SSO service enables you to provide access to one domain to users who have been authenticated to a different domain or to an on-premises identity store. For example, you might want your users to log in to the cloud by using a local directory such as Active Directory or Oracle Unified Directory. The SSO service is built on the federation capability of the identity infrastructure. The SSO service uses the industry-standard SAML 2.0 to exchange information between an identity provider and a service provider.

The Oracle Cloud identity infrastructure stores identities using LDAP schemas. Like most identity management systems, Oracle Cloud includes an identity store. The format and rules for defining users, groups, and roles are determined by specific LDAP directory schemas.

5.4 Login Management

An identity domain may have a split user population, where user identities are:

- » **Non-federated:** Stored on one local identity management system. These user identities are associated only with Oracle Cloud. As a result, they are known only to Oracle Cloud.
- » **Federated:** Stored across multiple distinct identity management systems and are coming from different domains. Federated users receive their identities from their administrator. These identities may be known to Oracle Cloud through an LDAP export to shared identity management (SIM). However, these users can't log in to Oracle Cloud directly. Instead, they are redirected to their federated site for logging in. At that time, the Oracle Cloud Single Sign-On service gets a SAML assertion from the identity provider. SAML assertion contains user information from the identity provider. Oracle Cloud Single Sign-On service parses the SAML assertion and asserts the identity to the identity domain.



5.5 Administrator On-Boarding

Administrator on-boarding is easy with Oracle Cloud. When you sign up for an Oracle Cloud account, you receive an e-mail. After receiving the e-mail, you activate the account and navigate to the associated cloud service. You start the request for a trial subscription from the Oracle Cloud website. When you request a trial subscription, the system assigns you to the following roles automatically:

- » Account administrator for the Oracle Cloud service
- » Identity domain administrator for the identity domain
- » Service administrator for the service

For a more detailed explanation of the Oracle Cloud identity concepts, go to https://docs.oracle.com/cloud/latest/trial_paid_subscriptions/OCUID/toc.htm



6. Service-Specific Security

The following sections describe the security provided for Oracle Cloud Infrastructure Compute Classic, Oracle Cloud Infrastructure Object Storage Classic, Oracle Cloud Infrastructure Networking Classic, Oracle Database Cloud Service, Oracle Database Exadata Cloud Service, Oracle Java Cloud Service, and Oracle Management Cloud.

6.1 Oracle Cloud Infrastructure Compute Classic Security

Instance Isolation

Oracle Cloud Infrastructure Compute Classic lets you create and run virtual machines on the Oracle Cloud infrastructure. The Oracle Cloud Infrastructure Compute Classic provides resizable computing capacity using server instances in Oracle's data centers.

Security within Oracle Cloud Infrastructure Compute Classic is provided on multiple levels: the hypervisor, guest operating system, a dynamic firewall, token-based API calls, user permissions, and SSH-based secure access to instances. The goal is to prevent customer workloads and data from being accessed by unauthorized users and systems.

Like many other cloud compute services, virtualization is the foundation of Oracle Compute Cloud Service. Many security-related concerns about virtualization are unwarranted. Multiple hardware-supported and software-supported isolation techniques address the risks associated with virtualization.

The first technique is instruction isolation. Intel VT-x and AMD-V both enable a virtual machine monitor to give the CPU to a virtual machine for direct execution until the time the virtual machine attempts to execute a privileged instruction. At that point, the virtual machine execution is suspended, and the CPU is given back to the virtual machine monitor.

In addition to CPU instruction isolation, the hypervisor also provides memory and device isolation by the virtualization of physical memory and physical devices including disks. This explicit virtualization of the physical resources leads to a clear separation between the guest OS and the hypervisor, resulting in a secure compute environment. Thus, different customer instances running on the same physical machine are isolated from each other via the hypervisor.



In Oracle's multitenant elastic compute service, the logical tenant isolation is achieved via virtualization, as previously described. Oracle also offers a dedicated compute solution, which is a fully isolated elastic compute service. It provides dedicated physical servers and cores and a network within an Oracle data center. Thus, customers get complete IO, CPU, and network isolation. The dedicated compute service uses the same virtualization technology used by the elastic compute service.

The elastic compute service also provides API namespace separation to ensure resources are not misused across accounts.

Guest Operating System

You have full administrative access and root access over your instances. Oracle doesn't access customer data in customer instances. Oracle supports the use of SSH to enable you and your users to securely log in to your Oracle Linux instances. Oracle recommends that you generate unique SSH key pairs for every user. These keys shouldn't be shared with Oracle or other organizations.

You control the updating and patching your guest OS, including security updates. Oracle-provided Oracle Linux machine images are updated regularly with the latest patches.

Secure Access to Instances Using SSH

Oracle supports the use of the SSH network protocol to enable you to securely log in to your Oracle Linux instances. If you created your instance using an Oracle-provided Oracle Linux image, then you can log in to your instance using SSH as the `opc` user, which is the default user on instances that are created using an Oracle-provided Oracle Linux instance.

Before creating a compute instance, you must generate at least one SSH key pair and upload the SSH public key. You can disable, enable, and delete an existing SSH public key. After logging in to your instance, you can add users on your instance. This requires that you generate a new SSH key pair for the new user and that you log in to your instance and become the root user. Then, you can create a new user and associate the SSH public key with the new user.



Dynamic Firewall

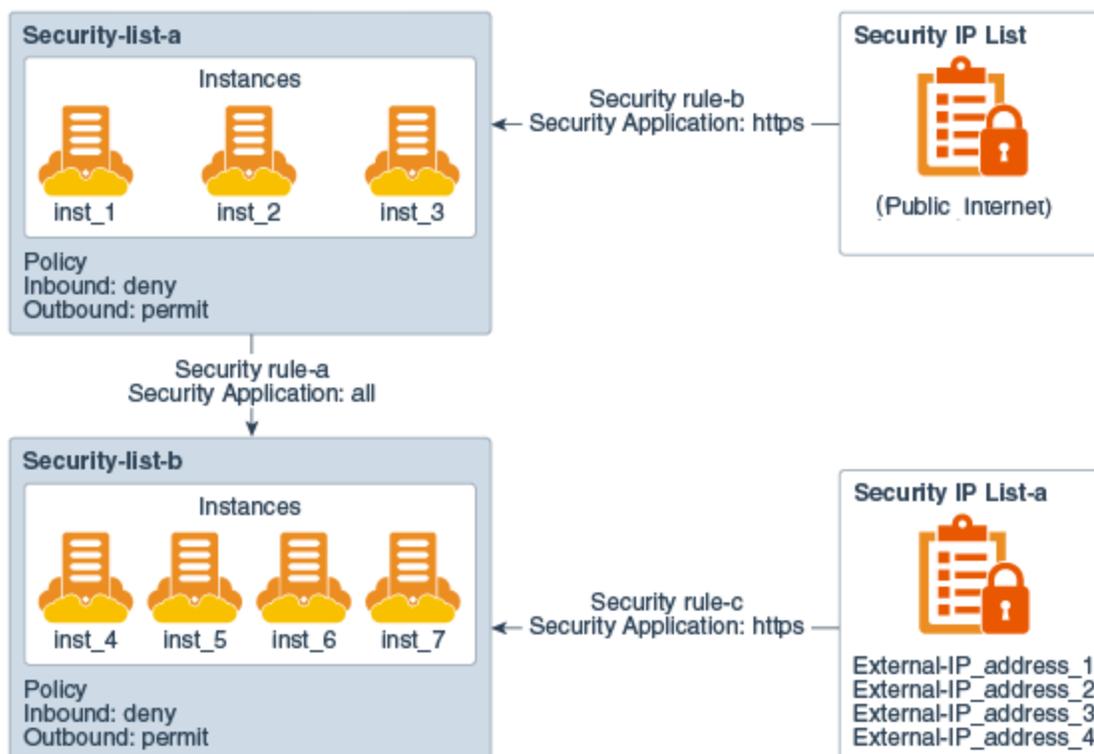
Oracle Cloud Infrastructure Compute Classic provides a complete firewall solution to control network traffic for your instances. The firewall is configured in the default deny-all mode. This means when you create an instance, by default, it doesn't allow any network traffic to and from other instances or an external host. You can implement fine-grained control over network access to your Oracle Cloud Infrastructure Compute Classic instances, both from other instances and from external hosts. The firewall can be configured in groups, which lets different classes of instances have different rules.

To enable unrestricted communication among some of your instances (for example, to enable all the instances hosting your development environment to communicate with each other), you can create a security list and add the instances to that security list. When you add an instance to a security list, the instance can communicate with all the other instances in the same security list. By default, the instances in a security list are isolated from hosts outside the security list. You can override this default by creating security rules. Each security rule defines a specific source, a destination, and a protocol-port combination over which communication is allowed. Security rules are essentially firewall rules, which you can use to permit traffic between Oracle Cloud Infrastructure Compute Classic instances in different security lists, as well as between instances and external hosts. The source and destination specified in a security rule can be either a security IP list (that is, a list of external hosts) or a security list. A security application is a protocol-port mapping that you can use in security rules. You can either create a security application by specifying the port type and port, or you can use one of the predefined security applications (such as SSH, HTTPS, SNMP-TCP) in security rules. As an example, you can set up a security rule to permit SSH access over port 22 from a set of external hosts (specified in a security IP list) to all the instances in a security list.

When you create an instance by using the web console, you can specify that the instance be configured to allow SSH access from hosts on the Internet. When you select this option, your instance is added to a default security list, and a security rule called `DefaultPublicSSHAccess` is created to enable SSH access to instances in the default security list. If you don't enable SSH access during instance creation, then to enable SSH access to your instance later, you must create a security list, add the instance to it, and set up a security rule to permit SSH traffic to the security list. The following diagram shows these communication paths:

- » Instances in Security-list-a can send traffic to instances in Security-list-b over any protocol, as defined by Security rule-a.

- » Instances in Security-list-a can receive HTTPS traffic from any host on the Internet, as defined by Security rule-b.
- » Instances in Security-list-b can receive traffic over SSH from any of the IP addresses specified in Security IP List-a, as defined by Security rule-c.



If no security rules are defined for a security list, then, by default, instances in that security list can't receive traffic from hosts outside the security list. However, instances in the security list can still access other instances in the same security list. When you remove an instance from a security list, the instance can no longer communicate with other instances in that security list, and traffic to and from that instance is no longer controlled by the security rules defined for that security list. A security IP list specifies a set of IP addresses that can be used as a source in security rules. A security IP list or a security list can be used in multiple security rules. In case of conflicts in the policy, the most restrictive policy takes precedence.

You can connect your instances to the Internet and access Oracle Cloud resources from anywhere using reserved IPs.



API Access

Oracle Cloud Infrastructure Compute Classic provides a REST application programming interface (API) that you can use to programmatically provision and manage instances and the associated resources. API calls to Oracle Cloud Infrastructure Compute Classic can be done using basic authentication (user name and password) or token-based authentication. If the authentication request succeeds, then the server returns a cookie that contains an authentication token that is valid for 30 minutes. The client making the API calls must include this cookie in the API calls. You can extend the expiration of the authentication token by 5 minutes from the time you run the `refresh_token` command. Refreshing the token extends the session, but not beyond the session's expiration time. A session is 3 hours.

Users and Roles

You can use the MyServices Users page to manage identity domain administrators, service administrators, users, roles, and passwords. (See the 5. Shared Identity and Access **Management** section in this document.)

You can use the following predefined roles for Oracle Cloud Infrastructure Compute Classic:

- » **TenantAdminGroup (identity domain administrator):** Users who are assigned this role can perform all the tasks in the MyServices application, including user and role management tasks.
- » **Service-instance-name.Compute_Operations (service administrator):** Users who are assigned this role can view, create, update, and delete Oracle Cloud Infrastructure Compute Classic resources. The identity domain administrator can create additional service administrators, as required, by assigning this role in Oracle Cloud MyServices. For business continuity, consider creating at least two users with the Compute_Operations role. These users must be IT system administrators in your organization.
- » **Service-instance-name.Compute_Monitor:** Users who are assigned this role can view Oracle Cloud Infrastructure Compute Classic resources. The identity domain administrator can create users with this role in Oracle Cloud MyServices.

Block Storage Security

A storage volume is a virtual disk that provides persistent block storage space for instances. Oracle Cloud Infrastructure Compute Classic allows you to create storage volumes from 1 GB to 2 TB. You



can attach up to 10 storage volumes to each Oracle Cloud Infrastructure Compute Classic instance. A storage volume can be attached to only one instance at a time. You can attach one or more storage volumes to an instance either while creating the instance or later when the instance is running. After creating an instance, you can easily scale up or scale down the block storage capacity for the instance by attaching or detaching storage volumes. However, you can't detach a storage volume that was attached during instance creation. Note that, when a storage volume is detached from an instance or when the instance is deleted, data stored on the storage volume isn't lost.

Storage volume access is restricted to the Oracle Cloud account that created the volume and to the Oracle Cloud users, which have the authorization to view or access the volume. Granting access to these users must be done via roles that were created using Oracle Shared Identity Management. (See the 5. Shared Identity and Access **Management** section in this document.) Oracle Cloud Infrastructure Compute Classic requires roles to perform the following storage volume operations:

- » Creating and attaching a storage volume: You can create storage volumes and attach them to instances to provide block storage capacity for storing data and applications. You can also associate a storage volume with a machine image, and then use the storage volume as the boot disk for an instance. To complete this task, you must have the Compute_Operations role.
- » Viewing details of a storage volume: You can use the web console to view details of a storage volume, such as the status, size, and the instance to which it is attached. This task requires the Compute_Monitor or Compute_Operations role.
- » Deleting a storage volume: If you delete a storage volume, then all the data and applications that were saved on that storage volume are lost. Delete a storage volume only when you're sure that you no longer need any of the data that's stored on that volume. To complete this task, you must have the Compute_Operations role.

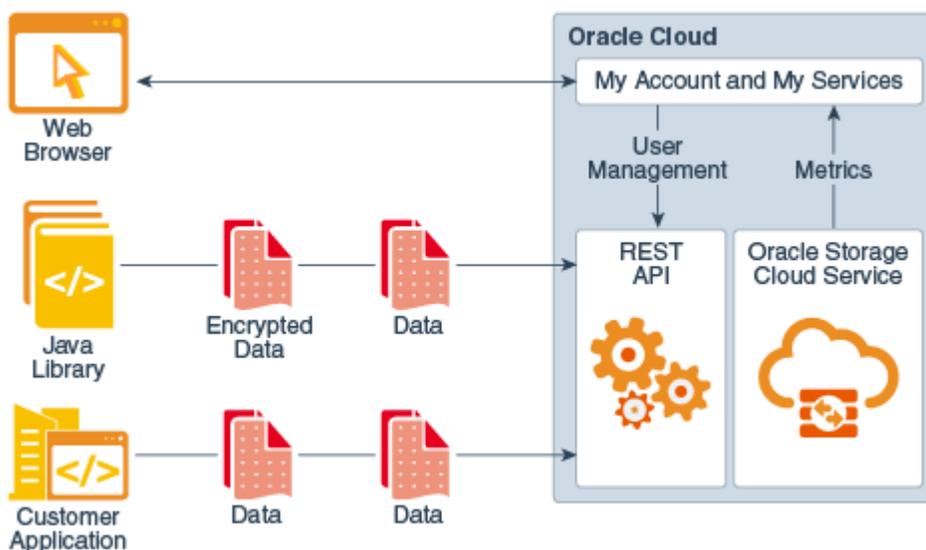
Encryption of sensitive virtual machine disks is generally a good security practice. You can use any in-guest encryption solution to encrypt your data within your virtual machines using any third-party in-guest encryption solution. Most of these solutions offer key management capabilities that you can use to implement a key management policy.

6.2 Oracle Cloud Infrastructure Object Storage Classic Security

Oracle Cloud Infrastructure Object Storage Classic is an Infrastructure as a Service (IaaS) product, which provides an enterprise-grade, multitiered, storage solution for storing unstructured data and accessing it anytime from anywhere. It's ideal for data backup, archiving, file sharing, and for storing large amounts of unstructured data like logs, sensor-generated data, and virtual machine (VM) images.

The Oracle Cloud Infrastructure Object Storage Classic architecture is highly available and redundant. It can be accessed directly via a REST API and indirectly via NFSv4, client SDKs, and third-party applications. When objects are stored in Oracle Cloud Infrastructure Object Storage Classic, the data is replicated across multiple storage nodes in the data center. This replication strategy ensures that stored object data can survive hardware failure.

The following diagram is an architectural overview of Oracle Cloud Storage Service.



Read and Write Access to Objects

Oracle Cloud Infrastructure Object Storage Classic stores data as objects within a flat hierarchy of containers. An object is most commonly created by uploading a file. It can also be created from ephemeral unstructured data. Objects are created within a container. A single object can hold up to 5 GB of data, but multiple objects can be linked together to hold more than 5 GB of contiguous data. A container is a user-created resource, which can hold an unlimited number of objects, unless you specify a quota for the container. Note that the containers can't be nested.

Read and write access to an object is controlled via access control lists (ACLs) for its container. Each container can be assigned its own read and write ACLs. By default, access to a container and its objects is private (that is, only the user who created the container can access it), but read access can be made public if required.



Users with the storage administrator role will always have read and write access to all containers in their service instance. All non-administrator users are subject to the ACLs for a given container. The service instance root path is an exception to this because it doesn't have ACLs associated with it. For this path, all users can obtain a list of containers, but only users with the storage administrator role can create or delete containers.

API Access

The primary method for accessing Oracle Cloud Infrastructure Object Storage Classic is through a RESTful web service, which is based on OpenStack Swift. The service can be accessed from anywhere over the Internet, at any time, and from any device. A Java library that wraps the RESTful web service is also available. No special hardware is required to start using the service.

Users and Roles

You can use the MyServices Users page to manage identity domain administrators, service administrators, users, roles, and passwords. (See the 5. Shared Identity and Access **Management** section in this document.)

You can use the following predefined roles for Oracle Cloud Infrastructure Object Storage Classic:

- » **TenantAdminGroup (identity domain administrator):** Users who are assigned this role can perform all the tasks in the MyServices application, including user and role management tasks.
- » **Storage.Storage_Administrator (service administrator):** Users who are assigned this role can perform all tasks for an Oracle Cloud Infrastructure Object Storage Classic instance, including user management. These users can also monitor and manage services, grant roles to users, create and delete containers, and modify container ACLs. For non-metered subscriptions, the role name would be service-instance-name.Storage_Administrator.
- » **Storage.Storage_ReadWriteGroup:** Users who are assigned this role can create, read, modify, and delete objects within containers as well as list containers and objects within containers unless the role was removed from the container's read ACL. For non-metered subscriptions, the role name would be service-instance-name.Storage_ReadWriteGroup.
- » **Storage.Storage_ReadOnlyGroup:** Users who are assigned this role can read objects, list containers, and list objects within containers unless the role was removed from the container's read ACL. For non-metered subscriptions, the role name would be service-instance-name.Storage_ReadOnlyGroup.



Encrypting Objects

You can encrypt objects before they are sent to Oracle Cloud Infrastructure Object Storage Classic. You can use the Java library or any other encryption solution to do this.

When you use the client-side encryption feature of the Java library, all encryption happens within the Java library, and no encryption happens within the service. Any user with the service administrator role or a role that is specified in the X-Container-Write ACL of the container can perform this task.

When you use the Java library, for every object that you create in Oracle Cloud Infrastructure Object Storage Classic, a unique symmetric key is generated. The Java library uses the symmetric key to encrypt your data before storing it. In addition, you must provide and manage an asymmetric key pair. After encrypting your data, the Java library encrypts the symmetric key as an envelope key by using the asymmetric key pair. Note that you can rotate a previously used key pair for a new key pair without downloading and reencrypting each object. The envelope key is stored as metadata alongside the object data.

When you use the Java library to access such encrypted objects, the envelope key is first retrieved and decrypted by using the asymmetric key pair that you provide. The resulting symmetric key is then used to decrypt the object data. Because the envelope key is object metadata, removing or tampering with it will result in making the encrypted object data unrecoverable. It is a best practice to limit write access to client-side encrypted objects to prevent this from happening.

Note that if you encrypt your data using the Java library, it can't be accessed through the REST API. This is because Oracle Cloud Infrastructure Object Storage Classic stores the envelope key as metadata on the object and Oracle doesn't publish the method for extracting the envelope key, decrypting it, and then decrypting the object. If you encrypt an object via client-side encryption using the Java library, then you must exclusively use the Java library to access the encrypted object in the future. You can't decrypt the encrypted object without the Java library.

When using the Java library's encryption feature, only 2048-bit RSA key pairs are supported, and only object data is encrypted, not object metadata. Segmented objects can't be encrypted. Non-encrypted objects can't be downloaded while using the encryption feature.



You can also use your own envelope encryption solution to encrypt your data before storing it in Oracle Cloud Infrastructure Object Storage Classic. In this case, you can use the REST API to access your encrypted objects.

Note that when you use client-side encryption, you are responsible for managing the lifecycle of the encryption keys including generating, rotating, and archiving the keys.

Oracle Cloud Infrastructure Storage Software Appliance Security

Oracle Cloud Infrastructure Storage Software Appliance is a virtual appliance to facilitate easy, secure, reliable data storage and retrieval from Oracle Cloud Infrastructure Object Storage Classic. To ensure that your data remains protected both when it is stored in Oracle Cloud Infrastructure Object Storage Classic and in transit, you can enable encryption of the data in Oracle Cloud Infrastructure Storage Software Appliance before it is stored in Oracle Cloud Storage Service.

Data encryption in Oracle Cloud Infrastructure Storage Software Appliance is done using a symmetric key, which is stored in a database on the appliance and is encrypted by using an asymmetric public/private key pair. Administrators can back up and store the asymmetric keys, and use them to recover encrypted data.

When a file is stored in Oracle Cloud Infrastructure Storage Software Appliance, it is first stored in the local disk cache in its original form. The file is encrypted before it is uploaded to Oracle Cloud Infrastructure Object Storage Classic. When a file is retrieved from Oracle Cloud Infrastructure Object Storage Classic, the data is decrypted while it is being streamed to the local disk cache.

To enable encryption for a file system, you must select the Enable Encryption check box when you create the file system in the management console. After enabling encryption for a file system, you can generate encryption keys and specify the keys in the management console. When required, you can change the encryption keys.

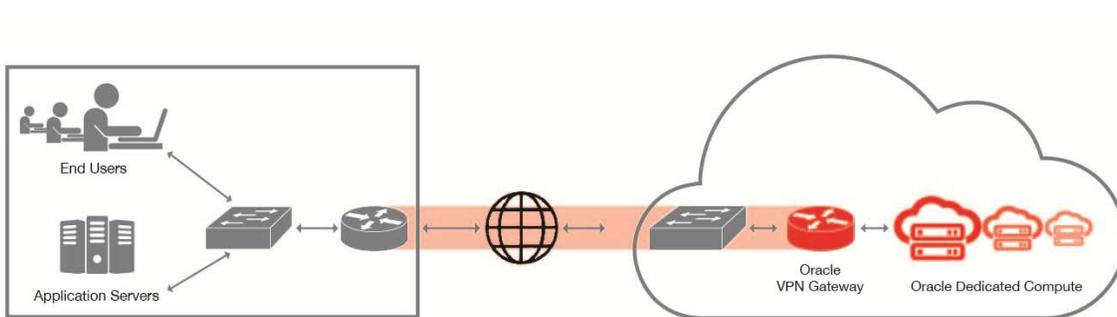
You control what needs to be encrypted by applying encryption at the container level. By controlling the encryption, you ensure that only sensitive assets are encrypted, which increases your storage efficiency. The built-in data integrity checks ensure that data is validated as it moves through the data path, to and from Oracle Cloud Infrastructure Object Storage Classic, enabling seamless end-to-end data integrity.

6.3 Oracle Cloud Infrastructure Networking Classic Security

Oracle Cloud provides a range of networking services that enable you to create a logically isolated network, establish a private network connection to the Oracle Cloud, and establish a deterministic route with predictable performance.

Site-to-Site VPN for Dedicated Compute

Oracle Cloud enables you to establish a secure connection from your Oracle Cloud Infrastructure Compute Classic zone by building a secure IPsec tunnel between the Oracle VPN gateway and the gateway installed in your data center.



Site-to-site VPN for dedicated compute has the following capabilities:

- » Multiple site-to-site tunnels can be set up with Oracle Cloud Infrastructure Compute Classic zone.
- » You can configure a range of IP addresses for compute instances.
- » Instances can access other Oracle services in the cloud.
- » External IP address can be configured for Internet access.
- » All the data between your data center and Oracle Dedicated Compute Cloud will be encrypted using a 128-bit AES symmetric key.
- » VPN devices are configured as a cluster for high availability.

Oracle Cloud REST API supports two models for site-to-site VPN:

- » **VPN gateway:** The VPN gateway model represents a network device that provides VPN gateway functionality. The gateway holds information to access the device, such as its IP address, login information, and the interface names of the interfaces associated with the zone.

- » **VPN endpoints:** The VPN endpoint model represents a VPN endpoint connected to a peer at the remote end of the VPN tunnel. A VPN endpoint is created on a VPN gateway. The model includes attributes such as the IP address of the peer, the pre-shared key to be used, the routes that are reachable via this endpoint, and whether or not the VPN connection is enabled.

Multitenant VPN Using Corente Cloud Services Exchange

Oracle Cloud Infrastructure Networking Classic offers a multitenant IPSec VPN solution, which uses a distributed virtual appliance located at the network edge that provides secure endpoints for virtual private networks over any IP networks with zero-touch installation. A services gateway is installed on customer data centers, and creates a secure end-to-end connection between customer data centers and Oracle Cloud.

FastConnect

Most enterprise applications are very sensitive to the variations in latency or the absolute latency itself. When applications on your private cloud (as in a hybrid cloud model) demand a level of consistent latency characteristics, the Internet falls short, and FastConnect addresses this by providing a fixed and consistent latency. FastConnect provides a private, high bandwidth connection between customer data centers and Oracle Cloud, offering more predictable network performance.

Transferring large amounts of data over the Internet is unpredictable, resulting in significantly lower performance or batch jobs not completing in time. As data transfer requirements increase, adding Internet capacity to your corporate network adds to the overall cost but with limited return or overall improvement in performance. FastConnect overcomes this problem by redirecting all Oracle Cloud traffic to a dedicated path, which improves the overall performance and also reduces the latency when collocated within the Equinix facility. Oracle offers a partner edition of FastConnect via Equinix Cloud Exchange.





As a customer of FastConnect Partner Edition via Equinix Cloud Exchange, you must meet the following prerequisites:

- » You must have network equipment capable of supporting Layer3 routing using BGP collocated at the Equinix IBX in the city where you want service.
- » You must establish connectivity with ECX –L3 in the city where you want service.
- » You must have a valid Oracle order for FastConnect Partner Edition with the appropriate port speed defined (currently 1 Gbps or 10 Gbps).
- » You must have a valid IP address and a valid Autonomous System Number (ASN) to establish a connection with Equinix Cloud Exchange. Work with your Internet service provider (ISP) or one of the registries to obtain an IP address and an ASN.

6.4 Oracle Database Cloud Service Security

Oracle Database Cloud Service provides the power and flexibility of Oracle Database in the cloud. You have the choice of a dedicated database instance with full administrative control or a dedicated pluggable database with a complete development and deployment platform managed by Oracle. In this document, we will elaborate specifically on the security capabilities of the full instance cloud service.

Oracle Database Cloud Service – Enterprise Edition provides dedicated virtual machines that are preconfigured and running Oracle Database 12c or Oracle Database 11g instances. Oracle Database Cloud Service offers general purpose and high memory virtual machine compute shapes that provide the full power of Oracle Database for any type of application, whether deploying production workloads or developing and testing. Oracle Database Cloud Service is ideal for businesses that want a full-featured Oracle database in the cloud, while retaining complete administrative control such as root OS and SYSDBA access. Oracle Database Cloud Service provides advanced cloud tooling for simpler management of the database including one-click automated backup with point-in-time recovery, one-click patching, and one-click upgrades.

The Exadata Cloud Service is similar to the Oracle Database Cloud Service. This Exadata Cloud Service gives you all the features and functionality of an Exadata Engineered System, but in the cloud. Customers can utilize the storage servers and flash cache for hyper fast queries, the hardware redundancy for superior uptime and high availability as well as flexible deployment options to fit every production workload. The Exadata Cloud Service enables customers to create their first database in hours, where traditionally on premises; this could take weeks or months. Simple provisioning through the UI, full OS access and advanced cloud tooling for patching, backup and recovery provide customers with a platform for deploying their production workloads with confidence.



SSH-Based Access

To securely access a port on a compute node associated with an Oracle Database Cloud Service or an Exadata Cloud Service instance, you use Secure Shell (SSH) client software that supports tunneling. When an Oracle Database Cloud instance is created, network access to the compute nodes of the service instance is provided by SSH connections on port 22.

Several SSH clients that support tunneling are freely available. You can use the `ssh` utility on the Linux platform. If you access your database instance from Windows, you can use PuTTY, which is a freely available SSH client program that supports SSH tunneling. After the SSH tunnel is created on Linux or Windows, you can access the port on the target compute node by specifying `localhost:local-port` on your system, where `local-port` is the source port you specified when you created the tunnel. MacOS has SSH installed by default.

When creating an Oracle Cloud Database, you must provide the service with a public encryption key. This key has a matching private key that only the customer has. Using these keys, access to the Cloud Database is restricted to only holders of the private key. If an access attempt is made using SSH where the matching private key is not presented, that access will be denied and logged.

Secure Access to Database Instances

Oracle Database Cloud Service relies on Oracle Cloud Infrastructure Compute Classic to provide secure network access to cloud database instances. You can use the Oracle Cloud Infrastructure Compute Classic console to perform network access operations such as enabling access to a port on a compute node associated with a cloud database. With the Exadata Cloud Service, network access is also controlled by the UI. Authorized users can allow network access to enter or exit the service using this console. Oracle does not have a copy of these keys.

Network Encryption and Integrity

Oracle Database Cloud Service customers can use database network encryption to secure connections to their cloud databases. With SSL/TLS, you can encrypt and optionally configure mutual authentication of database network connections. With Oracle native network encryption (SQLNet), you can encrypt and optionally execute integrity checking to prevent the modification of data in flight and



for illegitimate replay. These network encryption options support strong ciphers such as Advanced Encryption Standard (AES). Integrity checking supports modern hashing algorithms including SHA-2.

By default, Oracle Database Cloud instances and database clients are configured for Oracle native network encryption (SQLNet) and integrity checking. If a database client is later reconfigured to not use network encryption, then this potential threat is detected on the server, and the default server settings ensure the connection will be rejected.

Data-at-Rest Encryption

User-created database tablespaces where customers typically store their data are encrypted by default in all Oracle Database Cloud Service. New tablespaces you create with the `SQL CREATE TABLESPACE` command or any tool executing this command will be encrypted by default using the AES128 algorithm. The tablespace data file encryption is enabled in all standard and enterprise editions and versions of Oracle Database Cloud Service – Enterprise Edition as well as the Exadata Cloud Service.

Customers also can encrypt RMAN backups and Data Pump exports generated from cloud databases. Optimizations in the database pass through already encrypted tablespace data or encrypt the whole data stream where necessary. Backups and exports can be encrypted with the same key used by tablespace encryption, with a password, or both.

Master encryption keys used for data-at-rest encryption are created automatically by cloud databases and stored in a per-tenant Oracle wallet. The current key can be rotated periodically by a customer's authorized database security administrator using SQL commands. Historical master keys are retained in the Oracle wallet for encrypted backups that may need to be restored in the future. Customers with many cloud databases and proliferating Oracle wallets should use Oracle Key Vault (a separately licensable product) for centralized management of encryption keys and wallets. Oracle Key Vault is a security-hardened software appliance that runs in your data center, connecting to encrypted databases running in Oracle Cloud or on-premises.

Additional Security Controls

Oracle Database Cloud Service provides a number additional database security controls that can be used to protect essential cloud data. These optional controls are part of every database and can be configured after cloud database provisioning is complete.

Core controls include user privileges and user roles. As a best practice, you should grant only appropriate privileges and roles to cloud database users, following the security principle of least privilege. Cloud database auditing is another core control. You should use auditing to capture records of database actions and detect malicious activity. To get the most from auditing, it is recommended that you deploy Oracle Audit Vault and Database Firewall (separately licensed products). This enables you to move audit information to a central on-premises repository where you can run database activity reports and generate security alerts. It also provides database security firewall and monitoring capabilities that can track inbound SQL statements, giving you early warning of unauthorized database activity, and optionally blocking threats before they cause harm. Further security controls are available at no extra cost for particular cloud subscriptions and database releases. These are preventive controls you can configure to restrict access to your most sensitive or regulated data in Oracle Database Cloud Service. Many of these controls are unique in the database space and can be found only in Oracle databases.

Control	Description	Inclusions (Cloud Subscriptions)				Availability (Database Release)	
		Enterprise Edition	High Perf.	Extreme Perf.	Exadata Service	Oracle Database 12c	Oracle Database 11gR2
Advanced Security Data Redaction	Redacts sensitive cloud data from query results before display by applications. Enforces redaction at runtime, with low overhead, and according to conditions set in policies.		Yes	Yes	Yes	Yes	Yes
Database Vault	Reduces risk exposure coming from powerful database users such as a DBA and privileged application connections. Restricts operations these privileged accounts can perform. Enforced based on runtime conditions and factors.		Yes	Yes	Yes	Yes	Yes
Label Security	Implements concepts of U.S. Department of Defense Multi-Level Security (MLS), enabling rows with differing sensitivity to reside in the same table. Explicitly labels rows in cloud databases with group, compartment, and sensitivity levels.		Yes	Yes	Yes	Yes	Yes



Real Application Security	Provides a framework for application developers to define light-weight database user accounts (with no schema) and detailed object authorizations. Enables developers to author their security model once in an Oracle Database tier and reuse this model across multiple custom applications.	Yes	Yes	Yes	Yes	Yes	
---------------------------	--	-----	-----	-----	-----	-----	--

You also can use databases running in Oracle Database Cloud Service as data sources for Oracle Data Masking and Subsetting Pack, an optional pack of Oracle Enterprise Manager 12c. This important security control makes it easy to create sanitized copies of production cloud data for use by business partners in non-production environments such as development and test databases. A data source license for Oracle Data Masking and Subsetting Pack is included with High Performance, Extreme Performance, and Exadata Service subscriptions. It can be used with Oracle Database 11g R2 or Oracle Database 12c. For the most up to date security information on the Oracle Database please refer to the following URL:

<http://www.oracle.com/technetwork/database/security/overview/index.html>

6.5 Oracle Java Cloud Service Security

Oracle Java Cloud Service is a complete platform and infrastructure cloud solution for building, deploying, and managing Java EE applications. You get the industry's best application server running on top of an enterprise-grade cloud infrastructure. The platform is powered by Oracle WebLogic Server, the number one application server across conventional and cloud environments. You also have the option of adding an Oracle Coherence caching and data grid tier to your deployment.

Your environment is preinstalled and preconfigured using Oracle best practices for application deployment that maximize performance, scalability, and reliability. The infrastructure has the same core security capabilities as those offered by Oracle Cloud Infrastructure as a Service. With features like elastic compute and storage, you can run any workload in Oracle Java Cloud Service and grow your environment when your application needs to grow.

You secure all applications deployed to an Oracle Java Cloud Service instance the same way you secure an application environment and administer security for Oracle WebLogic Server in an on-premises instance.



The default security configuration makes use of users, groups, security roles, and security policies that are configured in the default authentication, authorization, credential mapping, and role mapping security providers. By default, the WebLogic Server security providers are configured in the default security realm, and the WebLogic Server embedded LDAP server is used as the data store for the security providers.

To use the default security configuration in your Oracle Java Cloud Service instance, use the WebLogic Server Administration Console to define users, groups, and security roles for the security realm, and create security policies to protect the WebLogic Server resources in the domain.

If the default security configuration doesn't meet your requirements, then you can create a new security realm with any combination of WebLogic Server and custom security providers. Then, you set the new security realm as the default security realm. Oracle recommends that you use an identity management system such as Oracle Identity Management for your production applications instead of the embedded LDAP server.

Users and Roles

Oracle Java Cloud Service uses roles to control access to tasks and resources. When the Oracle Java Cloud Service account is set up, the service administrator is given the Java administrator role and other service roles that are required to work with related Oracle Cloud services. Before anyone can access and use Oracle Java Cloud Service, user accounts with the Java administrator role and other service roles, as needed, must be created. Only the identity domain administrator can create user accounts and assign roles.

The users with the Java administrator role can perform many operations on the service instance such as create, delete, start, stop, scale, patch, back up, and restore. These users can also administer load balancers for service instances as well as monitor and manage the service usage in Oracle Cloud.

When Oracle Coherence is enabled for a service instance, the Java administrator can remove an Oracle Coherence data tier from a service instance (REST API only) and add an Oracle Coherence data tier to an existing service instance (REST API only).

When you create an Oracle Java Cloud Service instance, the following Oracle Cloud Infrastructure Compute Classic VM and Oracle WebLogic Server administrative user accounts are created:

- 
- » The VM operating system user, `opc`, has root privileges on the operating system running on a VM. The user can connect to a VM through SSH for direct VM-level access to an Oracle Java Cloud Service instance. The `opc` user can create other OS accounts on a VM using the appropriate OS tool through the SSH interface. The `oracle` user can't be used to log in to a machine. This user only has regular user permissions to start and stop Oracle products that were installed on the machine.
 - » The WebLogic Server administrator can manage Oracle WebLogic Server in Oracle Java Cloud Service, and can access and use the WebLogic Server Administration Console. The WebLogic administrator can also manage users and groups in the embedded LDAP as well as configure other identity providers.

Note that the WebLogic Server administrator account and VM OS user accounts aren't stored or managed in Oracle Cloud. You provide the user name and password for the WebLogic Server administrator when you create an Oracle Java Cloud Service instance. The credentials and permissions for the WebLogic Server administrator and all user accounts that the administrator creates are stored and managed in Oracle WebLogic Server. See the online WebLogic Server security documents for details about securing your Oracle Java Cloud instances using the WebLogic Server security capabilities.

6.6 Oracle Management Cloud Security

Oracle Management Cloud (OMC) is a suite of next-generation integrated monitoring, management, and analytics cloud services, built on a scalable big data platform that provides real-time analysis and deep technical and business insights. By using OMC, customers can eliminate multiple information silos, resolve application issues faster, and run IT like a business.

OMC includes the following: Oracle Application Performance Monitoring Cloud Service, Oracle Log Analytics Cloud Service, Oracle IT Analytics Cloud Service and Oracle Infrastructure Monitoring Cloud Service. Customers may subscribe to one or more of these services.

Service-specific data is uploaded to Oracle Management Cloud's unified data platform. Customers can access this data through the graphical user interface or application programmable interfaces (API) to monitor the performance of their applications and troubleshoot a problem by analyzing logs, or perform capacity planning for their IT infrastructure. These OMC services are available on Oracle Cloud. From security point of view, these are categorized as Software as a Service (aka SaaS) offerings.

OMC Services run in secured Oracle Cloud infrastructure. This section discusses additional OMC specific security capabilities.



Type of Data Uploaded to Oracle Management Cloud

Data from customer's application and computing infrastructure is uploaded using Oracle Management Cloud agents. Collection of every type of data needs to be explicitly enabled by customer. Cloud Service agents will use read-only access to the sources of data at runtime.

Below are some of the categories of data uploaded to Oracle Management Cloud:

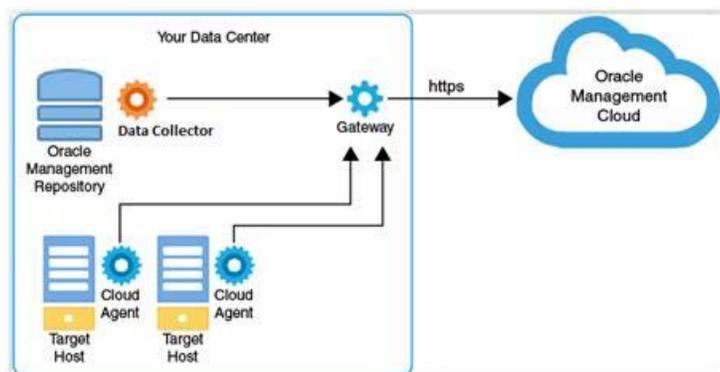
- » *Application Performance Monitoring Data*: This includes performance statistics of applications monitored by the service.
- » *Log Data*: This includes application, platform, and infrastructure log files across customer's computing infrastructure.
- » *Automatic Workload Repository (AWR) of Oracle Databases*: This performance statistics of Oracle Databases collected automatically.
- » *Enterprise Manager Data*: This data is collected from the assets that are monitored by the customer's on-premise Enterprise Manager Cloud Control. The collected data is stored in the associated repository. The data includes configuration data, performance metrics and event information about the targets managed by Enterprise Manager Cloud Control.

Agent Connection to Cloud

All traffic between customer's systems and Oracle Management Cloud is secured using TLS encryption. This encryption applies to data sent over network by agents as well as user access to Web Based applications

Oracle Management Cloud Agents connect to Oracle Management Cloud over the Internet using secured HTTPS protocol. Hence only outbound HTTPS connectivity is needed from customer's datacenter to Oracle Management Cloud. This obviates the need for any complex VPC/VPN setup.

Additionally, outbound Oracle Management Cloud agent connections can be routed thru an Oracle Management Cloud Gateway Server which can be the point of egress from customer's data center to Oracle Management Cloud. The Gateway Server can be deployed in a network zone which has access to customer's internal network and public internet. This ensures that all the servers which are managed by Oracle Management Cloud can continue to be safely deployed in customer's internal network without requiring any outbound internet access.



Data Isolation

Each customer's data is isolated in the multi-tenant infrastructure of Oracle Cloud services. This includes Oracle's industry leading multi-tenant database. Data stored in files is separated by each customer. Network traffic for each customer is logically isolated using separate URLs, routing rules, Access Controls. Data isolation is maintained for archived data stores like backups.

Identity and Access Management

All users accessing Oracle Management Cloud is secured using Oracle Cloud's shared Identity and Access management solution.

Cloud Agents which are used to automatically upload machine data to Oracle Cloud are also authenticated. Agent Identity is validated using keys and tokens issued at by Oracle Management Cloud which are customer specific. These keys and tokens could be revoked by the customer at anytime invalidating the agent.

API Access

Oracle Management Cloud exposes RESTful APIs for access to data. All APIs are secured using HTTPS and are protected by authentication. Additionally, customers will need to provide unique identifiers issued to them for any API access. Every API call is authenticated.



7. Oracle's Approach to Engineering Secure Cloud Services

The Oracle Cloud Services development process follows the Oracle Software Security Assurance (OSSA) program. The OSSA is Oracle's methodology for incorporating security into the design, building, testing, and maintenance of its services.

From initial architecture considerations to service post-release, all aspects of cloud services development consider security. Here is a summary of secure software development phases we go through:

- » Design Phase: Security training about guiding security principles and Oracle's secure coding standards help ensure that our engineers, architects and product managers make the best security decisions possible. Assessing threats during architectural risk analysis meetings help us identify potential security issues as early in the development lifecycle as possible.
- » Coding Phase: We address standard vulnerability types through the use of secure coding standards and patterns. In this phase we use static code analysis tools to identify security flaws and fix all significant security findings before our services move to testing phase.
- » Testing Phase: Our internal security professionals and independent security consultants use Oracle internal tools, third party tools for dynamic analysis and fuzz testing, and manual testing to identify potential security issues.
- » Prior to service release: Before we release a cloud service, Oracle validates that the functionality being developed meets Oracle's cloud security requirements. We use independent security professionals to evaluate and monitor the product for potential security issues.

See the [Oracle Software Security Assurance](#) online documents to learn more about OSSA.



8. Conclusion

The protection of customer data is a primary design consideration for all of Oracle's Cloud infrastructure and services. Oracle Cloud was developed to offer secure infrastructure and platform services that are used by Oracle customers to run their mission-critical enterprise workloads and store their data. Oracle believes that it has the right security philosophy, strategy, proven expertise, and resources to protect customer data and enable customers to build secure and private cloud solutions. Oracle is fully committed to continuing to invest in security capabilities to create the most secure public cloud infrastructure and trusted cloud services. These capabilities enable Oracle customers to have effective and manageable security, to run their workloads with more confidence, and to build trusted hybrid cloud solutions.



Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0116

Oracle Cloud Infrastructure Classic and Platform Cloud Services Security
November 2017



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