Cloud Engineering

Week 10 Intro

SWINBURNE UNIVERSITY OF TECHNOLOGY

Typical Week

Watch Lecture Videos for the week before your first class

Attend every Q&A session – useful assessment tips

Attend every Lab

- Read Entire Instructions before Class
- Can get ahead on labs using Lab Reports to free up time

Start working on assignments and preparing for tests early

Typical Week

Consultation

- Every Teaching Week
- Underutilised

Discussion Board on Swinburne Canvas

- General questions

Lectures to watch

Swinburne Lectures

- High Level Overview
- Needed to pass

Oracle Lecture Videos

- Deep Dive
- More Topics and More Depth
- Aiming for high marks
- Prepare for certification

Week 10 Intro

This week:

Security

- IAM Policies
- Data Encryption
- WAF
- Monitoring

Billing and Cost Management

Security

Week 10 Intro – Security

Security

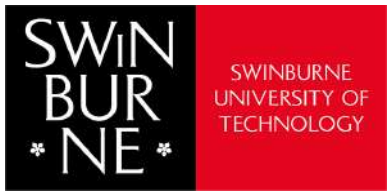
IAM Policies

Data Encryption

WAF

Monitoring

Billing and Cost Management



Billing and Cost Management

Cost Analysis and Budgets

Service Limits and Quotas

Next week

Next Week

Multi-Cloud

Lecture References

Recommend Viewing

Swinburne Lecture – High Level Overview

Oracle Academy – Deeper dive

Cloud Engineering

Identity and Access Management (IAM) Policies

SWINBURNE UNIVERSITY OF TECHNOLOGY

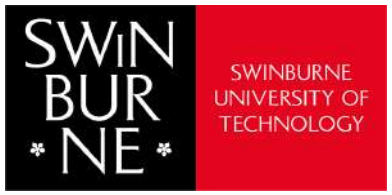
Identity and Access Management (IAM) Policies

This Presentation:

IAM

- Principle of least privilege
- Compartments
- Principals, Authentication (AuthN), Authorization (AuthN)
- IAM Policies

The Principle of Least Privilege



Principal of Least Privilege

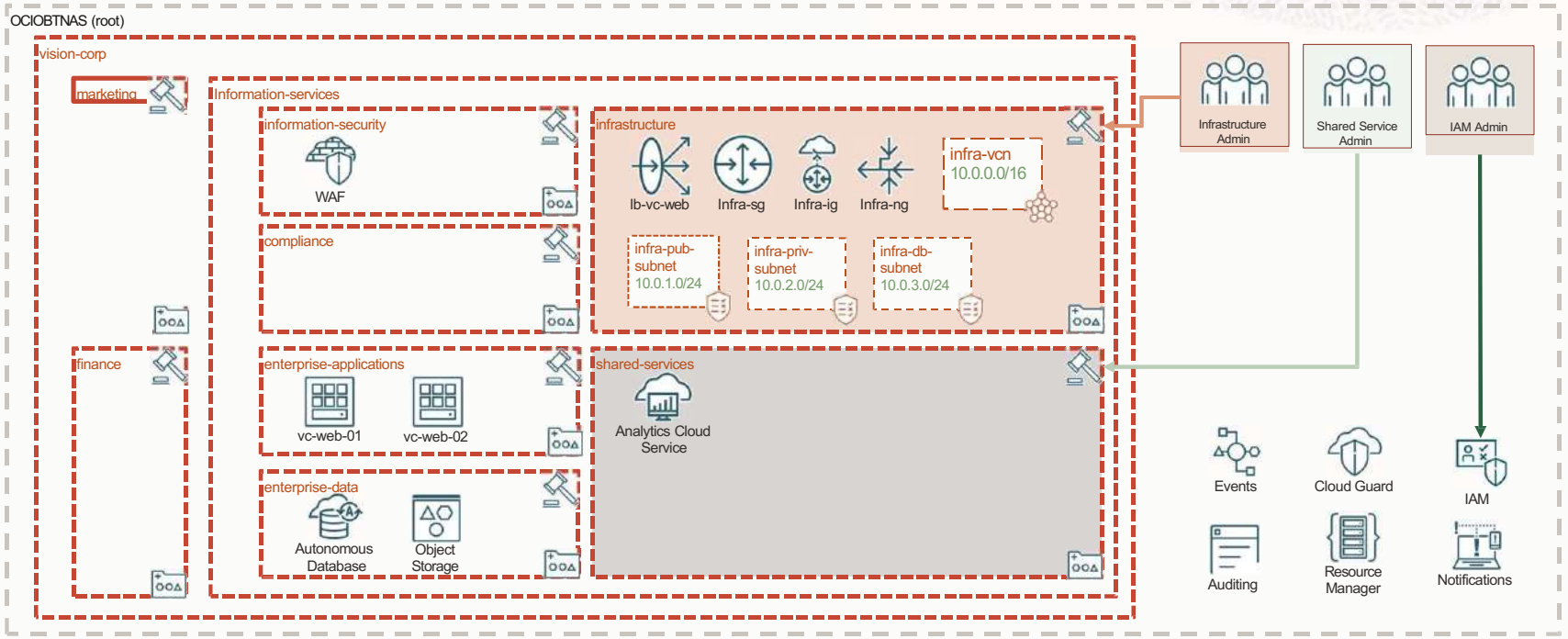
Only minimum necessary permissions

e.g. consider Risk of user getting compromised

Compartments

Compartments

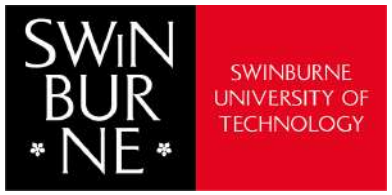
A compartment is a logical grouping of related resources that can be accessed only by groups that have been given permission



Compartment

- A compartment is a collection of related resources (VCN, instances,..) that can be accessed only by groups that have been given permission (by an administrator in your organization)
- Compartments help you organize and control access to your resources
- Design considerations:
  - Each resource belongs to a single compartment but resources can be connected/shared across compartments (VCN and its subnets can live in different compartments)
  - A compartment can be deleted after creation or renamed
  - A compartment can have sub compartments that can be up to six levels deep
  - Most resources can be moved to a different compartment after they are created (some restrictions apply)
  - After creating a compartment, you need to write at least one policy for it, otherwise it cannot be accessed (except by administrators or users who have permission to the tenancy)
  - Sub compartment inherits access permissions from compartments higher up its hierarchy
  - When you create a policy, you need to specify which compartment to attach it to

Principals, Authentication and Authorization



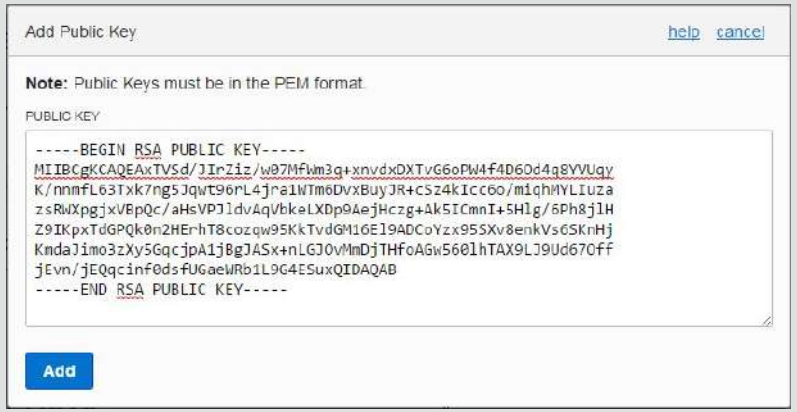
Principals

- A principal is an IAM entity that is allowed to interact with OCI resources
- Principals – IAM users and Instance Principals
- **IAM Users and Groups**
  - Users are persistent identities setup through IAM service to represent individual people or applications
  - When customers sign-up for an OCI account, the first IAM user is the default administrator
  - Default administrator sets up other IAM users and groups
  - Users enforce security principle of least privilege
    1. User has no permissions until placed in one (or more) groups and
    2. Group having at least one policy with permission to tenancy or a compartment
  - A Group is a collection of users who all need the same type of access to a particular set of resources
  - Same user can be member of multiple groups
- **Instance Principals**
  - Instance Principals lets instances (and applications) to make API calls against other OCI services removing the need to configure user credentials or a configuration file

Authentication

IAM service authenticates a Principal by –

- **Username, Password**
  - You use the password to sign in to the web console
  - An administrator will provide you with a one-time password when setting up your account
  - At your first log in, you are prompted to reset the password
- API Signing Key
  - Required when using the OCI API in conjunction with the SDK/CLI
  - Key is an RSA key pair in the PEM format (min 2048 bits)
  - In OCI Console, copy and paste the contents of the PEM public key file. Use the private key with the SDK or with your own client to sign your API requests
- Auth Tokens
  - Oracle-generated token strings to authenticate with 3rd party APIs that do no support OCI signature-based authentication (e.g. ADW)
  - Auth tokens do not expire




```
begin
 DBMS_CLOUD.create_credential (
     credential_name => 'OBJ_STORE_CRED',
     username => '<userXX>',
     password => '<your Auth Token>'
  ) ;
end;
/
```

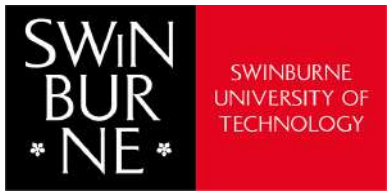
ORACLE Academy

Authorization

- Authorization specifies various actions an authenticated Principal can perform
- OCI Authorization - define specific privileges in policies and associating them with principals
- Supports security principle of least privilege; by default, users are not allowed to perform any actions (policies cannot be attached to users, but only groups)
- Policies are comprised of one or more statements which specify what groups can access what resources and at what level of access
- Policies are written in human-readable format:
  - Allow group **<group_name>** to **<verb>** **<resource-type>** in tenancy
  - Allow group **<group_name>** to **<verb>** **<resource-type>** in compartment **<compartment_name>** [where **<conditions>**]
- Policy Attachment: Policies can be attached to a compartment or the tenancy. Where you attach it controls who can then modify it or delete it

ORACLE Academy

IAM Policies



Policy Syntax

Allow **<subject>** to **<verb>** **<resource-type>** in **<location>** where **<conditions>**

Verb	Type of access
inspect	Ability to list resources
read	Includes inspect + ability to get user-specified metadata/actual resource
use	Includes read + ability to work with existing resources (the actions vary by resource type)*
manage	Includes all permissions for the resource

* In general, this verb does not include the ability to create or delete that type of resource

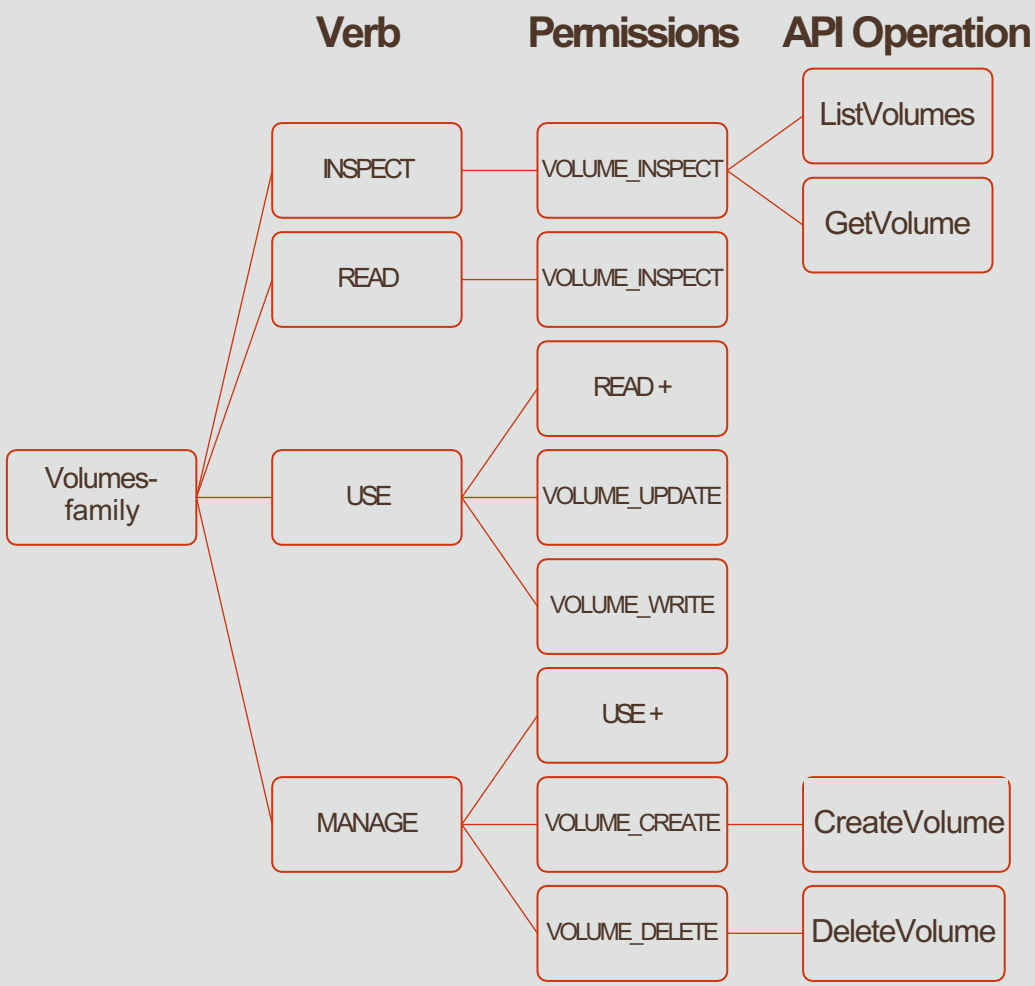
Aggregate resource-type	Individual resource type
all-resources	
database-family	db-systems, db-nodes, db-homes, databases
instance-family	instances, instance-images, volume-attachments, console-histories
object-family	buckets, objects
virtual-network-family	vcn, subnet, route-tables, security-lists, dhcp-options, and many more resources (link)
volume-family	volumes, volume-attachments, volume-backups
Cluster-family	clusters, cluster-node-pool, cluster-work-requests
File-family	file-systems, mount-targets, export-sets
dns	dns-zones, dns-records, dns-traffic,..

The IAM Service has no family resource-type, only individual ones

ORACLE Academy

Verbs & Permissions

- When you write a policy giving a group access to a particular verb and resource-type, you're actually giving that group access to one or more predefined permissions
- Permissions are the atomic units of authorization that control a user's ability to perform operations on resources
- As you go from inspect > read > use > manage, the level of access generally increases, and the permissions granted are cumulative
- Each API operation requires the caller to have access to one or more permissions. E.g., to use ListVolumes or GetVolume, you must have access to a single permission: VOLUME_INSPECT



ORACLE Academy

Common Policies

1. Network Admins manage a cloud network
   - Allow group NetworkAdmins to **manage virtual-network-family** in **tenancy**
2. Users launch compute instances
   - Allow group InstanceLaunchers to **manage instance-family** in compartment ABC
   - Allow group InstanceLaunchers to **read app-catalog-listing** in tenancy
   - Allow group InstanceLaunchers to **use volume-family** in compartment ABC
   - Allow group InstanceLaunchers to **use virtual-network-family** in compartment XYZ

https://docs.cloud.oracle.com/iaas/Content/Identity/Concepts/commonpolicies.htm

Advanced Policy Syntax

- As part of a policy statement, you can specify one or more conditions that must be met to get access
- Allow <subject> to <verb> <resource-type> in <location> where **<conditions>**
- You use variables when adding conditions to a policy; 2 types
  - **request** – relevant to the request itself
  - **target** – relevant to the resource(s) being acted upon in the request)
  - E.g. variable request.operation represents the API operation being requested (e.g. ListUsers); target.group.name rep the name of the group
- Variable name is prefixed accordingly with either request or target followed by a period
- Examples:
  - Allow group Phoenix-Admins to manage all-resources in tenancy where request.region='phx'

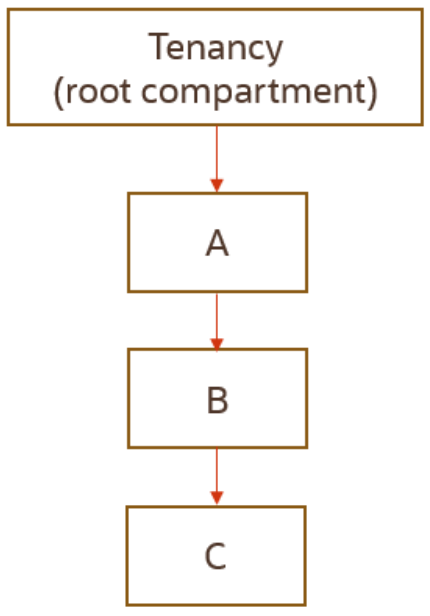
-

https://docs.cloud.oracle.com/iaas/Content/Identity/Reference/policyreference.htm#Resource

Policy Inheritance and Attachment

Policy Inheritance

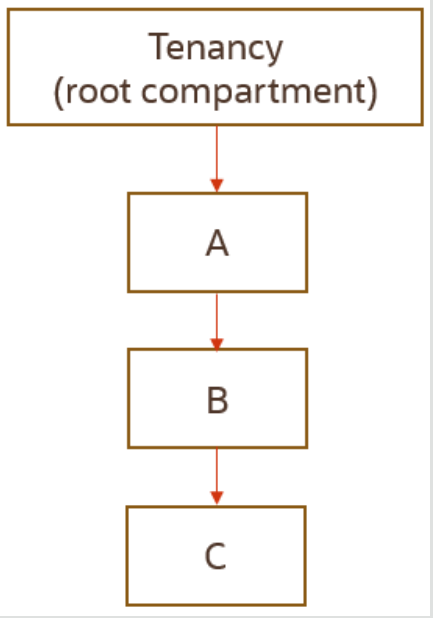
- Concept of inheritance: Compartments inherit any policies from their parent compartment
  - E.g. OCI has a built-in policy for Administrators, Allow group Administrators to manage all-resources in tenancy
  - Due to Policy Inheritance, the Administrators group can also do anything in any of the compartments in the tenancy
- Three levels of compartments: A, B, and C
  - Policies that apply to resources in Compartment A also apply to resources in Compartments B and C
  - Allow group NewtworkAdmins to manage virtual-network-family in compartment A allows the group NetworkAdmins to manage VCNs in Compartment A, B, and C



ORACLE Academy

Policy Attachment

- Concept of attachment: when you create a policy you must attach it to a compartment (or tenancy). Where you attach it controls who can then modify it or delete it
  - Attach it to tenancy (root compartment), then anyone with access to manage policies in the tenancy can then change or delete it.
  - Attach to a child compartment, then anyone with access to manage the policies in that compartment (e.g. compartment admins) can change or delete it
- You want to create a policy to allow NetworkAdmins to manage VCNs in Compartment C. Attach to:
  - C or B – Allow group NewtworkAdmins to manage virtual-network-family in compartment C
  - A – Allow group NewtworkAdmins to manage virtual-network-family in compartment B:C
    - Only Compartment A admins can modify it
    - NetworkAdmins can still only manage VCNs in Compartment C
  - Tenancy – Allow group NewtworkAdmins to manage virtual-network-family in compartment A:B:C



ORACLE Academy

References

References

Oracle Cloud Academy Foundations I Section 23

Day One and Beyond - Season 4 - Oracle Cloud Technical Quick Start:
https://www.youtube.com/watch?v=8kYEYNMK4zg

Cloud Engineering

Web Application Firewall (WAF)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Web Application Firewall (WAF)

This Presentation:

WAF

- Background
- What is a WAF
- OCI WAF
  - OWASP

Background

OSI Model

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Core to Edge Security

Security	Description
Edge Security	WAF
Access Security	IAM
Data Security	At-rest and In-Transit encryption
Network Security	Off-box virtualisation
Physical Security	Physical Isolation, Datacentre security

OSI Model - Application Layer (Layer 7)

HTTP/S

Telnet

SSH

FTP

SMTP

DNS

HTTP/S

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTPS)

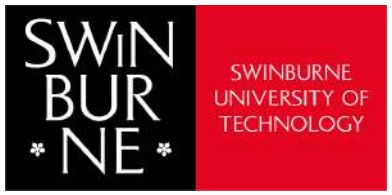
Web Application Firewall

Cybersecurity threats are growing

Hackers exploit vulnerabilities

- Weak targets
- Rich Targets

What is a Web Application Firewall?



Web Application Firewall

Uses Rules

- Filters HTTP/S Traffic
- Detect Threats
- Protect Against Common Attacks
    - Cross-Site Scripting (XSS)
    - SQL Injection
    - Specific IPs
    - Bad Bots

Web Application Firewall

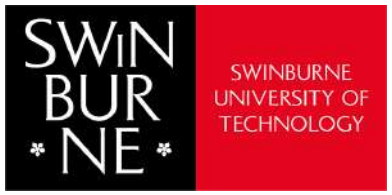
Handling Traffic

Good Traffic – Allow

Monitor Traffic – Audit Log

Bad Traffic – Block

OCI Web Application Firewall



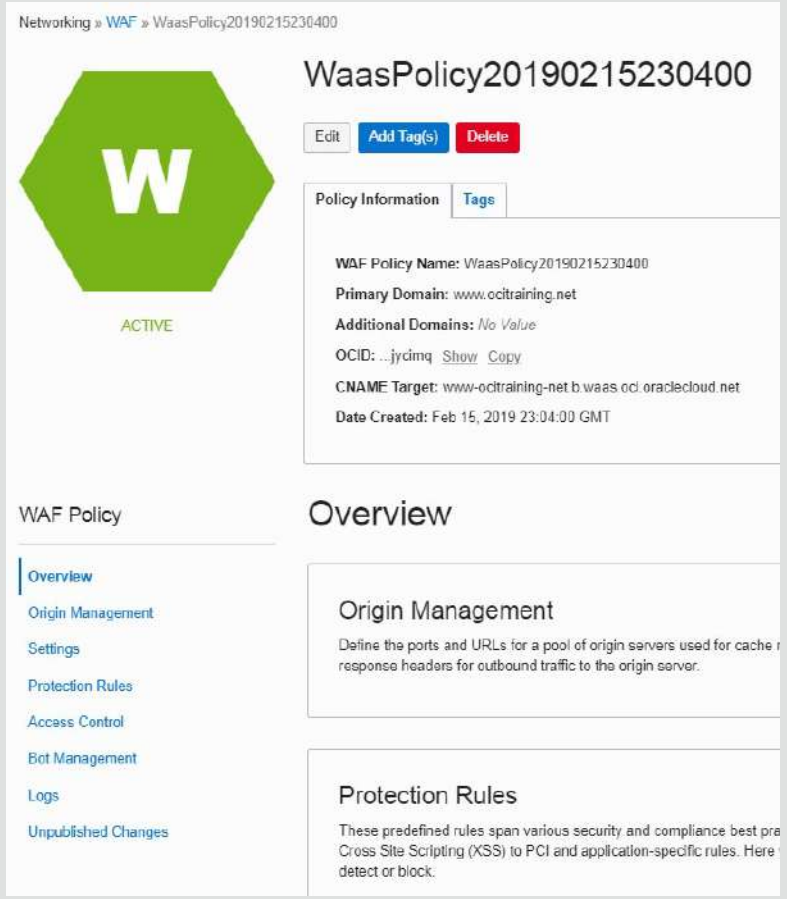
OCI Web Application Firewall

- OCI Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic
- Use cases:
  - Protect any internet-facing endpoint from cyberattacks and malicious actors
  - Protect against cross-site scripting (XSS) and SQL injection, activities that allow attackers to gain unauthorized access to privileged information
  - Bot management – dynamically blocking bad bots
  - Protection against layer 7 distributed denial-of-service (DDoS) attacks
  - Aggregated threat intelligence from multiple sources including Webroot BrightCloud

ORACLE Academy

Key OCI WAF Components

- Supports over 250 rulesets to protect against SQL injection, cross-site scripting, HTML injection, and many more threats
- JavaScript Challenge, CAPTCHA Challenge, Device Fingerprint Challenge and white listing capabilities work in conjunction with rulesets to further detect and mitigate bad bots and allow legitimate human and bot traffic
- User access controls can be configured on the basis of countries, IP addresses, URLs, and other request attributes to prohibit risky traffic
- Multi-cloud support provides WAF protection for any internet-facing application in any environment: OCI, on-premises, and across multi-cloud deployments



ORACLE Academy

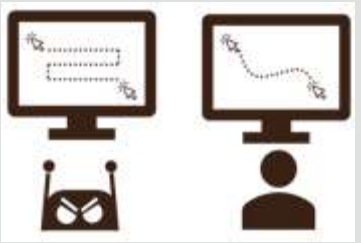
OCI WAF Rulesets

- OCI WAF uses OWASP ModSecurity Core Rule Set to protect against the most common web vulnerabilities. These rules are managed and maintained by the open source community.
- OCI WAF comes pre-configured with protection against the most important threats on the Internet as defined by OWASP Top 10. These include:
  - A1 – Injections (SQL, LDAP, OS, etc.)
  - A2 – Broken Authentication and Session Management
  - A3 – Cross-site Scripting (XSS)
  - A4 – Insecure Direct Object References
  - A6 – Sensitive Data Exposure
  - A7 – Missing Function-Level Access Control
- Each type of vulnerability ruleset is shown within the OCI console, with granular controls for each specific rule.

Challenges and Whitelisting Capabilities

- JavaScript Challenge: fast and efficient way to block a large percentage of bot attacks
  - After receiving an HTTP request, a piece of JavaScript is sent back to the browser of every client, attacker, and real user. It instructs the browser to perform an action. Legitimate browsers will pass the challenge without the user's knowledge, while bots—which are typically not equipped with JavaScript—will fail and be blocked
- CAPTCHA Challenge
  - If a specific URL should be accessed only by a human, you can control it with CAPTCHA protection.
  - You can customize the comments for the CAPTCHA Challenge for each URL
- Whitelisting: Allows you to manage which IP addresses appear on the IP whitelist
  - Requests from the whitelisted IP addresses bypass all challenges, such as DDoS policies and WAF rulesets.

Bot Management



Entity Attributes and Behavioral Detection

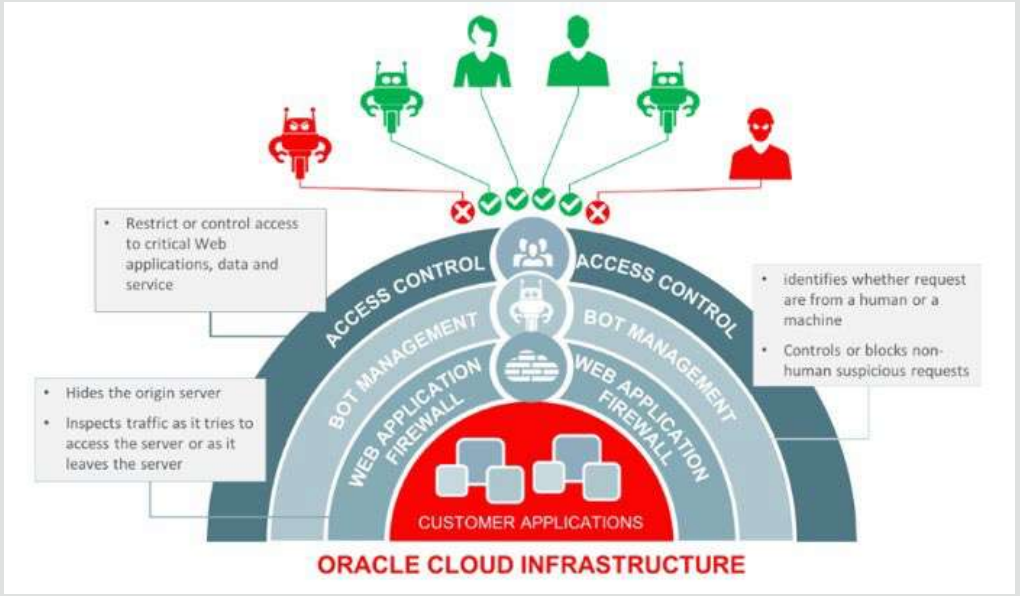
- Human Interaction
  - Oracle WAF identifies normal usage patterns based on legitimate user behavior to the site. The WAF will challenge with CAPTCHA or block requests when it detects abnormalities or traffic exceeds defined interaction thresholds.

- Device Fingerprinting (available in the API)
  - Oracle WAF collects unique various characteristics about a device entity, generating a hashed signature. This hashed signature is then compared to other requests to determine the same signature is being leverages across different contexts.

Access Controls

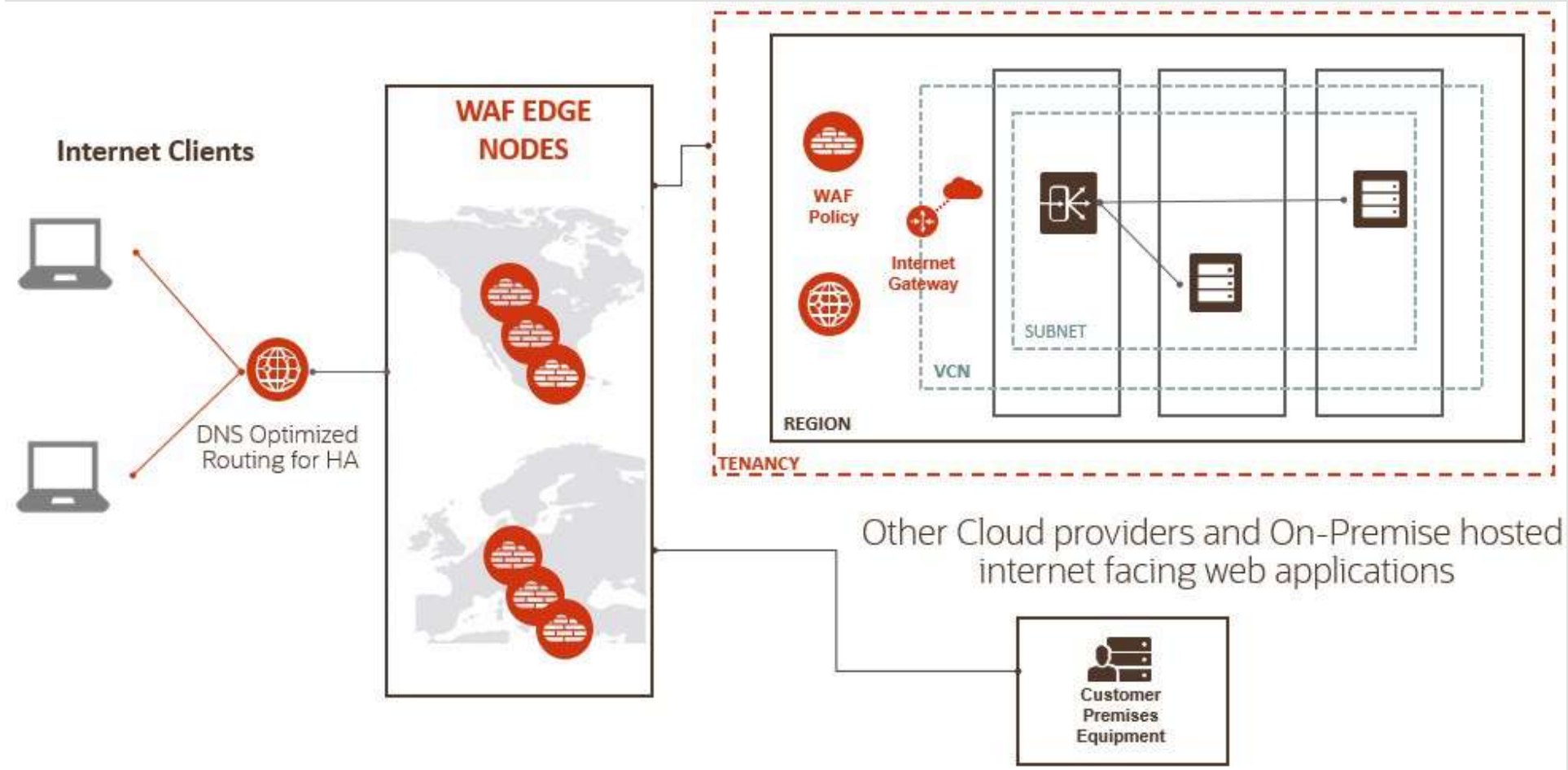
Use the access controls to restrict or control access to your critical web applications, data and services. E.g., in some cases, an offering may need to stay within a specific country. Regional access control can be used to restrict users from certain geographies.

- Control access, based on HTTP header information. Block requests if the HTTP header contains specific names or values or allow raffic with proper HTTP regular expression
- Control access based on URL address matching or partial matching or match proper URL regular expressions



ORACLE Academy

Oracle Cloud Infrastructure WAF Architecture



Shared Responsibility Model for WAF

Responsibility	Oracle	Customer
Configure WAF on-boarding dependencies (DNS, Ingress rules, network)	No	Yes
On-board/Configure the WAF policy for the web application	No	Yes
Construct new rules based on the new vulnerabilities and mitigations	Yes	No
Review and accept new recommended rules	No	Yes
Keep WAF infrastructure patched and up-to-date	Yes	No
Monitor data-plane logs for abnormal, undesired behavior	Yes	Yes
Monitor for Distributed Denial of Services (DDoS) attacks	Yes	No
Provide High Availability (HA) for the WAF	Yes	No
Tune the WAF's access rules and bot management strategies for your traffic	No	Yes

Benefits of Oracle Cloud Infrastructure WAF

- Consolidate threat intelligence
- Push malicious traffic farther away from your origin
- Augment your Security Operations Center (SOC)
- Better Visibility into internet traffic metrics
- Consolidate governance through policies, audit, and tagging
- Off-load patching and maintenance of Web Application Firewall
- Global traffic management and optimization
- Consolidate WAF policy for OCI and non-OCI applications
- Low cost

References

References

Oracle Cloud Academy Foundations I Section 15

https://blogs.oracle.com/cloud-infrastructure/post/core-to-edge-security-the-oracle-cloud-infrastructure-edge-network

https://www.oracle.com/au/security/cloud-security/isolated-network-virtualization/#prevent

Cloud Generation 2: Larry Ellison Keynote at Oracle OpenWorld 2018: https://www.youtube.com/watch?v=b5qZVk0F_yg

Cloud Engineering

Data Encryption

SWINBURNE UNIVERSITY OF TECHNOLOGY

Data Encryption

This Presentation:

- Encryption at Rest
- Encryption in Transit

Core to Edge Security

Security	Description
Edge Security	WAF
Access Security	IAM
Data Security	At-rest and In-Transit encryption
Network Security	Off-box virtualisation
Physical Security	Physical Isolation, Datacentre security

Why Encrypt?

Data Breaches

- Loss of Customer Trust
- Legal Action
- Financial losses
- Go Broke

Encryption at Rest

Where data is stored

- Block Volume
- File Storage
- Object Storage

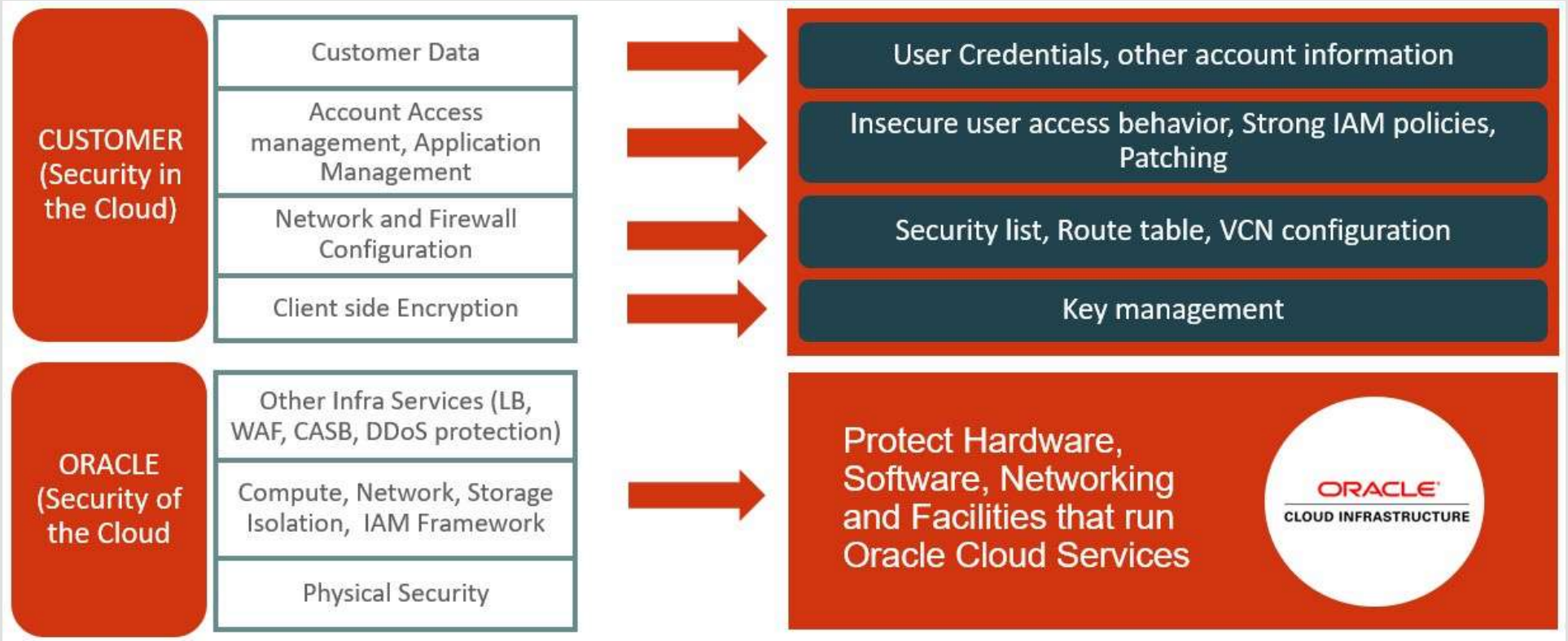
Encryption in Transit

When data is moving

Around the Cloud

Between customer and the Cloud

Shared Responsibility Model in Oracle Cloud Infrastructure



Oracle Cloud Infrastructure Security Capabilities At a Glance

1	**Customer Isolation**	Bare Metal Instance, VM Instance, VCN IAM, Compartments
2	**Data Encryption**	Default Encryption for Storage, Key Management, DB Encryption
3	**Security Controls**	User Authentication and Authorization, Instance Principals, Network Security Control, Web Access Firewall
4	**Visibility**	Audit Logs, CASB Based monitoring and enforcement
5	**Secure Hybrid Cloud**	Identity Federation Third Party Security Solution, IPSEC VPN, Fast Connect
6	**High Availability**	Fault-independent data center, Fault Domain, SLA
7	**Verifiably Secure Infrastructure**	Security Operations, Compliance Certification and Attestation, Customer penetration and Vulnerability testing

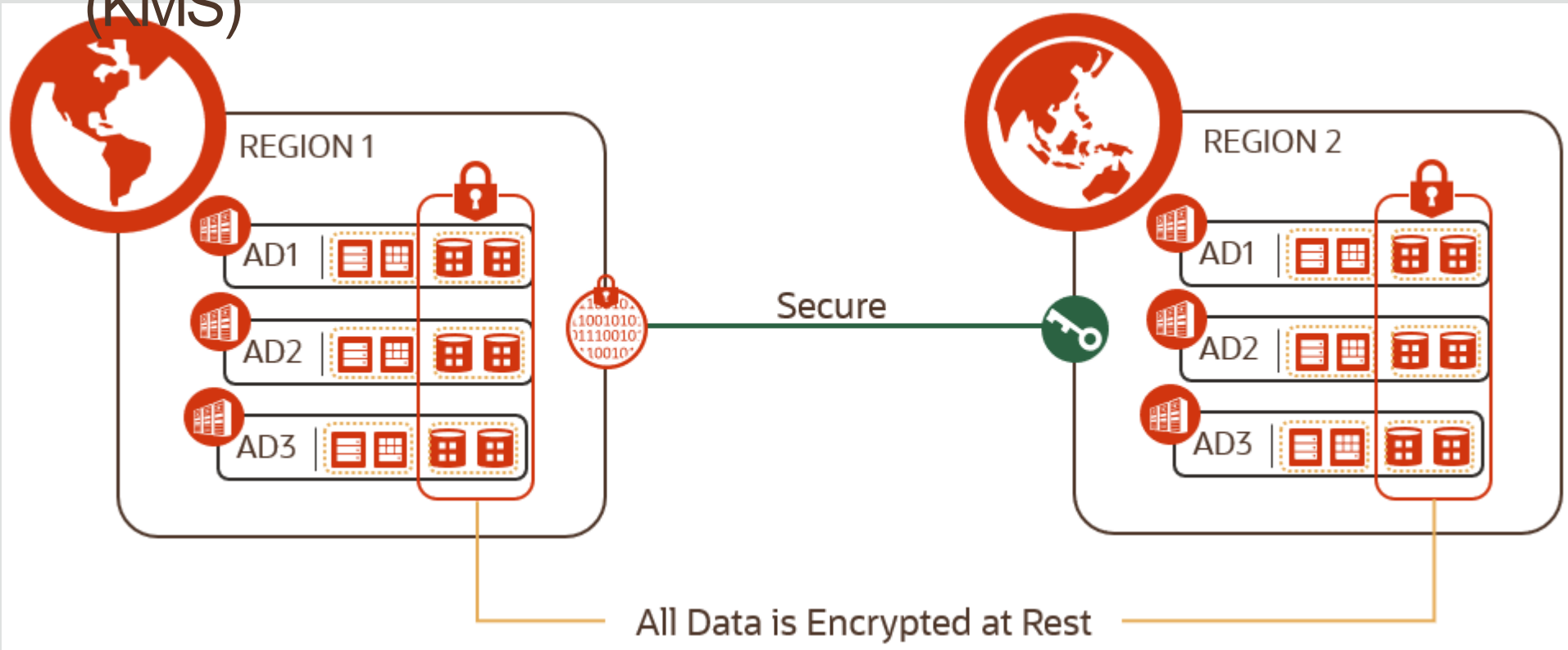
ORACLE
Academy

Storage Encryption

- Block Storage and Remote Boot Volumes
  - Volumes and backups encrypted at rest using AES 256-bit key (keys managed by Oracle)
  - Data moving between instance and block volume is transferred over internal and highly secure network.
  - in-transit encryption can be enabled (paravirtualized volume attachments.)
- Object Storage
  - Client-side encryption using customer keys
  - Data encrypted with per-object keys managed by Oracle
  - All traffic to and from Object Storage service encrypted using TLS
  - Object integrity verification
- File System Storage
  - Encrypted at rest and between backends (NFS servers and storage servers)
- Data Transfer Service
  - Uses standard Linux dm-crypt and LUKS utilities to encrypt block devices

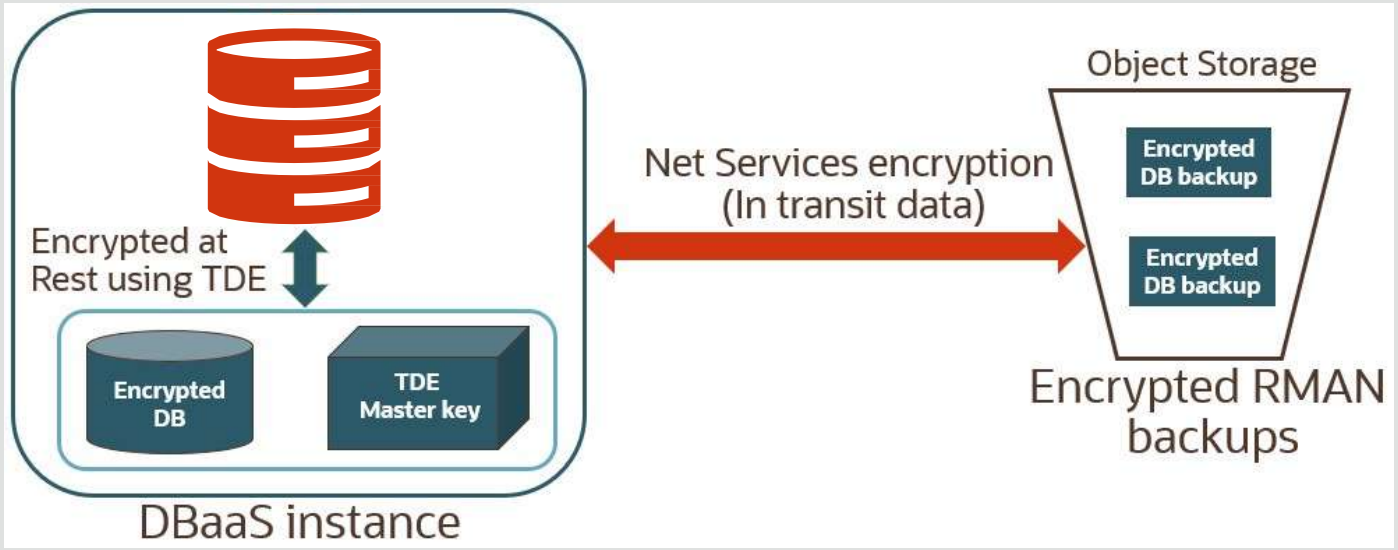
Data Encryption: At Rest and In Transit

Oracle manager OR Customer managed keys (KMS)



Database Encryption: At Rest and In Transit

- Oracle TDE encryption for DB files and Backups at Rest. Key Store/Wallet for managing master key
- For improved security, you can configure backup encryption for RMAN backup sets
- Native Oracle Net Services encryption and integrity capabilities for encrypting data in transit
  - Advanced Encryption Standard (AES), DES, 3DES, and RC4 symmetric cryptosystems for protecting the confidentiality of Oracle Net Services traffic



ORACLE Academy

Key Management

Oracle Key Management provides you with

- Highly available, durable, and secure key storage. Encrypt your data using keys that you control
- Centralized key management capabilities (Create/Delete, Disable/Enable, rotate)
- IAM Policies for Users/Groups and OCI resources
- Key Life Cycle management
- FIPS 140-2 Security Level 3 security certification

ORACLE Academy

References

References

Oracle Cloud Academy Foundations I Section 27

Cloud Generation 2: Larry Ellison Keynote at Oracle OpenWorld 2018: https://www.youtube.com/watch?v=b5qZVk0F_yg

Cloud Engineering

Monitoring

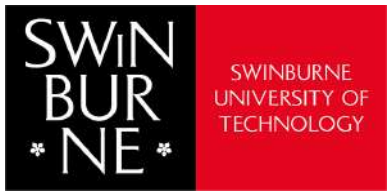
SWINBURNE UNIVERSITY OF TECHNOLOGY

Monitoring

This Presentation:

- OCI Monitoring Service
- Metrics, Alarms, Monitoring Query Language

OCI Monitoring Service



OCI Monitoring Service

Metrics & Alarms

Extensive list of supported services: https://docs.oracle.com/en-us/iaas/Content/Monitoring/Concepts/monitoringoverview.htm#SupportedServices

Available via OCI Console, API, SDK and Terraform

OCI Monitoring Service

Technical e.g. CPU utilisation

Not monitoring costs

Metrics

Metrics

Predefined Metrics

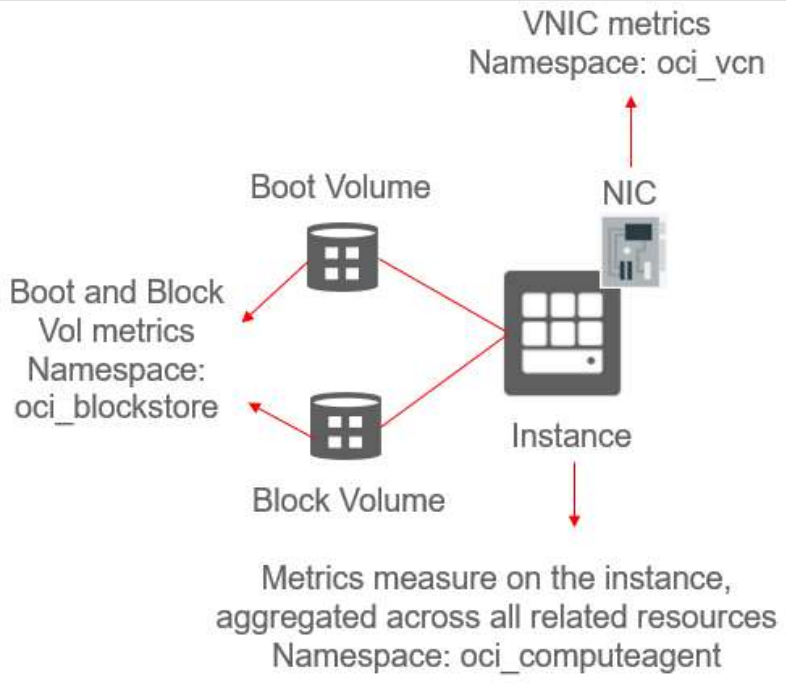
Monitoring Query Language

Custom Metrics

Metrics

- Metric: a measurement related to health, capacity, or performance of a given resource. E.g. CpuUtilization metric measures usage of a compute instance
- Metric → Namespace + Dimension + Metadata
  - Namespace: an indicator of the resource, service, or application that emits the metric. E.g. the CpuUtilization metric lists the metric namespace oci_computeagent as its source
  - Dimension: a qualifier to filter or group metric data. E.g. dimension name-value pair for filtering by AD: availabilityDomain = "VeBZ:PHX-AD-1"
  - Metadata: A reference provided in a metric definition. E.g. unit (bytes), for oci_computeagent metricDiskBytesRead (provides additional information for a metric)
- Metric Stream: An individual set of aggregated data for a metric. A stream can be either specific to a single resource or aggregated across all resources in the compartment

Compute Metrics

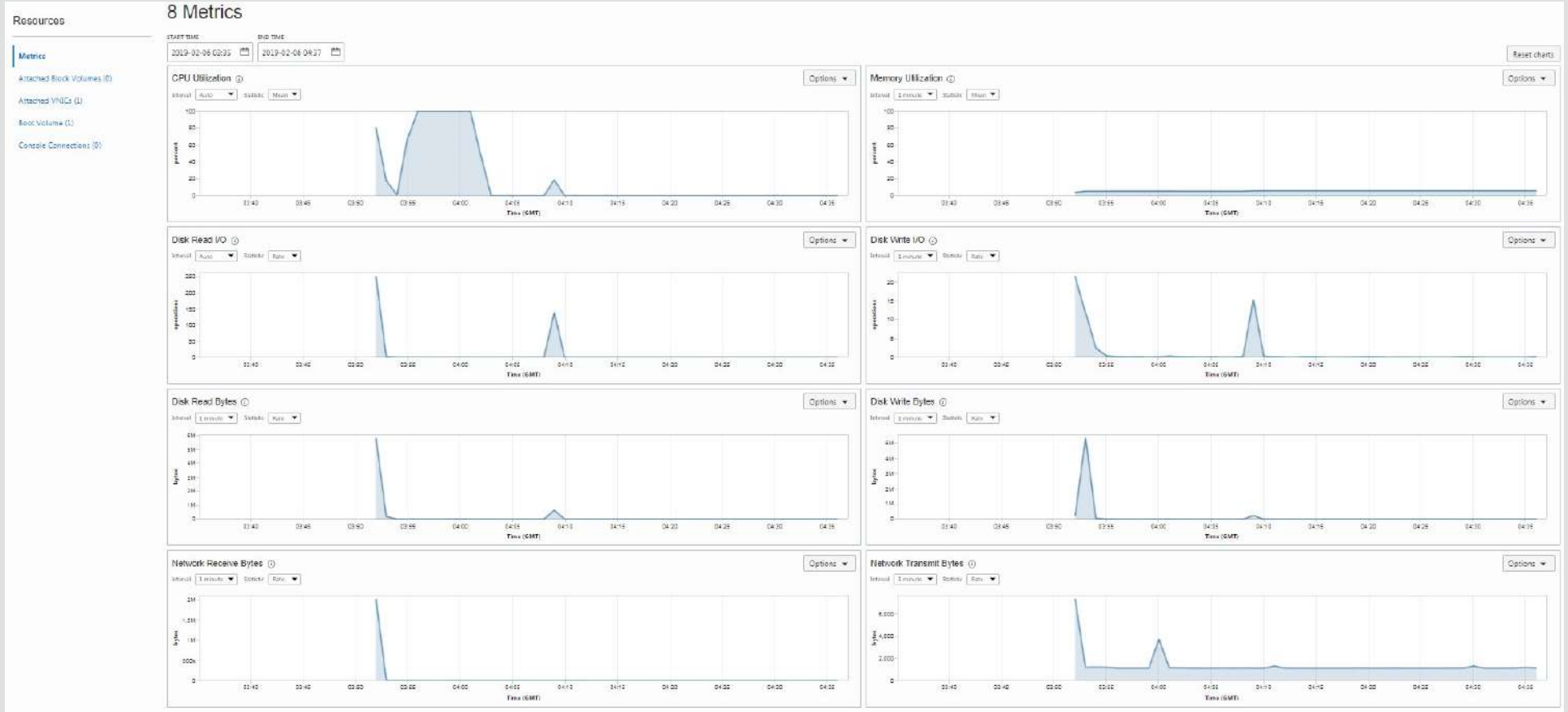


Metric Namespace*	Resource OCID	Where measured
oci_computeagent	Instance OCID	On the instance. Metrics in this namespace are aggregated across all the related resources on the instance. E.g., DiskBytesRead is aggregated across all the instance's attached storage volumes, and NetworkBytesIn is aggregated across all the instance's attached VNICs
oci_blockstore	Boot/Block OCID	By the Block Volume service. The metrics are for an individual boot/block volume
oci_vcn	VNIC OCID	By the Networking service. The metrics are for an individual VNIC

Other namespaces include oci_lbaas, oci_objectstorage, oci_notification

ORACLE Academy

Metrics



ORACLE Academy

Metric Queries

- Monitoring Query Language (MQL) expression can be used to evaluate returning aggregated data. The query must specify a metric, statistic, and interval
- Syntax: metric[interval]{dimensionname=dimensionvalue}.groupingfunction.statistic
  - Interval: frequency at which data points are aggregated. E.g. 5 min
  - Statistic: available functions include count, max, mean, rate, min, sum, and percentile
- Examples
  - Max CPU utilization at 1 min intervals, CpuUtilization[1m].max()
  - Maximum CPU Utilization at a one-minute interval, filtered to a single resource, CpuUtilization[1m]{resourceId="ocid1.instance.oc1.phx.exampleuniqueID"}.max()
  - All read IOPS at a one-minute interval, filtered to a compartment, aggregated for the maximum, IopsRead[1m]{compartmentId="ocid1.compartment.oc1.phx..exampleuniqueID"}.grouping().max()

Alarms

Alarms

Metric meets threshold

Trigger alarm

Send Notification

Alarms

- The Alarms feature of the Monitoring service publishes alarm messages to configured destinations managed by the OCI Notification service
- Monitoring Query Language (MQL) expression can be used to evaluate for the alarm. An alarm query must specify a metric, statistic, interval, and a trigger rule (threshold or absence)
- Alarm states
  - Firing
  - Reset - The alarm is not detecting the metric firing; the metric is no longer being emitted
  - Suspended

Use Case

- Service Metrics: same metrics as the resource specific ones, but for all the resources in a compartment. Allows for filtering with Dimensions
- Metric Explorer: Dive into detail on a specific metric and show multiple resource metrics together. Also includes a powerful Metric Query Language (MQL) interface for complex queries
- Alarm Definition: create an alarm based on a metric and create a notification via OCI Notifications Service (email and PagerDuty)
- Alarms Status: review the status of the configured firing alarms
- Both Monitoring pages plus the Resource specific charts allow the customer to create Alarms directly, prepopulating the query

Design Considerations

Compute instance – public IP / service gateway

No Fast Connect / VPN support

Pricing

- OCI Monitoring Ingestion:
  - Price $0.0025 per 1 million data points ingested, first 500 Million data points ingested per month free
- OCI Monitoring Retrieval:
  - Price $0.0015 per 1 million data points analyzed, first 1 Billion data points analyzed per month free

References

References

Oracle Cloud Academy Foundations I Section 18

Cloud Engineering

Billing and Cost Management

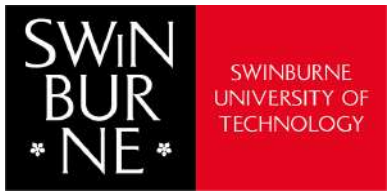
SWINBURNE UNIVERSITY OF TECHNOLOGY

Billing and Cost Management

This Presentation:

- Budgeting is for Students
- Cost Analysis, Budgets
- Service Limits & Quotas

Budgeting is for Students not just for the Real World



Budgets

One of the first things to do

Try to Avoid Bill Shock

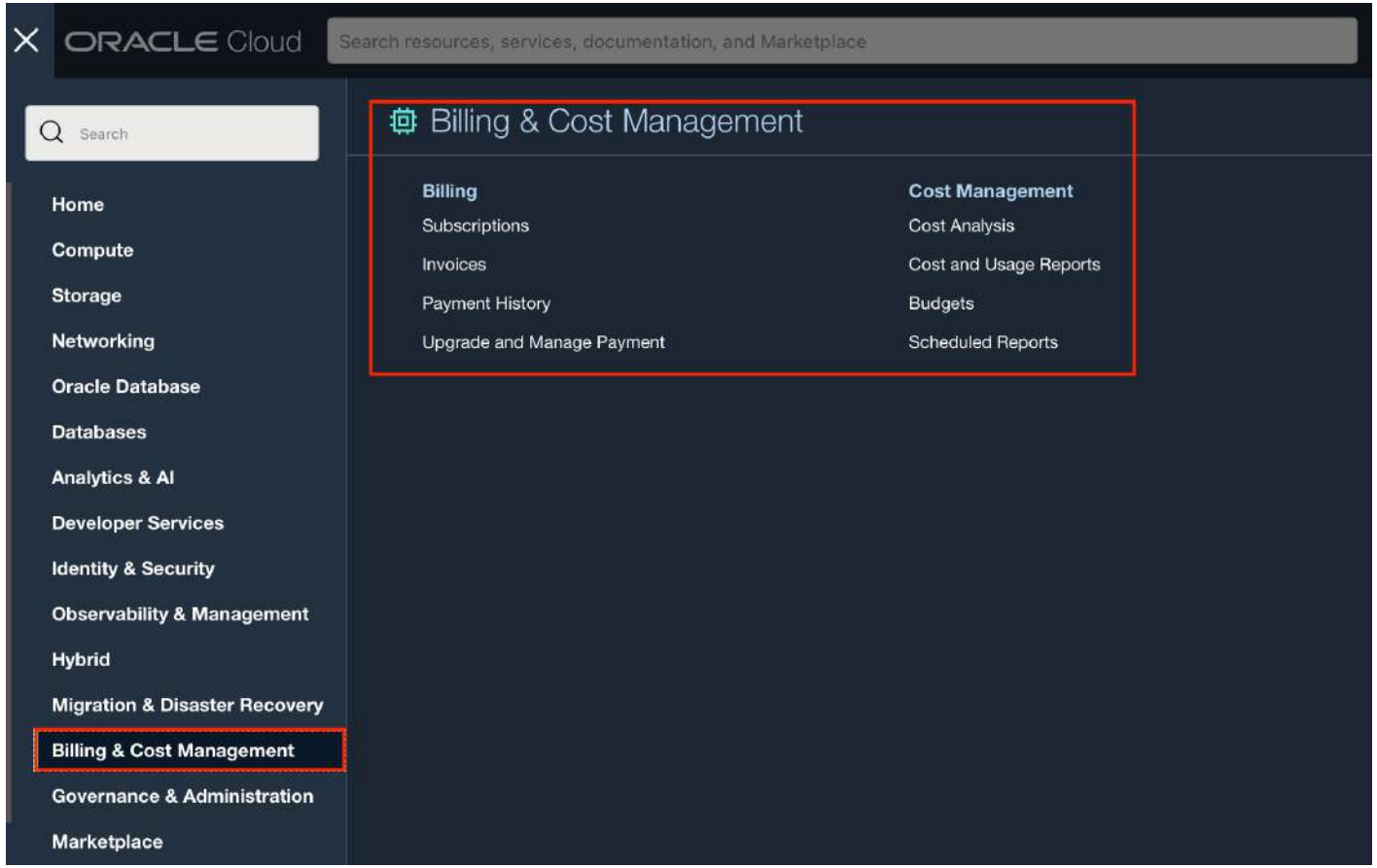
Free Tier and Always Free

Try to use where possible for learning

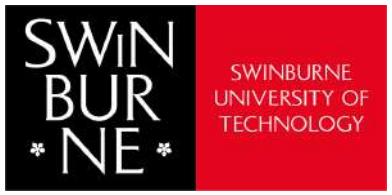
If signed up to OCI using invite to student email:

$400 of free credits for 365 days

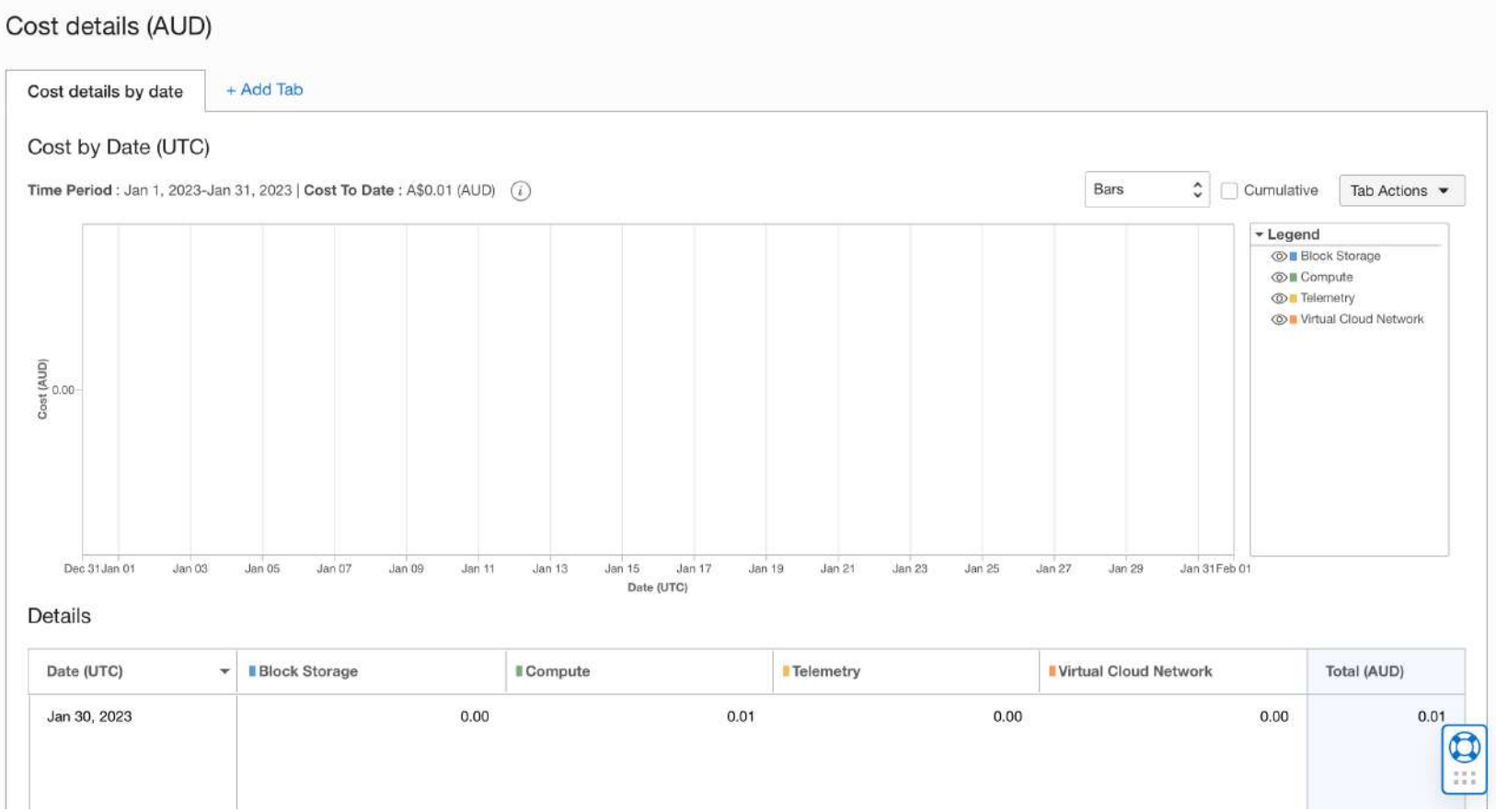
Billing and Cost Management



Cost Analysis and Budgets

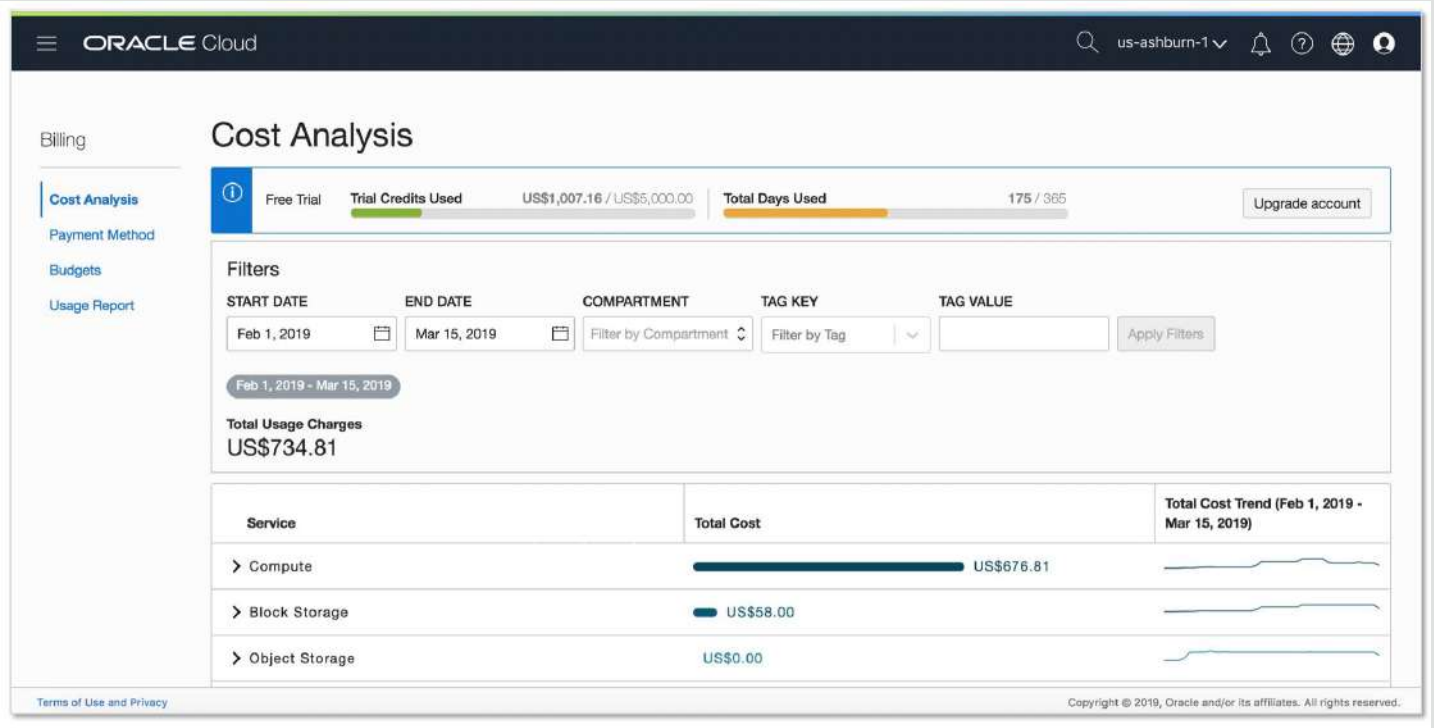


Cost Analysis



OCI Cost Analysis

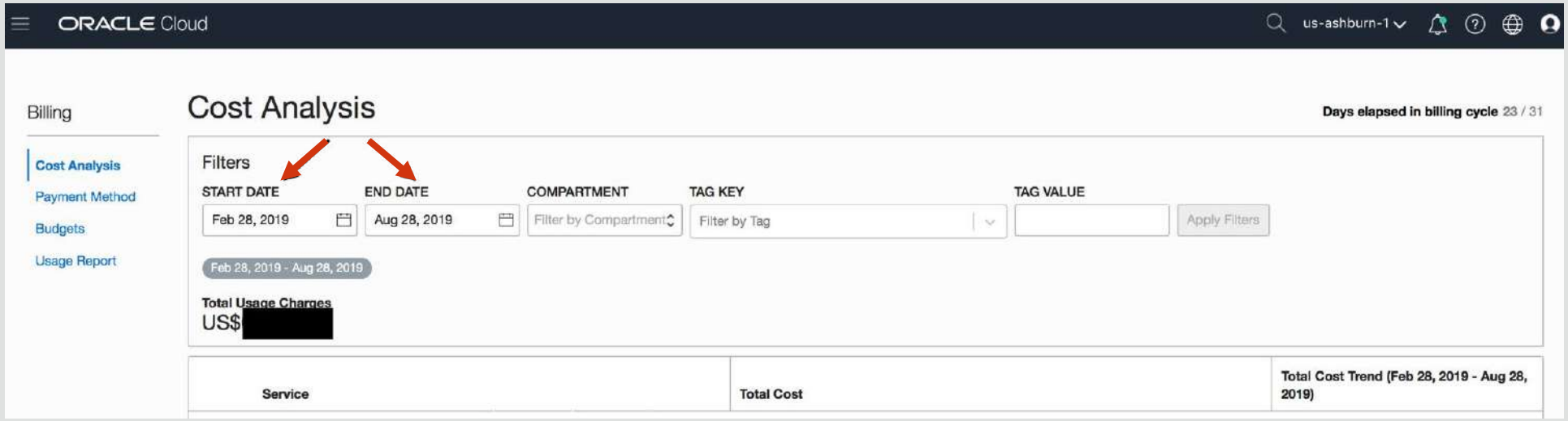
- Visualization tools Help understand spending patterns at a glance
- Filter costs by Date, Tags and Compartments
- Trend lines show how spending patterns are changing
- To use Cost Analysis you must be a member of the Administrators group



ORACLE Academy

Cost Analysis: Filter Costs by Date

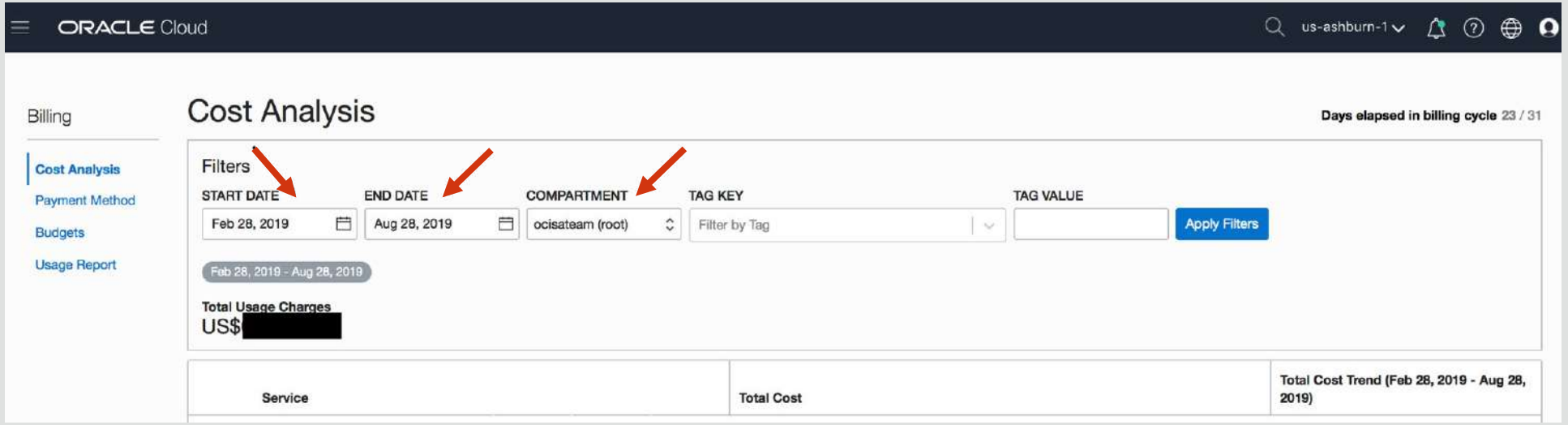
1. Open the navigation menu. Under **Governance and Administration**, go to **Billing** and click **Cost Analysis**.
2. In **Start Date**, select a date.
3. In **End Date**, select a date (within six months of the start date).
4. Click **Apply Filters**.



ORACLE Academy

Cost Analysis: Filter Costs by Tags

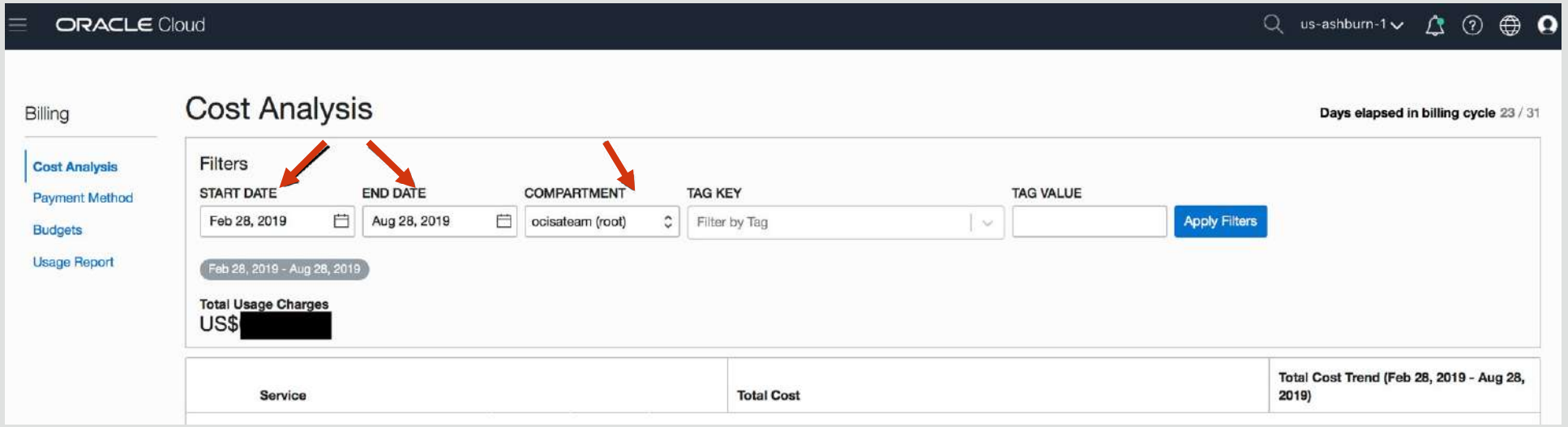
1. Open the navigation menu. Under **Governance and Administration**, go to **Billing** and click **Cost Analysis**.
2. From **Tag Key**, select a tag.
3. Click **Apply Filters**.



ORACLE Academy

Cost Analysis: Filter Costs by Compartments

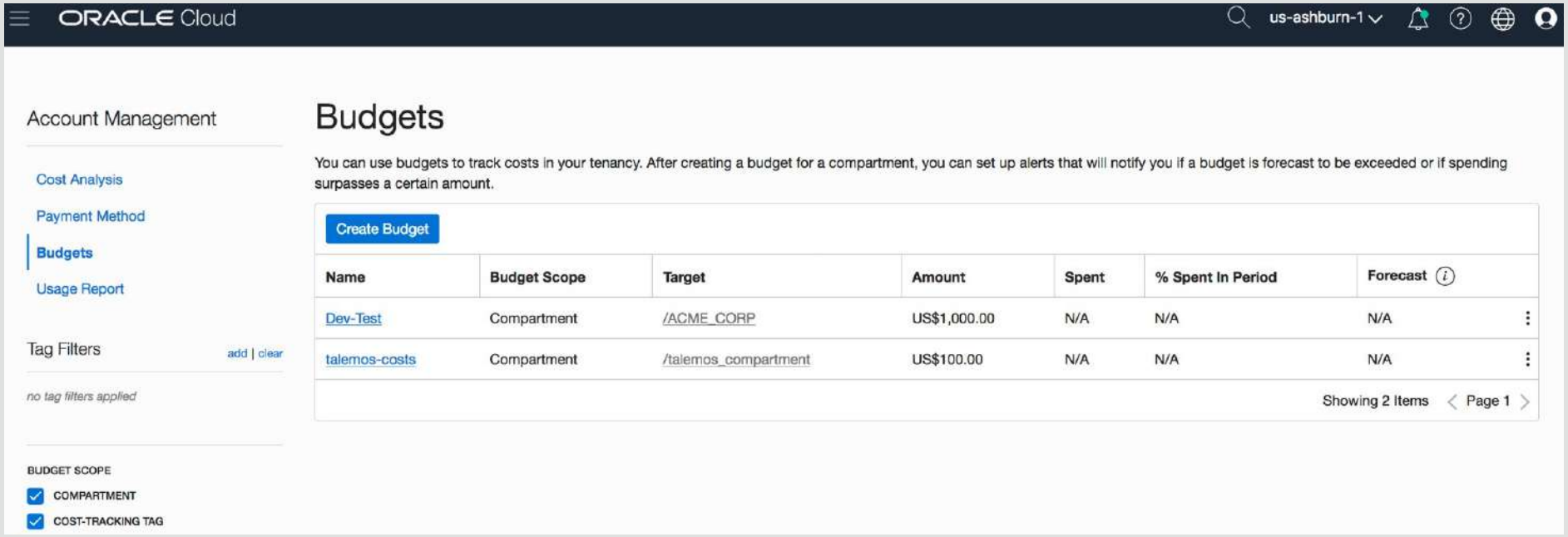
1. Open the navigation menu. Under **Governance and Administration**, go to **Billing** and click **Cost Analysis**.
2. From **Compartment**, select a compartment.
3. Click **Apply Filters**.



ORACLE Academy

OCI Budgets

- Track actual and forecasted spending for the entire tenancy or per compartment
- Set alerts on your budgets at predefined thresholds to get notified
- View all of your budgets and spending from one dashboard



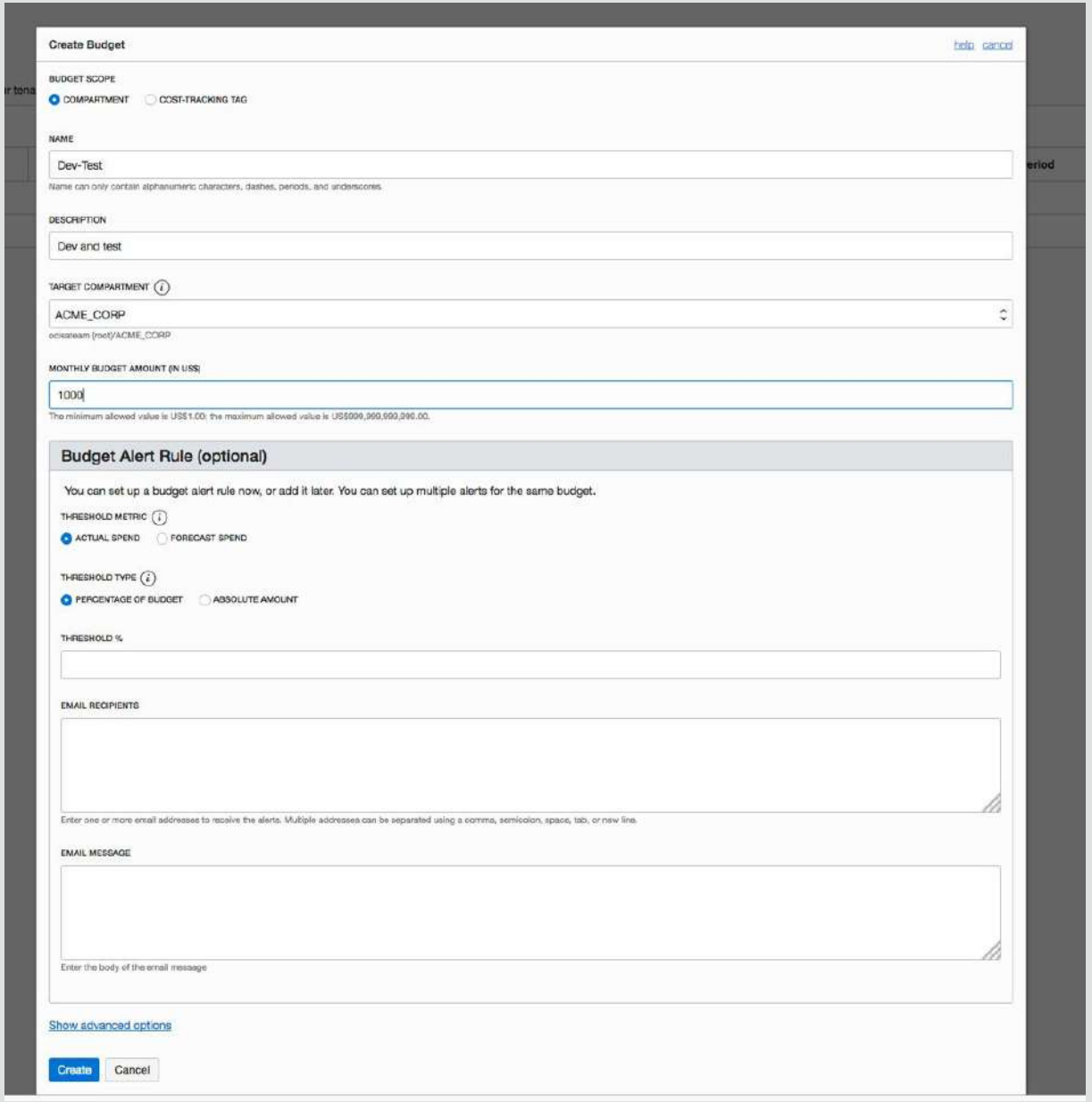
ORACLE Academy

Accessing OCI Budgets

- To use budgets, you must be in a group that can use "usage-budgets" in the tenancy
- All budgets are created in the root compartment, regardless of the compartment they are targeting

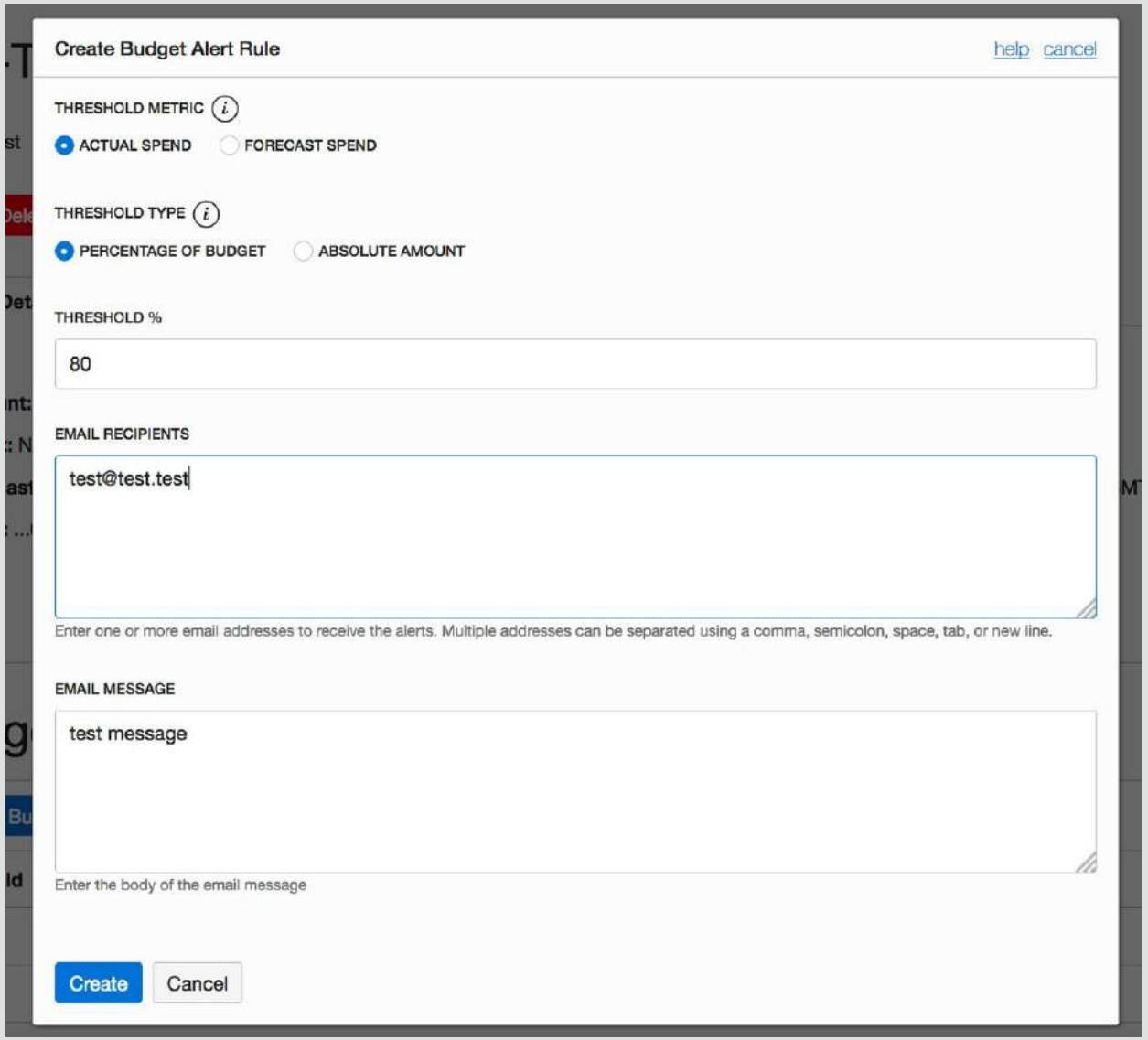
IAM Policy	Description
Allow group accountants to inspect usage-budgets in tenancy	Accountants can inspect budgets including spend.
Allow group accountants to read usage-budgets in tenancy	Accountants can read budgets including spend (same as list).
Allow group accountants to use usage-budgets in tenancy	Accountants can create and edit budgets and alerts rules.
Allow group accountants to manage usage-budgets in tenancy	Accountants can create, edit, and delete budgets and alerts rules.

Create Budgets



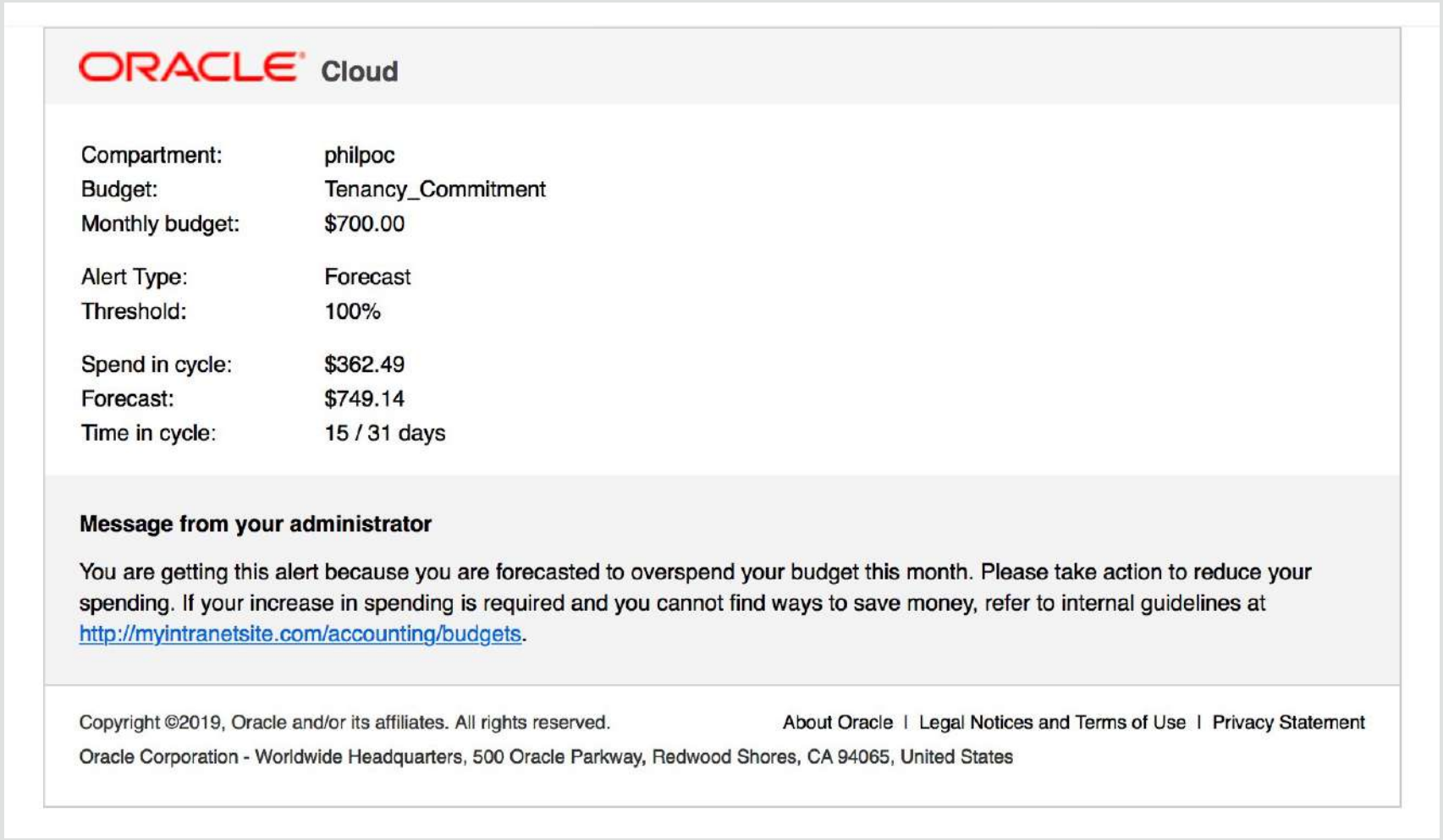
ORACLE Academy

Budgets Alerts



ORACLE Academy

Budget Alert Emails



ORACLE Cloud

Compartment:	philpoc
Budget:	Tenancy_Commitment
Monthly budget:	$700.00
Alert Type:	Forecast
Threshold:	100%
Spend in cycle:	$362.49
Forecast:	$749.14
Time in cycle:	15 / 31 days

Message from your administrator

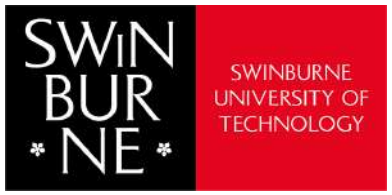
You are getting this alert because you are forecasted to overspend your budget this month. Please take action to reduce your spending. If your increase in spending is required and you cannot find ways to save money, refer to internal guidelines at http://myintranetsite.com/accounting/budgets.

About Oracle | Legal Notices and Terms of Use | Privacy Statement

Oracle Corporation - Worldwide Headquarters, 500 Oracle Parkway, Redwood Shores, CA 94065, United States

ORACLE Academy

Service Limits and Quotas



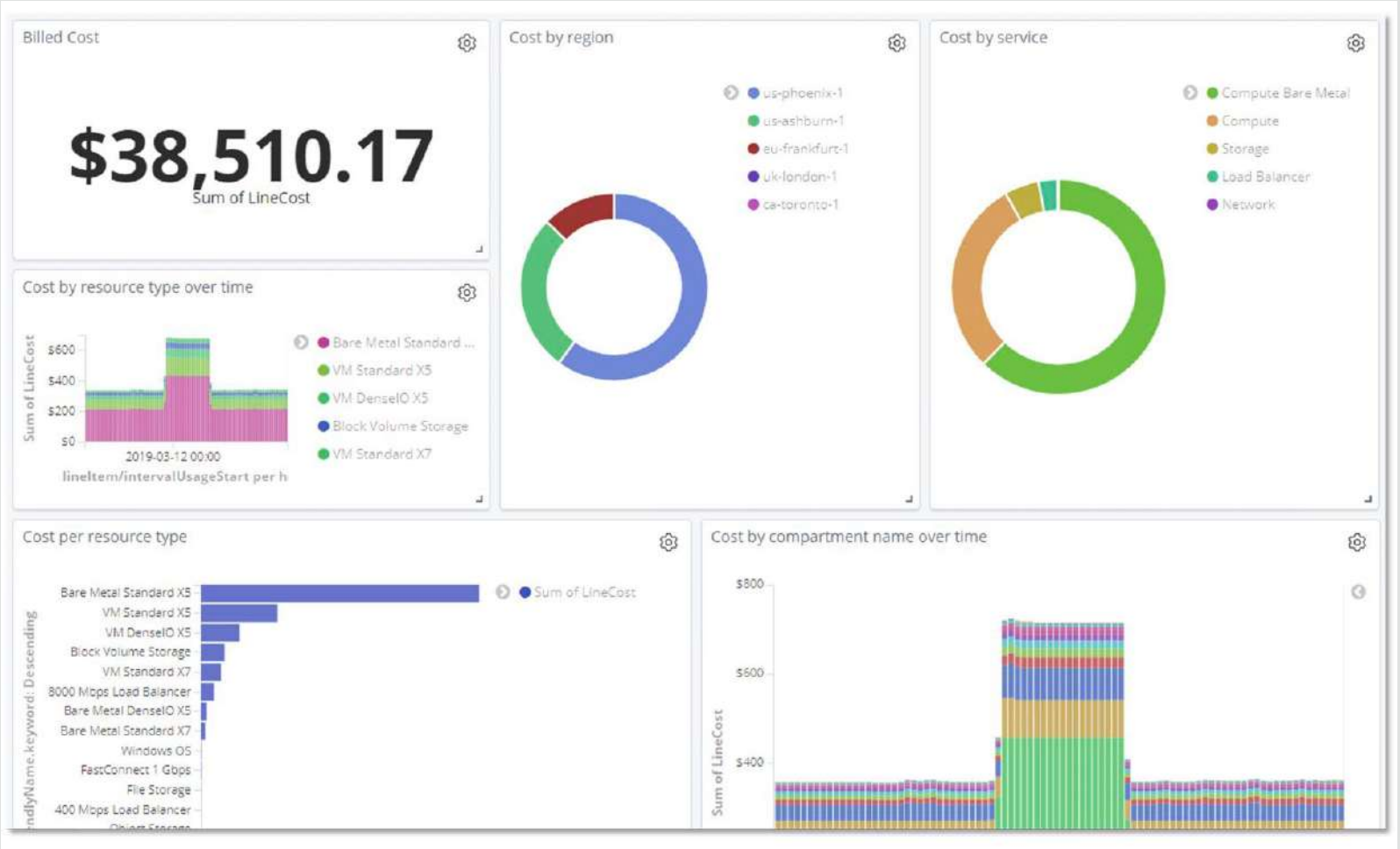
Usage Reports

- Detailed information about your OCI consumption
- CSV file with one record per resource per hour with metadata and tags
- Automatically generated daily, and stored in an Oracle-owned object storage bucket
- Contain 24 hours of usage data
- Retained for one year
- Can be used in conjunction with your rate card for:
  - Invoice reconciliation
  - Custom reporting
  - Cross-charging
  - Cost optimization
  - Resource inventory

Accessing Usage Reports

- Reports are generated in another tenancy and stored in an Oracle-owned object storage bucket
- Set up a cross-tenancy IAM policy to access your usage reports
  - *define tenancy usage-report as ocid1.tenancy.oc1..abc..*
  - *endorse group MyGroupName to read objects in tenancy usage-report*
- Download using console
  1. Open the navigation menu. Under Governance and Administration, go to Billing and select Usage Report.
  2. Click the report you want to download from the list, and follow your browser's instructions for downloading.
- Download using API
  - Use the Object Storage APIs
  - stored in the tenancy's home region
  - Object storage namespace used for the reports is bling; the bucket name is the tenancy OCID

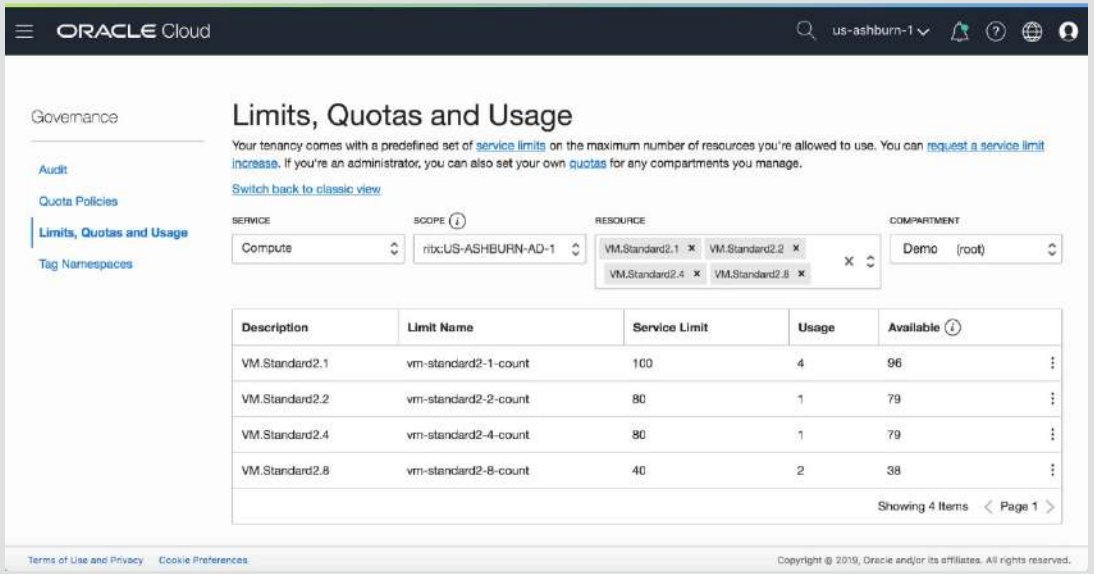
Sample Dashboard from a Usage Report



ORACLE Academy

Service Limits and Usage

- When you sign up for Oracle Cloud Infrastructure, a set of service limits are configured for your tenancy.
- The service limit is the quota or allowance set on a resource.
- You can view your tenancy's limits, quotas, and usage in the Console.
  - You can check Limits and Quotas before a deployment
- You can submit a request to increase your service limits from within the Console.



ORACLE Academy

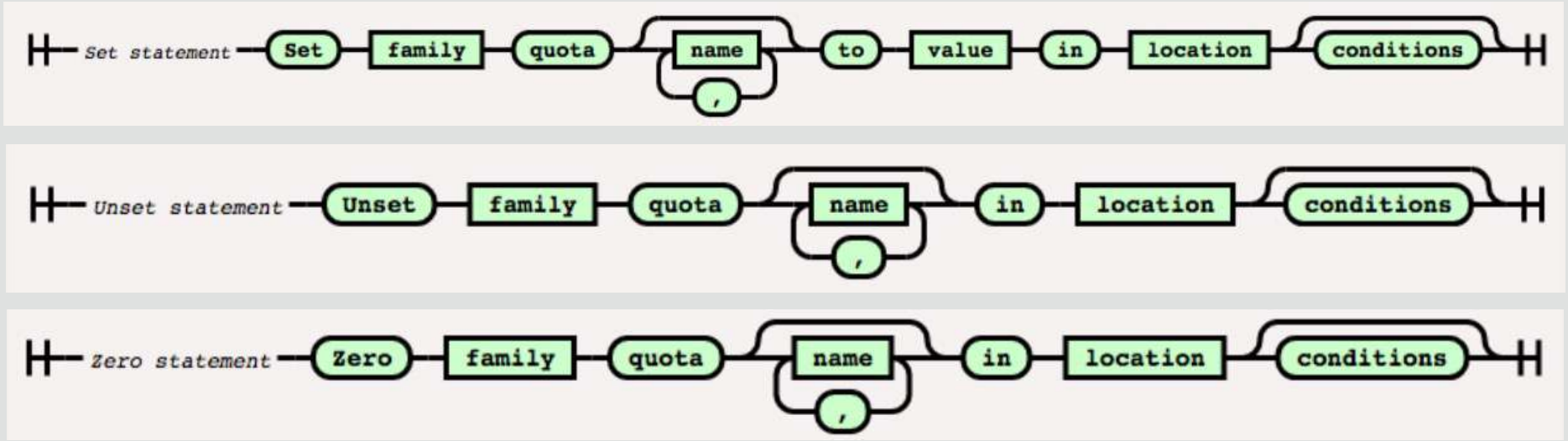
Compartment Quotas

- Quotas give you better control over how resources are consumed by letting you allocate resources to projects or departments
  - Allocate high-value and expensive resources only to specific compartments
  - Restrict a compartment's usage to a small set of resources, restrict resource counts or disable services as necessary
- Similar to Service Limits; but service limits are set by Oracle, and compartment quotas are set by administrators
- Set using policy statements written in a simple declarative language that is similar to the IAM policy language

ORACLE Academy

Quota Policies

- **set** - sets the maximum number of a cloud resource that can be used for a compartment
- **unset** - resets quotas back to the default service limits
- **zero** - removes access to a cloud resource for a compartment



Quota Policies Examples

- This example policy statement only allows one VM.Standard2.1 Compute instance in a single compartment in a single region:
  - zero compute quotas in tenancy
  - set compute quota vm-standard2-1-count to 10 in compartment IT where request.region = us-phoenix-1
- You can clear quotas by using an unset statement, which removes the quota for a resource - any limits on this resource will now be enforced by the service limits:
  - zero compute quotas in tenancy
  - unset compute quota vm-dense-io1-16-count in tenancy

Cost Management Best Practices

- Create a budget that matches your commitment amount and an alert at 100 percent of the forecast.
  - Gives you an early warning if your spending increases and you're at risk of getting an overage.
- Use compartments for cost management along with access-control. Many customers set up one compartment per department for cost management and cross-charging.
- Use cost-tracking tags (like cost-center) to allocate cost in more granular ways.
- Enable monitoring on all resources. You can merge monitoring data with cost data to gain powerful insights on how to improve resource utilization.
- Use the usage report to analyze costs and drive custom solutions.

References

References

Oracle Cloud Academy Foundations I Section 25