UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Presentation 2 – AWS M2 and M4

- AWS M2 - Cloud Economics and Billing
- AWS M4 - AWS Cloud Security

aws academy

Vytvorené v rámci projektu **KEGA 026TUKE-4/2021**

Outline

- **AWS M2 - Cloud Economics and Billing**
  - Fundamentals of pricing
  - Total Cost of Ownership
  - AWS Organizations
  - AWS Billing and Cost Management
  - Technical Support

- **AWS M4 - AWS Cloud Security**

Fundamentals of pricing

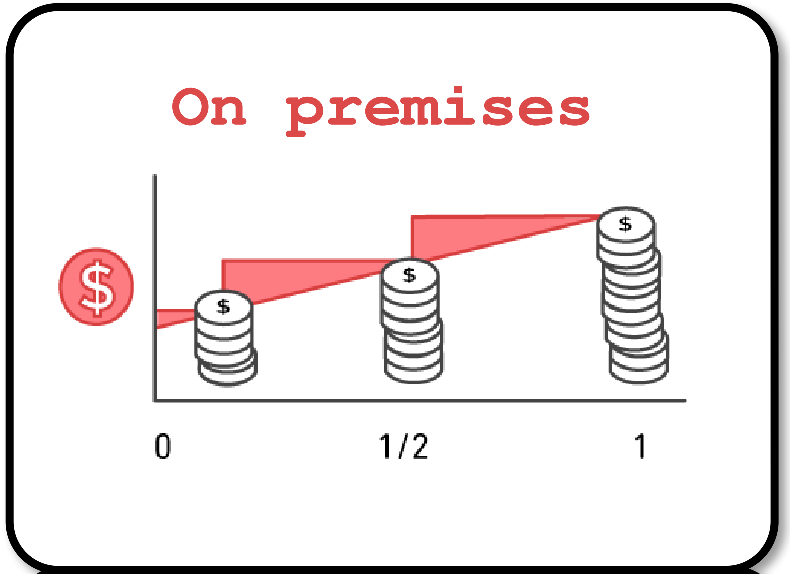
Three fundamental drivers of cost with AWS

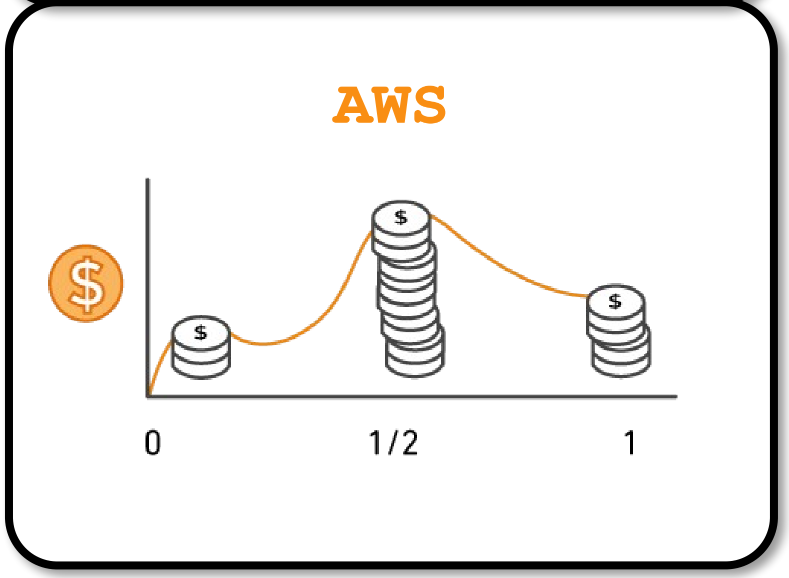
AWS pricing model

- There are three fundamental drivers of cost with AWS:
  - Compute
    - Charged per hour/second*
    - Varies by instance type
  - Storage
    - Charged typically per GB
  - Data transfer
    - Outbound is aggregated and charged
    - Inbound has no charge (with some exceptions)
    - Charged typically per GB

- How do you pay for AWS?
  - Pay for what you use
  - Pay less when you reserve
  - Pay less when you use more
  - Pay even less as AWS grows

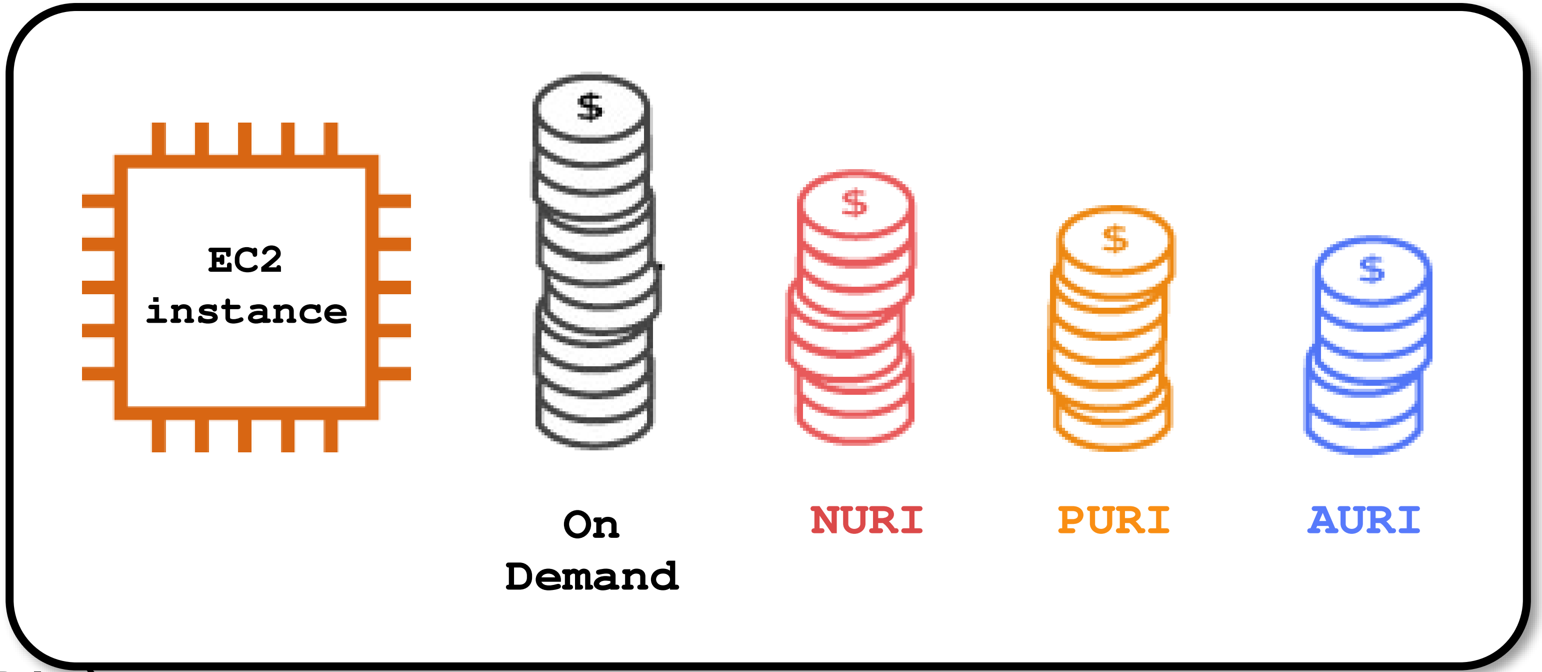
Pay for what you use





- Pay for what you use
  - Start or stop using a product at any time.
  - No long-term contracts are required.
  - pay only for the services that you consume with no large upfront expenses

Pay less when you reserve

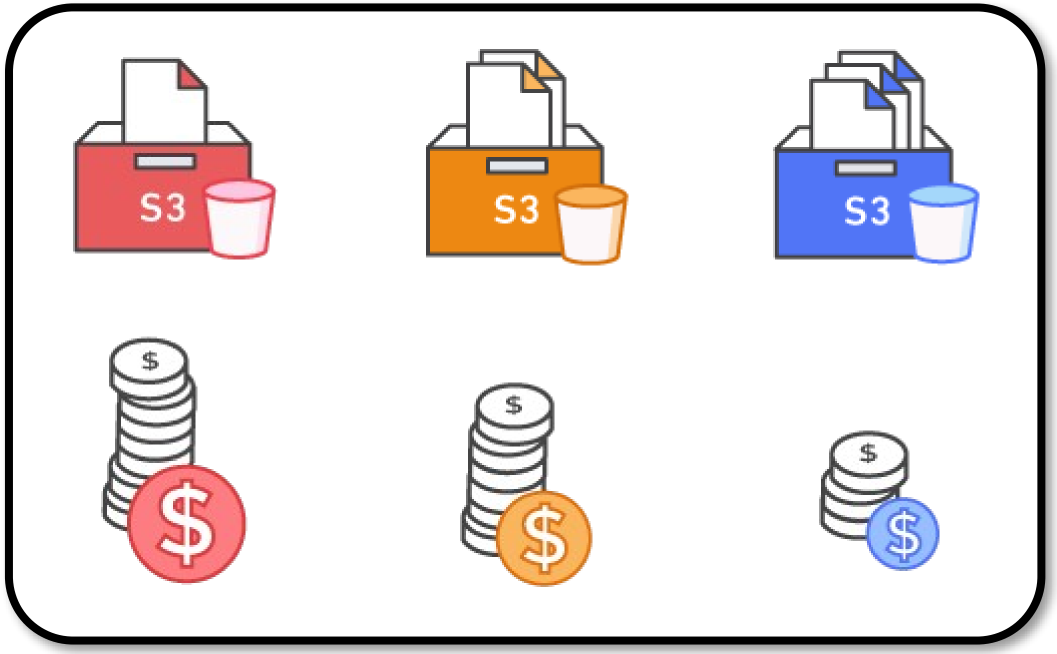


- Some services can be reserverd
  => and cheaper
- Reserved Instances (RIs):
  - Allows to save up to 75 percent compare to on-demand instances
  - Provides greater discount when you make a larger upfront payment
- RI options:
  - All Upfront Reserved Instance (AURI) ✉ largest discount
  - Partial Upfront Reserved Instance (PURI) ✉ lower discounts
  - No Upfront Payments Reserved Instance (NURI) ✉ smaller discount

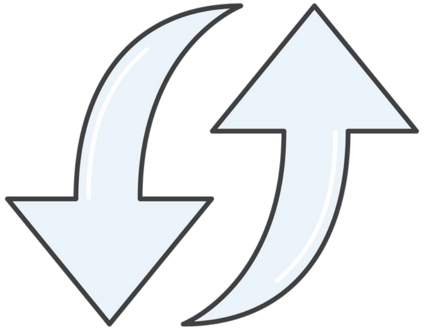
Pay less by using more

Realize volume-based discounts:

- **Savings** as usage increases.
- **Tiered pricing**
  - for services like Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS), or Amazon Elastic File System (Amazon EFS) ✉ the more you use, the less you pay per GB.
- Multiple storage services deliver **lower** storage costs based on needs.



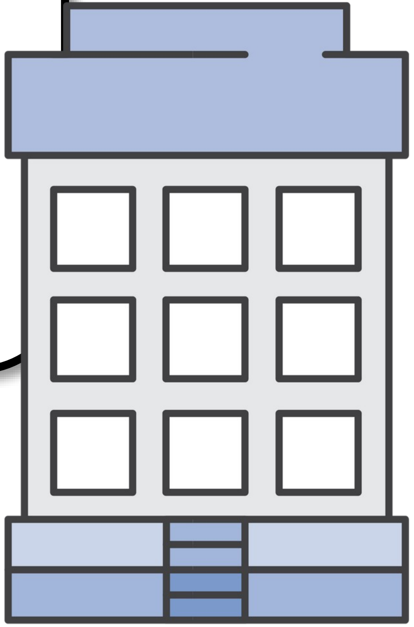
Pay even less as AWS grows



- As AWS grows:
    - AWS focuses on lowering cost of doing business.
    - This practice results in AWS passing savings from economies of scale to you.
    - Since 2006, AWS has lowered pricing 75 times (as of September 2019).
    - Future higher-performing resources replace current resources for no extra charge.

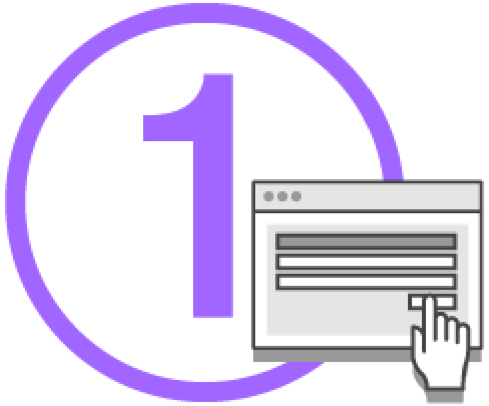
Custom pricing

- For high-volume projects with unique requirements the Custom pricing model is available
  - Meet varying needs through custom pricing.
  - Available for high-volume projects with unique requirements.



AWS Free Tier

- Enables you to gain free hands-on experience with the AWS platform, products, and services.
    - Amazon Elastic Compute Cloud (Amazon EC2) T2 micro instance, Amazon S3, Amazon Elastic Block Store (Amazon EBS), Elastic Load Balancing, AWS data transfer, and other AWS services
    - Free for 1 year for new customers.



Sign up for an AWS account

Learn with 10-minute tutorials

Start building with AWS

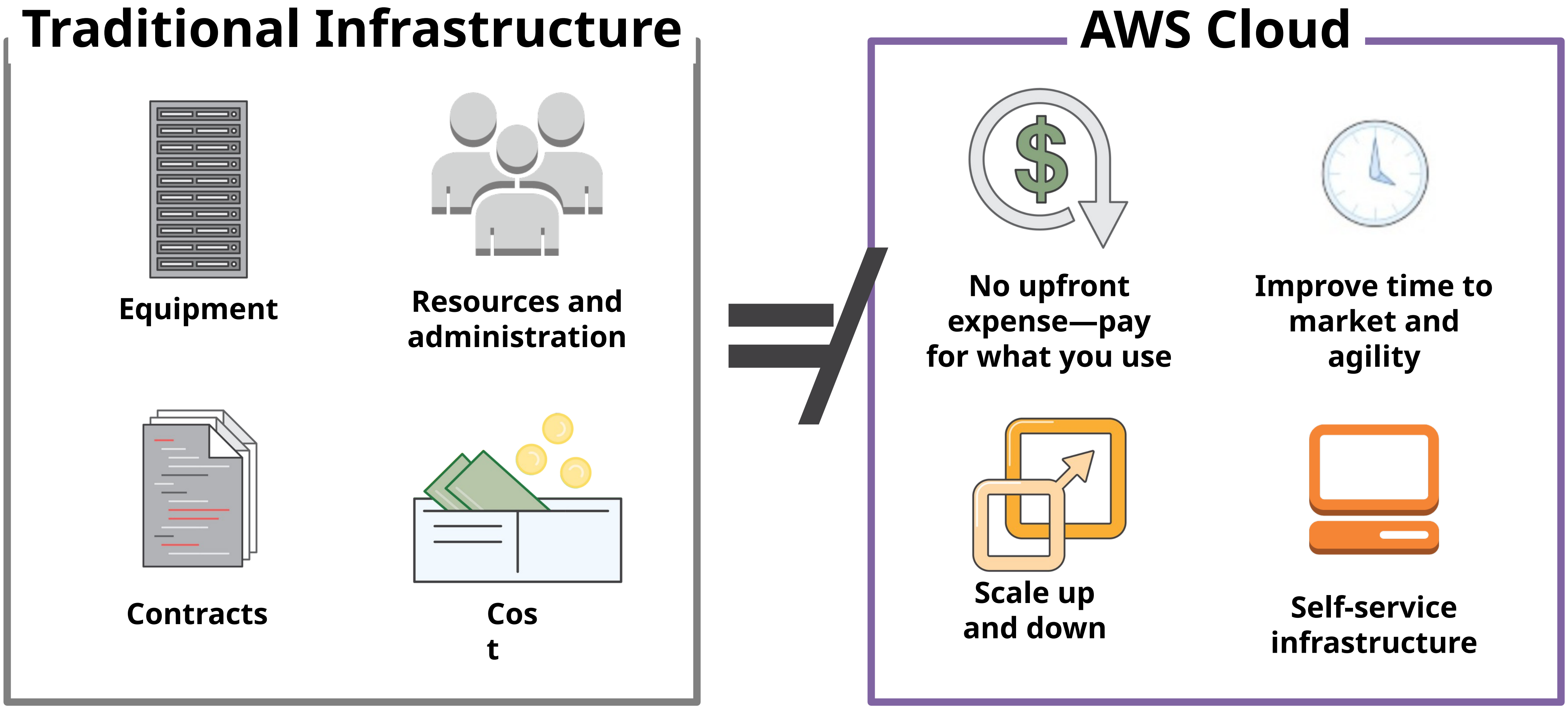
Services with no charge

- Amazon VPC
- Elastic Beanstalk**
- Auto Scaling**
- AWS CloudFormation**
- AWS Identity and Access Management (IAM)

****Note: There might be charges associated with other AWS services that are used with these services.**

Total Cost of Ownership

On-premises versus cloud



Traditional Infrastructure

Equipment

Resources and administration

Contracts

Cos
t

≠

AWS Cloud

No upfront expense—pay for what you use

Improve time to market and agility

Scale up and down

Self-service infrastructure

What is Total Cost of Ownership (TCO)?

- Total Cost of Ownership (TCO)
  - the financial estimate to help identify direct and indirect costs of a system.

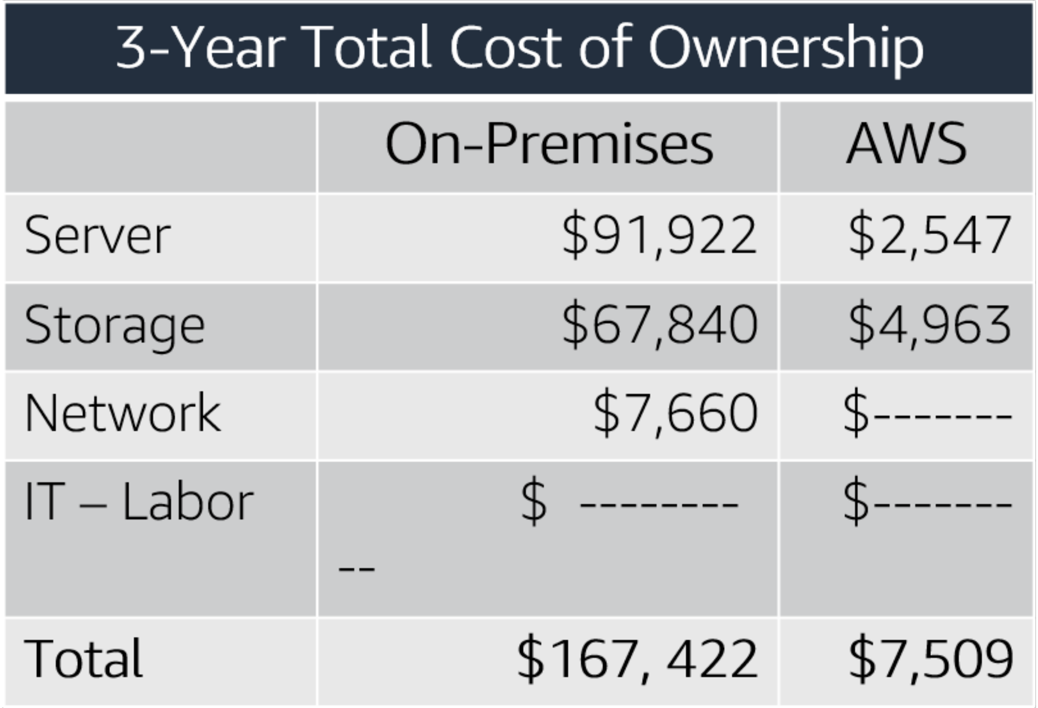
- Why use TCO?
  - To compare the costs of running an entire infrastructure environment or specific workload on-premises versus on AWS
  - To budget and build the business case for moving to the cloud

TCO considerations

1	Server Costs	Hardware: Server, rack chassis power distribution units (PDUs), top-of-rack (TOR) switches (and maintenance)	Software: Operating system (OS), virtualization licenses (and maintenance)	Facilities cost		
				Space	Power	Cooling
2	Storage Costs	Hardware: Storage disks, storage area network (SAN) or Fibre Channel (FC) switches	Storage administration costs	Facilities cost		
				Space	Power	Cooling
3	Network Costs	Network hardware: Local area network (LAN) switches, load balancer bandwidth costs	Network administration costs	Facilities cost		
				Space	Power	Cooling
4	IT Labor Costs	Server administration costs				

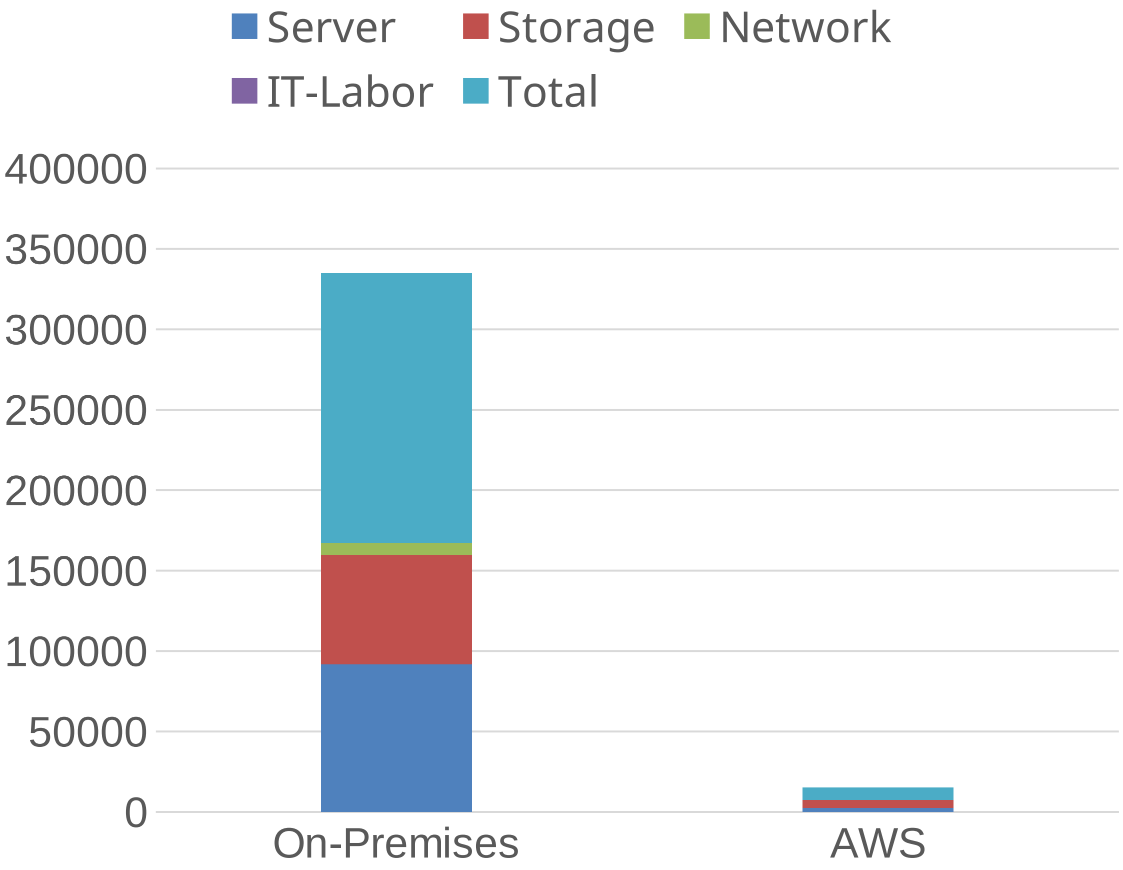
On-premises versus all-in-cloud

Save up to 96 percent a year by moving your infrastructure to AWS.
Your 3-year total savings would be $159,913.



3-Year Total Cost of Ownership		
	On-Premises	AWS
Server	$91,922	$2,547
Storage	$67,840	$4,963
Network	$7,660	$-------
IT – Labor	$ -------- --	$-------
Total	$167, 422	$7,509

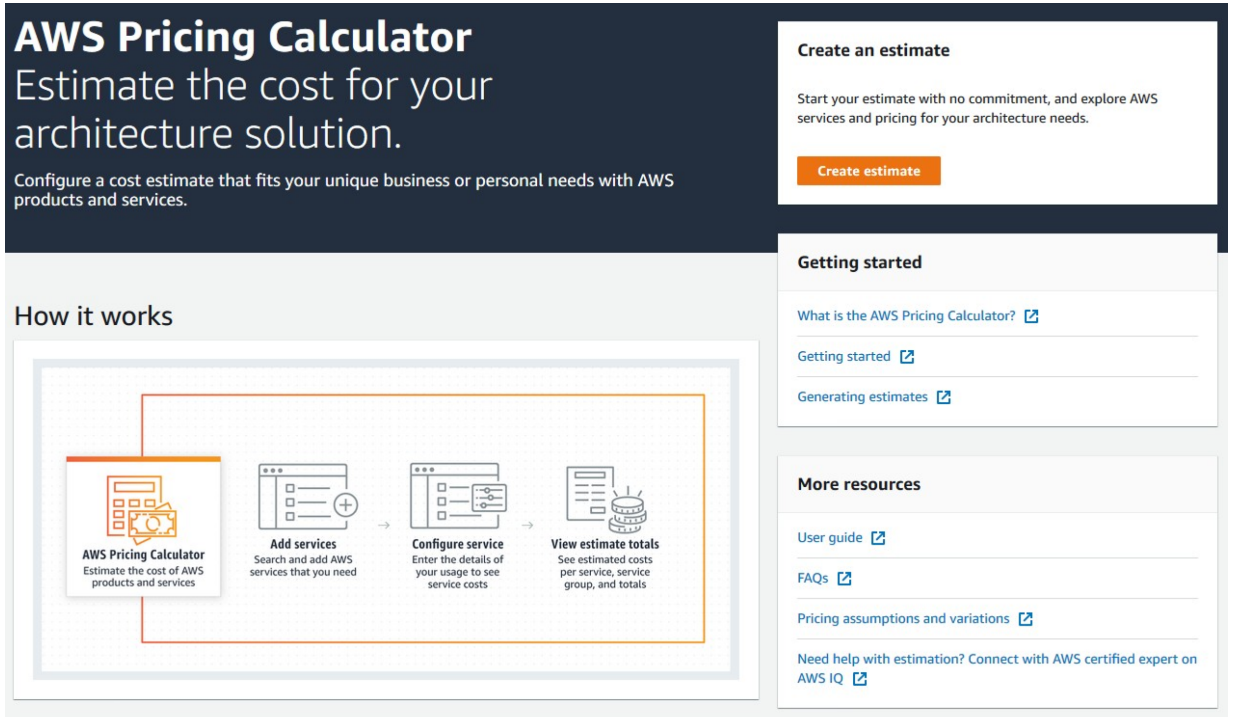
AWS cost includes business-level support and a 3-year PURI EC2 instance



AWS Pricing Calculator

Used to:

- Estimate monthly costs
- Identify opportunities to reduce monthly costs
- Model your solutions before building them
- Explore price points and calculations behind your estimate
- Find the available instance types and contract terms that meet your needs
- Name your estimate and create and name groups of services



AWS Pricing Calculator

Estimate the cost for your architecture solution.

Configure a cost estimate that fits your unique business or personal needs with AWS products and services.

Create an estimate

Start your estimate with no commitment, and explore AWS services and pricing for your architecture needs.

Create estimate

How it works

AWS Pricing Calculator
Estimate the cost of AWS products and services

Add services
Search and add AWS services that you need

→

Configure service
Enter the details of your usage to see service costs

→

View estimate totals
See estimated costs per service, service group, and totals

Getting started

What is the AWS Pricing Calculator?

Getting started

Generating estimates

More resources

User guide

FAQs

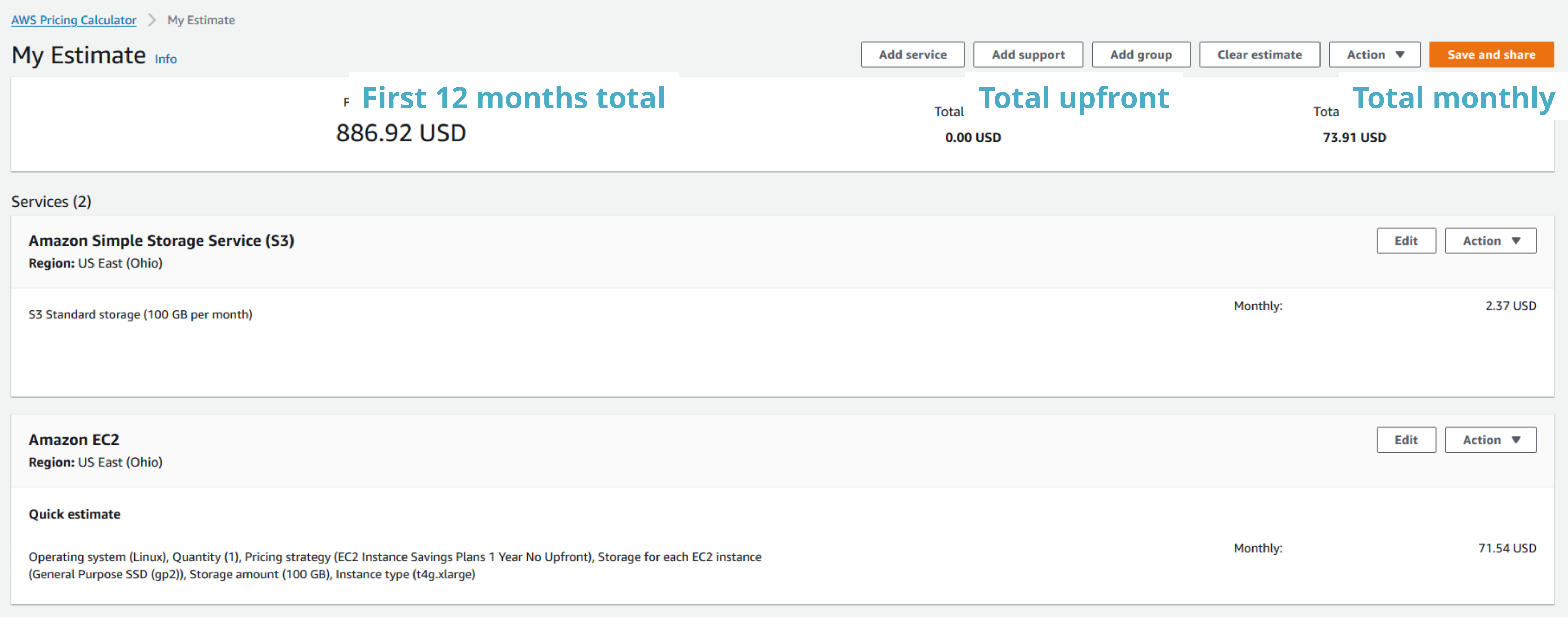
Pricing assumptions and variations

Need help with estimation? Connect with AWS certified expert on AWS IQ

Access the AWS Pricing Calculator

Reading an estimate

our estimate is broken into: first 12 months total, total upfront, and total monthl



My Estimate Info

F First 12 months total
886.92 USD

Total Total upfront
0.00 USD

Tota Total monthly
73.91 USD

Services (2)

Amazon Simple Storage Service (S3)
Region: US East (Ohio)

S3 Standard storage (100 GB per month) Monthly: 2.37 USD

Amazon EC2
Region: US East (Ohio)

Quick estimate

Operating system (Linux), Quantity (1), Pricing strategy (EC2 Instance Savings Plans 1 Year No Upfront), Storage for each EC2 instance (General Purpose SSD (gp2)), Storage amount (100 GB), Instance type (t4g.xlarge) Monthly: 71.54 USD

Additional benefit considerations

Hard benefits

- Reduced spending on compute, storage, networking, security
- Reductions in hardware and software purchases (capex)
- Reductions in operational costs, backup, and disaster recovery
- Reduction in operations personnel

Soft Benefits

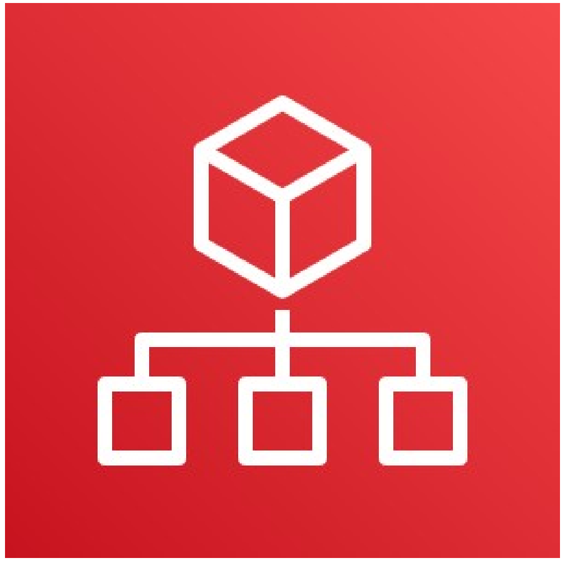
- Reuse of service and applications that enable you to define (and redefine solutions) by using the same cloud service
- Increased developer productivity
- Improved customer satisfaction
- Agile business processes that can quickly respond to new and emerging opportunities
- Increase in global reach

Ak chcete pridať obrázok, kliknite na ikonu

AWS Organizations

Introduction to AWS Organizations

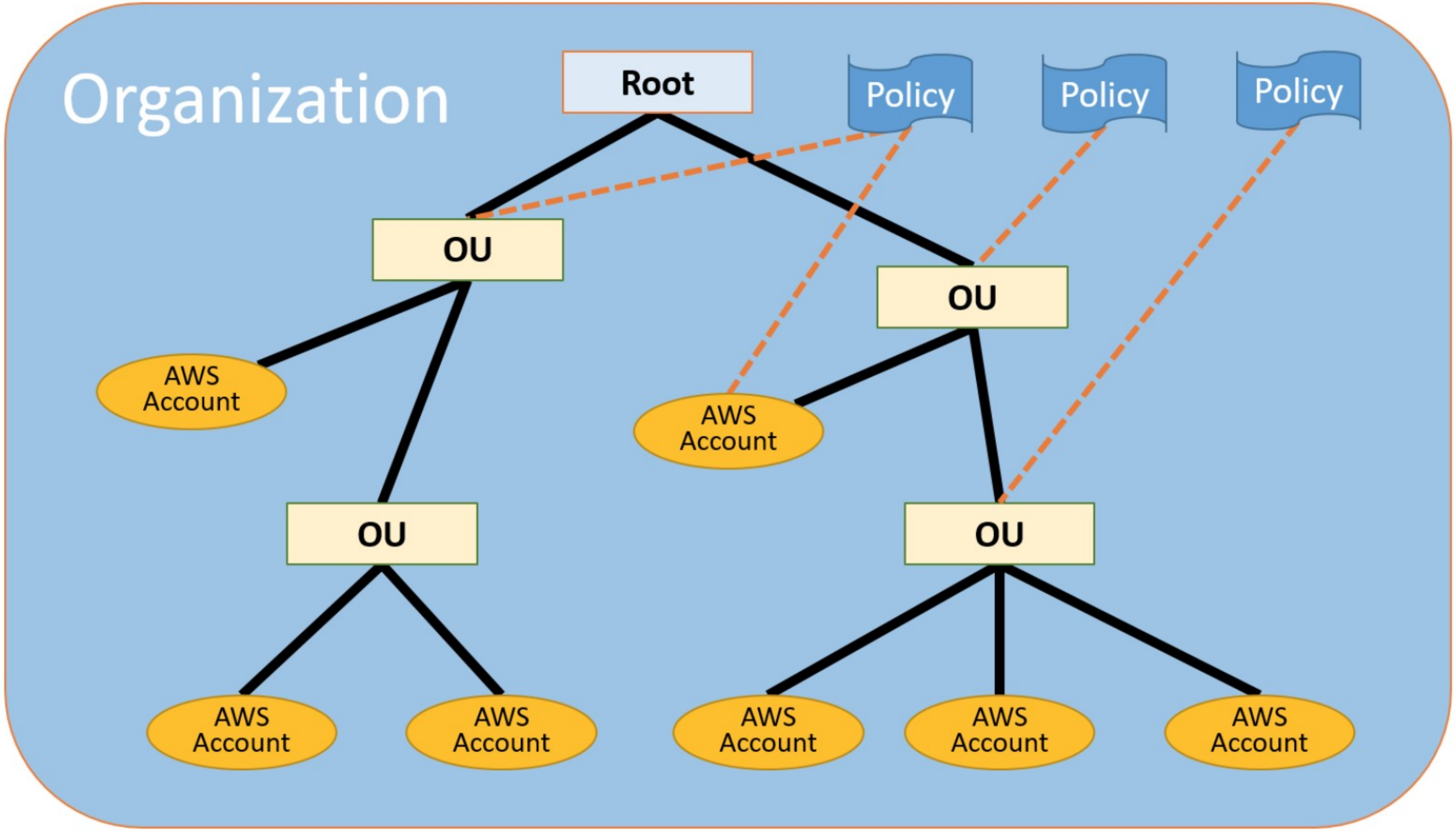
- AWS Organizations
  - free account management service
  - enables consolidate multiple AWS accounts into an organization
- The main benefits of AWS Organizations are:
  - Centrally managed access policies across multiple AWS accounts.
  - Controlled access to AWS services.
  - Automated AWS account creation and management.
  - Consolidated billing across multiple AWS accounts.



AWS Organizations

AWS Organizations terminology

- ROOT
- OU
- AWS Account



*Organizational Units (OUs)

Key features and benefits

AWS Organizations

Policy-based account management

Group based account management

Application programming interfaces (APIs) that automate account management

Consolidated billing

Security with AWS Organizations

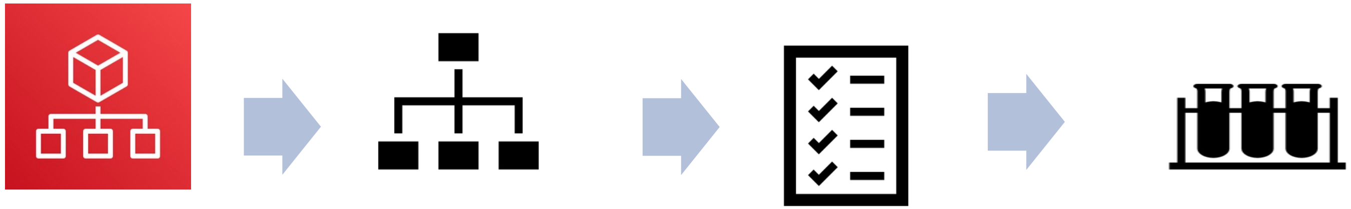
Control access with

AWS Identity and Access Management (IAM).

IAM policies enable you to allow or deny access to AWS services for users, groups, and roles.

Service control policies (SCPs) enable you to allow or deny access to AWS services for individuals or group accounts in an organizational unit (OU).

Organizations setup



Step 1 Create Organization

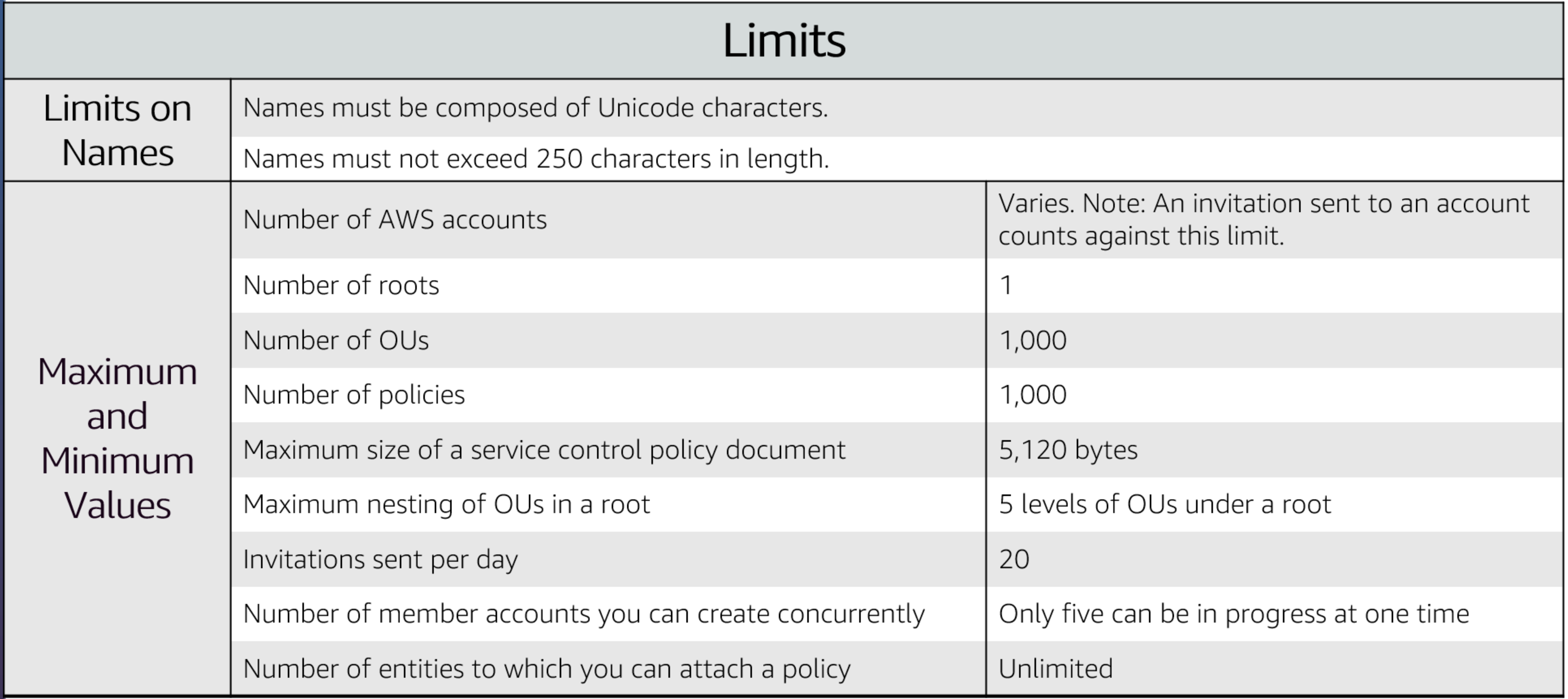
Step 2 Create organizational units

Step 3 Create service control policies

Step 4 Test restrictions

- Steps for setting up AWS Organizations:
  - Step 1 is to create your organization with your current AWS account as the primary account. You also invite one AWS account to join your organization and create another account as a member account.
  - Step 2 is to create two organizational units in your new organization and place the member accounts in those OUs.
  - Step 3 is to create service control policies, which enable you to apply restrictions to what actions can be delegated to users and roles in the member accounts. A service control policy is a type of organization control policy.
  - Step 4 is to test your organization’s policies. Sign in as a user for each of the roles (such as OU1 or OU2) and see how the service control policies impact account access. Alternatively, you can use the IAM policy simulator to test and troubleshoot IAM and resource-based policies that are attached to IAM users, groups, or roles in your AWS account.
- *Note: Keep in mind that this process assumes that you have access to two existing AWS accounts, and that you can sign in to each account as an administrator.*

Limits of AWS Organizations



Limits		
Limits on Names	Names must be composed of Unicode characters.	
	Names must not exceed 250 characters in length.	
Maximum and Minimum Values	Number of AWS accounts	Varies. Note: An invitation sent to an account counts against this limit.
	Number of roots	1
	Number of OUs	1,000
	Number of policies	1,000
	Maximum size of a service control policy document	5,120 bytes
	Maximum nesting of OUs in a root	5 levels of OUs under a root
	Invitations sent per day	20
	Number of member accounts you can create concurrently	Only five can be in progress at one time
	Number of entities to which you can attach a policy	Unlimited

Accessing AWS Organizations

AWS Organizations

- AWS Management Console
- AWS Command Line Interface (AWS CLI) tools
- Software development kits (SDKs)
- HTTPS Query application programming interfaces (API)

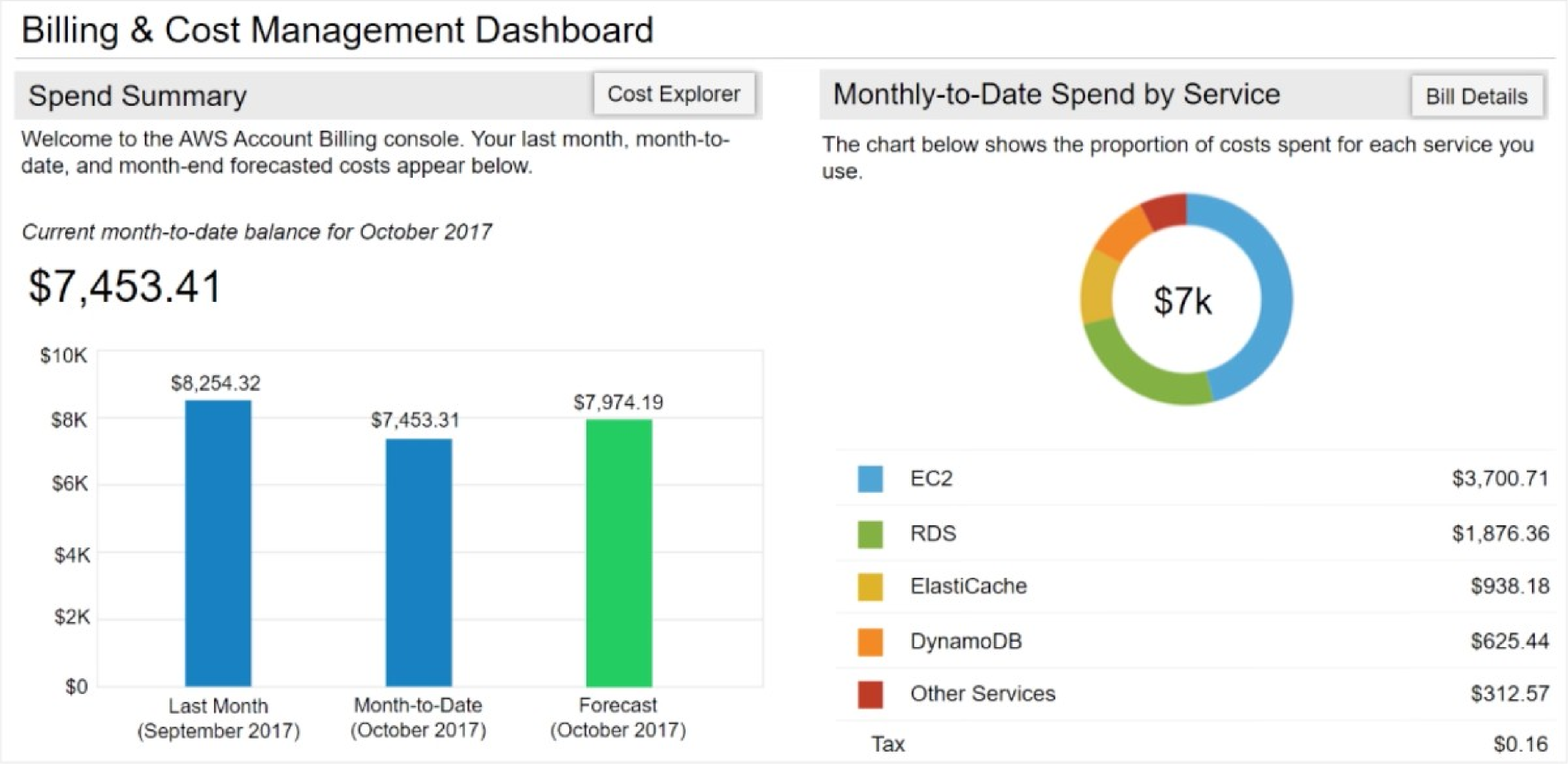
Ak chcete pridať obrázok, kliknite na ikonu

AWS Billing and Cost Management

Introducing AWS Billing and Cost Management

- Introducing AWS Billing and Cost Management
  - Service that is used for
    - to pay your AWS bill
    - monitor your usage
    - budget costs
  - Enables to forecast and obtain a better idea of what costs and usage might be in the future

AWS Billing Dashboard



Billing & Cost Management Dashboard

Spend Summary

Welcome to the AWS Account Billing console. Your last month, month-to-date, and month-end forecasted costs appear below.

Current month-to-date balance for October 2017

$7,453.41

Monthly-to-Date Spend by Service

The chart below shows the proportion of costs spent for each service you use.

🟦	EC2	$3,700.71
🟩	RDS	$1,876.36
🟨	ElastiCache	$938.18
🟧	DynamoDB	$625.44
🟥	Other Services	$312.57
	Tax	$0.16

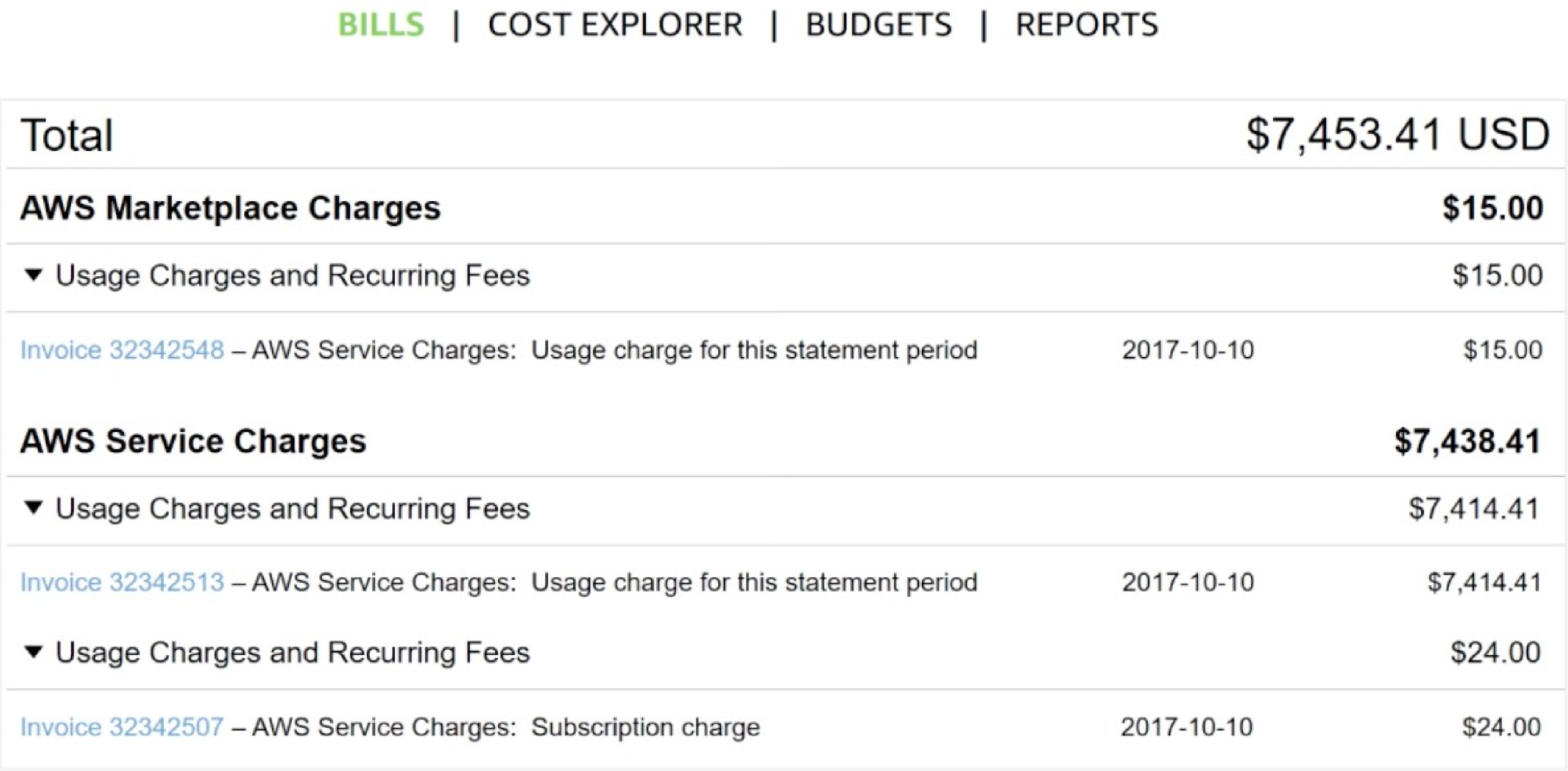
Tools

AWS Budgets

AWS Cost and Usage Report

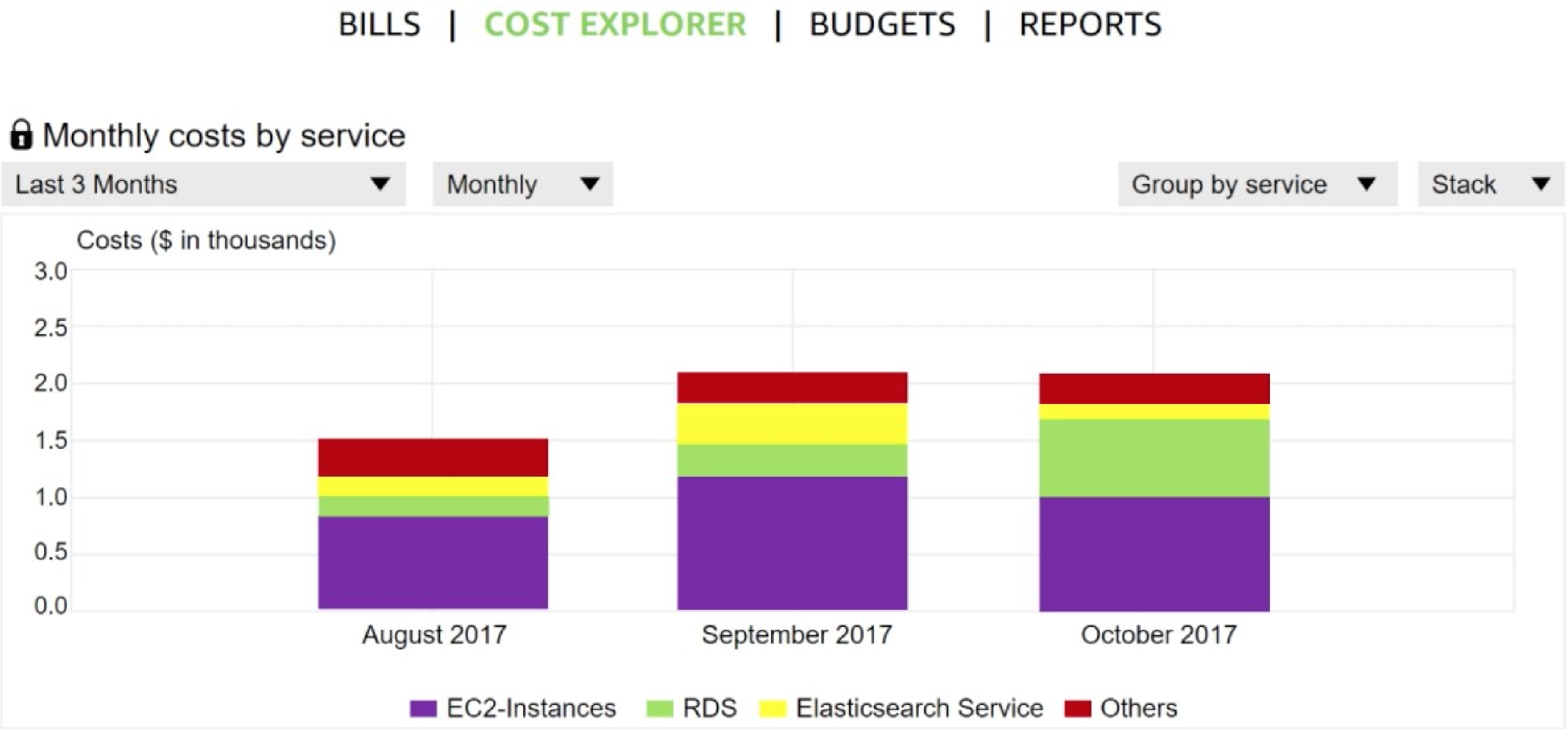
AWS Cost Explorer

Monthly bills



Total		$7,453.41 USD
AWS Marketplace Charges		**$15.00**
▼ Usage Charges and Recurring Fees		$15.00
Invoice 32342548 – AWS Service Charges: Usage charge for this statement period	2017-10-10	$15.00
AWS Service Charges		**$7,438.41**
▼ Usage Charges and Recurring Fees		$7,414.41
Invoice 32342513 – AWS Service Charges: Usage charge for this statement period	2017-10-10	$7,414.41
▼ Usage Charges and Recurring Fees		$24.00
Invoice 32342507 – AWS Service Charges: Subscription charge	2017-10-10	$24.00

Cost Explorer



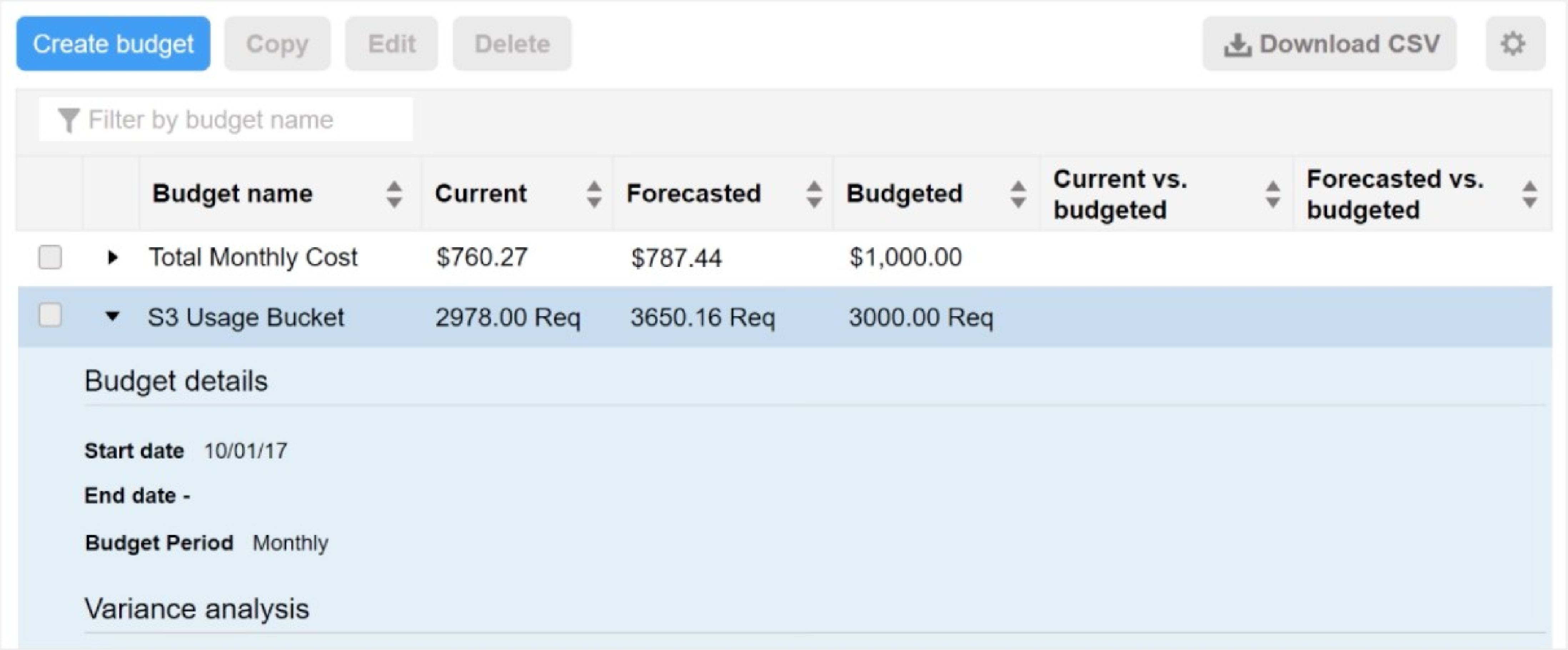
BILLS | COST EXPLORER | BUDGETS | REPORTS

Monthly costs by service

Last 3 Months ▼ Monthly ▼ Group by service ▼ Stack ▼

Forecast and track costs

BILLS | COST EXPLORER | BUDGETS | REPORTS



		Budget name	Current	Forecasted	Budgeted	Current vs. budgeted	Forecasted vs. budgeted
□	▸	Total Monthly Cost	$760.27	$787.44	$1,000.00		
□	▾	S3 Usage Bucket	2978.00 Req	3650.16 Req	3000.00 Req		

Budget details

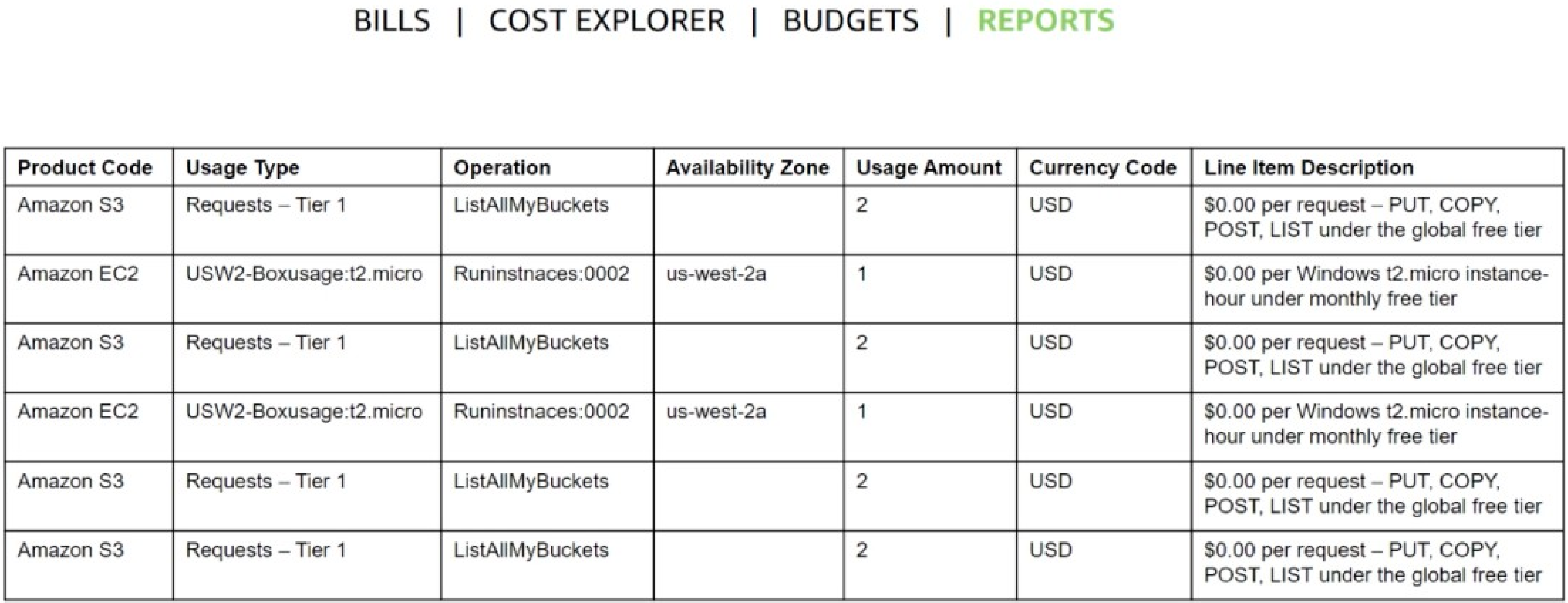
Start date 10/01/17

End date -

Budget Period Monthly

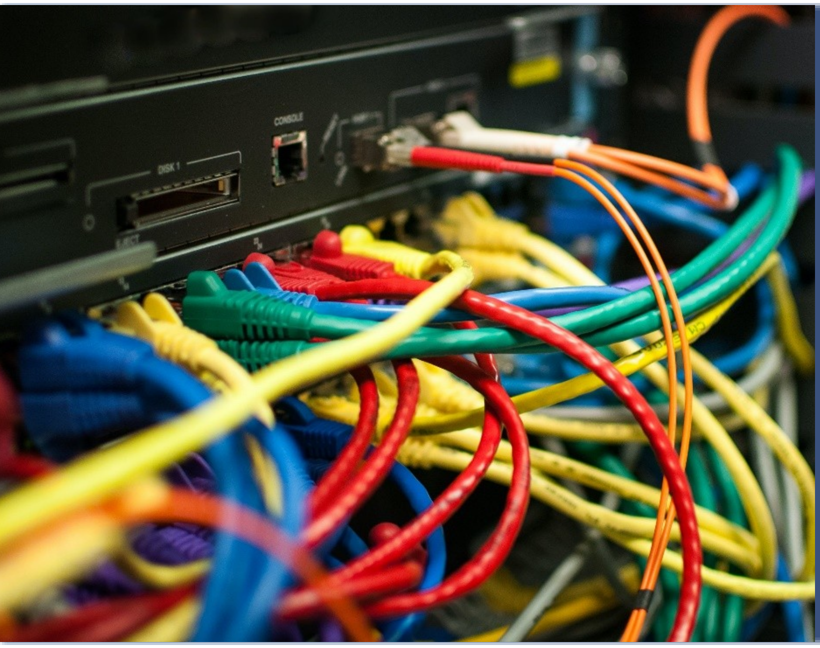
Variance analysis

Cost and usage reporting



BILLS | COST EXPLORER | BUDGETS | REPORTS

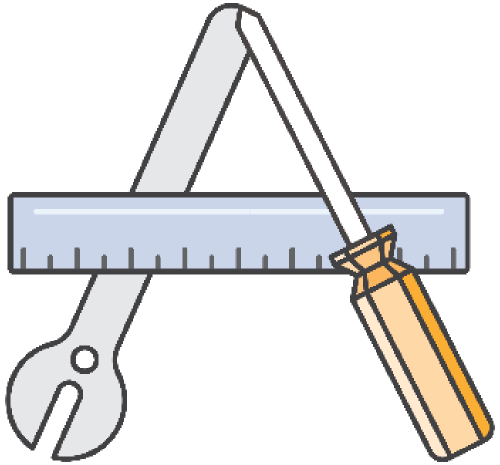
Product Code	Usage Type	Operation	Availability Zone	Usage Amount	Currency Code	Line Item Description
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	$0.00 per request – PUT, COPY, POST, LIST under the global free tier
Amazon EC2	USW2-Boxusage:t2.micro	Runinstnaces:0002	us-west-2a	1	USD	$0.00 per Windows t2.micro instance-hour under monthly free tier
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	$0.00 per request – PUT, COPY, POST, LIST under the global free tier
Amazon EC2	USW2-Boxusage:t2.micro	Runinstnaces:0002	us-west-2a	1	USD	$0.00 per Windows t2.micro instance-hour under monthly free tier
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	$0.00 per request – PUT, COPY, POST, LIST under the global free tier
Amazon S3	Requests – Tier 1	ListAllMyBuckets		2	USD	$0.00 per request – PUT, COPY, POST, LIST under the global free tier



AWS technical support

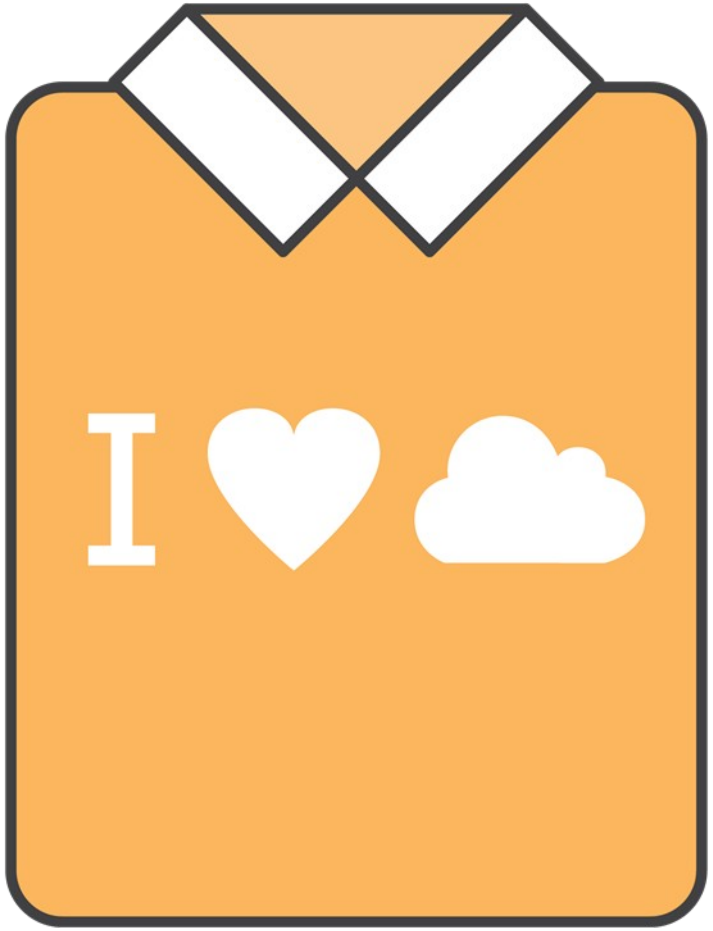
AWS support

- Provide unique combination of tools and expertise:
  - AWS Support
  - AWS Support Plans
- Support is provided for:
  - Experimenting with AWS
  - Production use of AWS
  - Business-critical use of AWS



AWS support

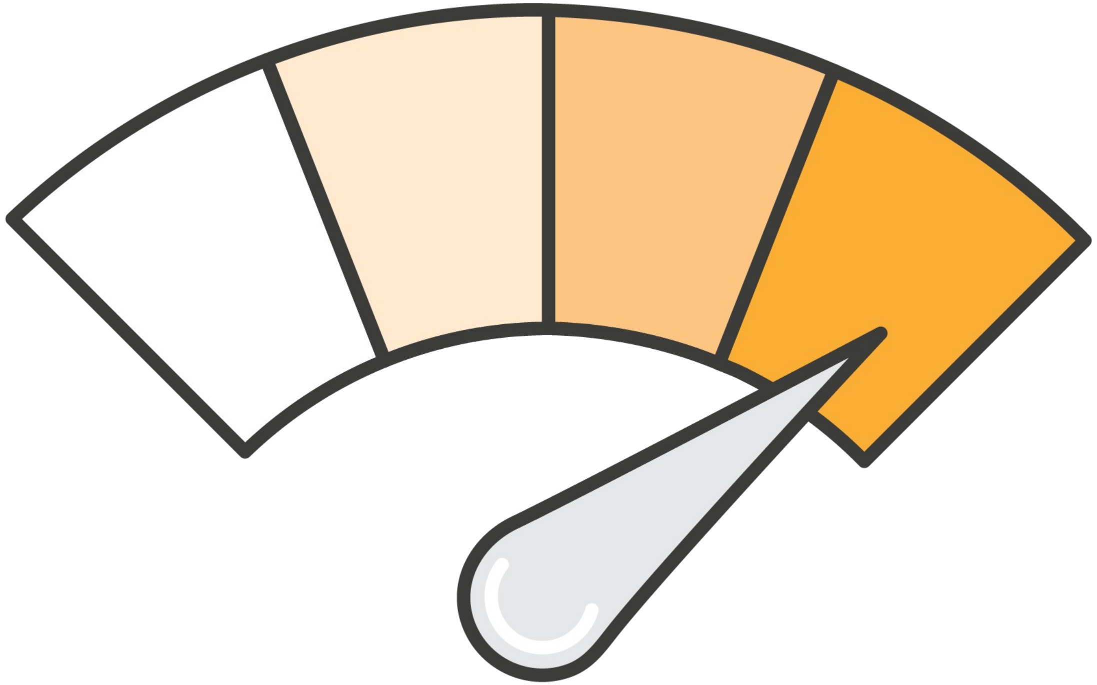
- Proactive guidance :
  - Technical Account Manager (TAM)
- Best practices :
  - AWS Trusted Advisor
- Account assistance :
  - AWS Support Concierge



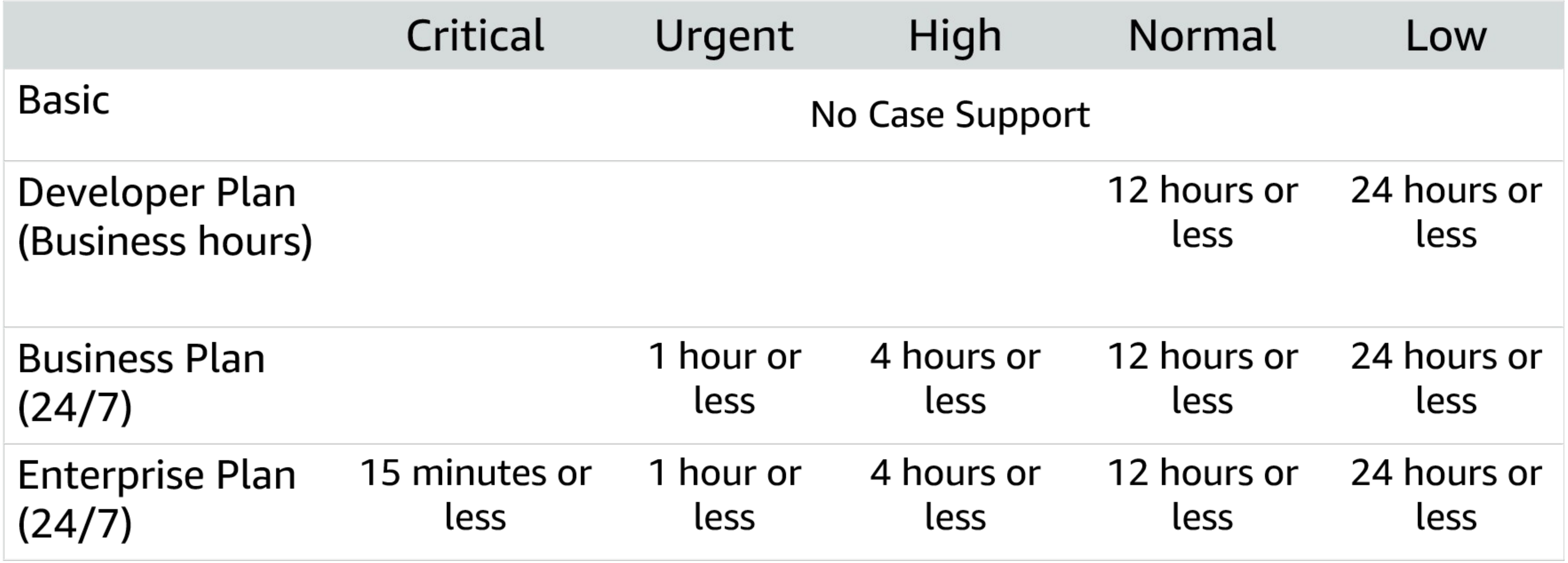
Support plans

AWS Support offers four support plans:

- **Basic Support** – Resource Center access, Service Health Dashboard, product FAQs, discussion forums, and support for health checks
- **Developer Support**: Support for early development on AWS
- **Business Support**: Customers that run production workloads
- **Enterprise Support**: Customers that run business and mission-critical workloads



Case severity and response times



	Critical	Urgent	High	Normal	Low
Basic	No Case Support				
Developer Plan (Business hours)				12 hours or less	24 hours or less
Business Plan (24/7)		1 hour or less	4 hours or less	12 hours or less	24 hours or less
Enterprise Plan (24/7)	15 minutes or less	1 hour or less	4 hours or less	12 hours or less	24 hours or less

Additional resources

- AWS Economics Center: http://aws.amazon.com/economics/
- AWS Pricing Calculator: https://calculator.aws/#/
- Case studies and research: http://aws.amazon.com/economics/
- Additional pricing exercises: https://dx1572sre29wk.cloudfront.net/cost/

UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Presentation 2 – AWS M4

- AWS M2 - Cloud Economics and Billing
- AWS M4 - AWS Cloud Security

aws academy

Vytvorené v rámci projektu **KEGA 026TUKE-4/2021**

Outline

- AWS shared responsibility model
- AWS Identity and Access Management (IAM)
- Securing a new AWS account
- Securing accounts
- Securing data on AWS
- Working to ensure compliance

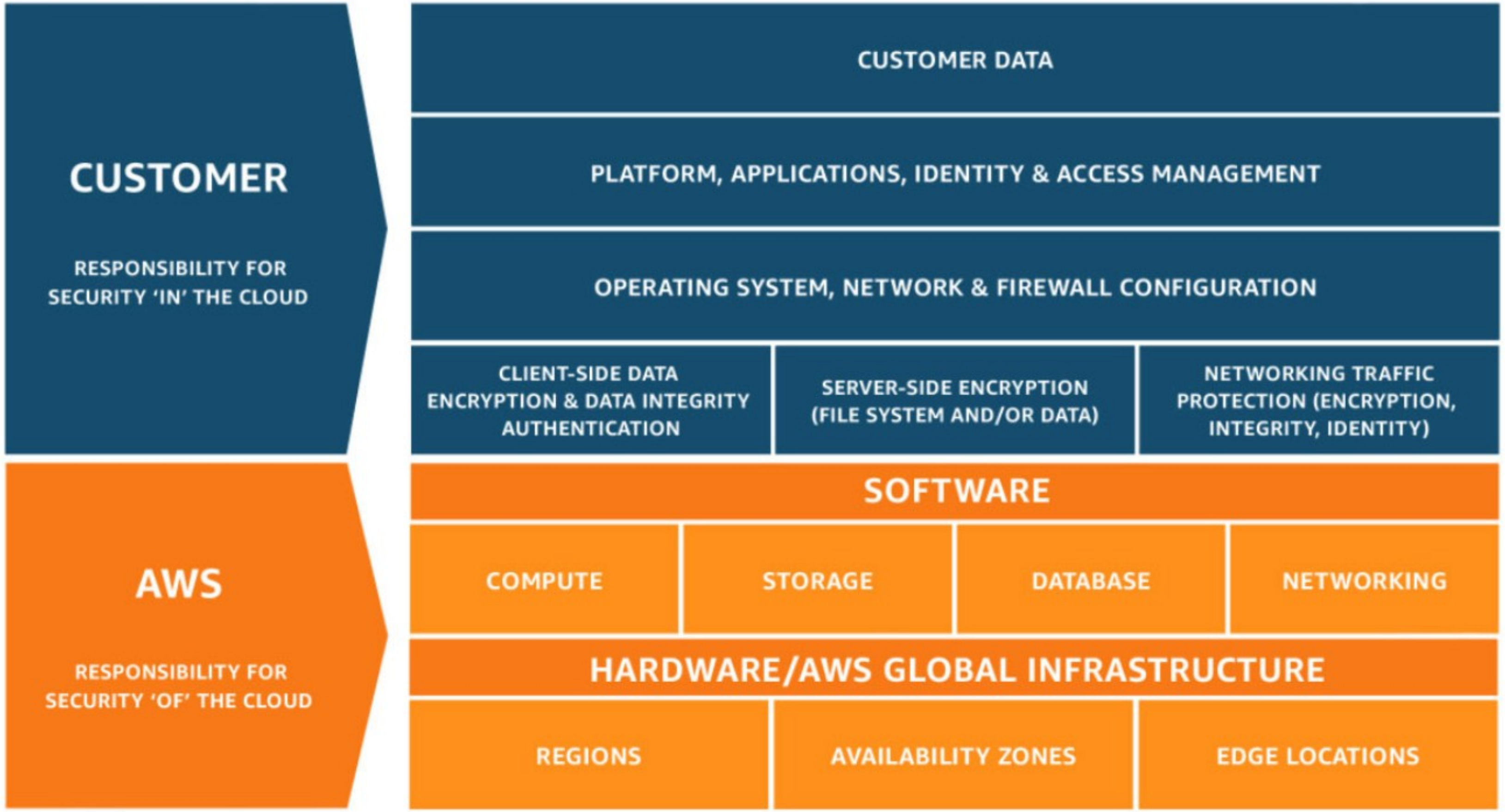
Ak chcete pridať obrázok, kliknite na ikonu

AWS shared responsibility model

AWS shared responsibility model

- Security and compliance
  - shared responsibility between the customer
  - And AWS

= *security “of” the cloud* versus *security “in” the cloud*



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

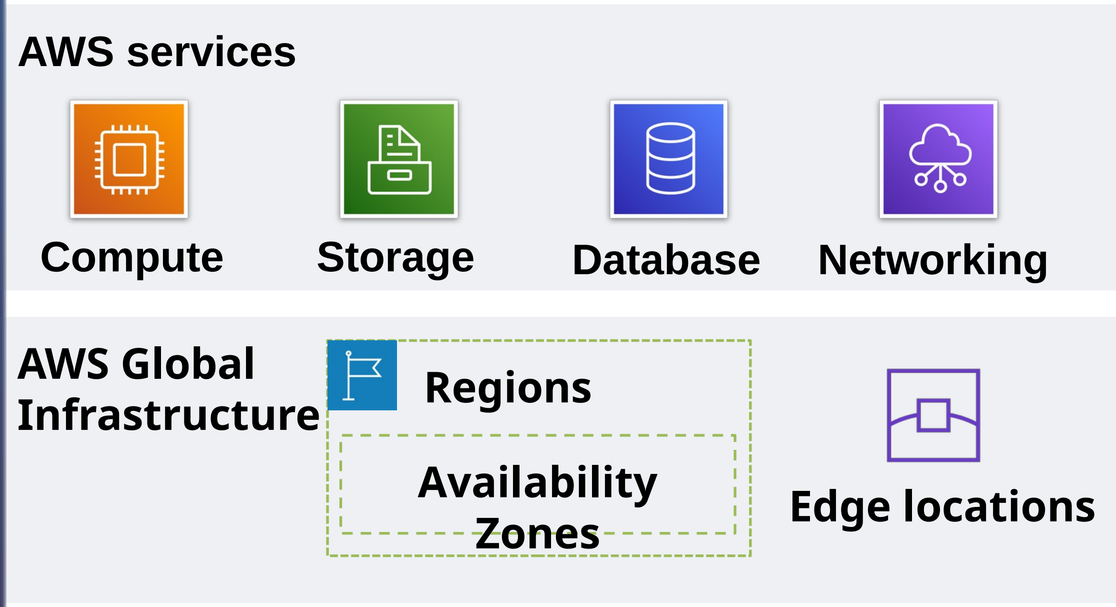
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

AWS responsibility: Security *of* the cloud


AWS services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Regions

Availability Zones

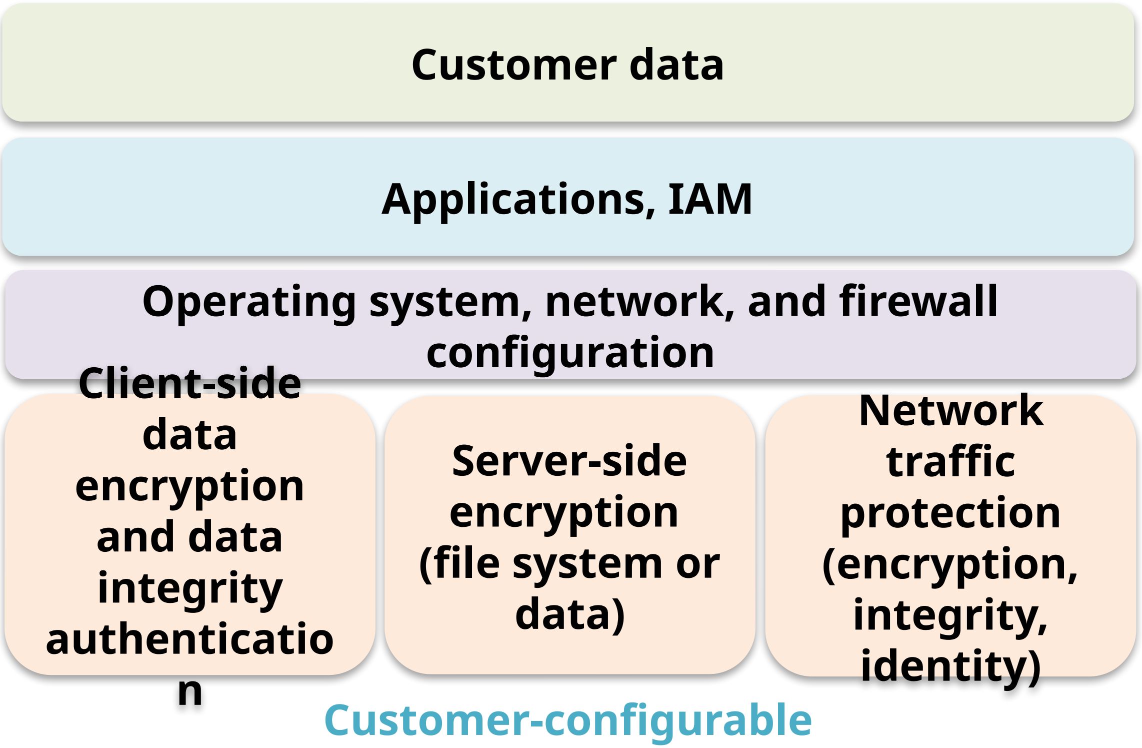
Edge locations

AWS responsibilities:

- Physical security of data centers
  - Controlled, need-based access
- Hardware and software infrastructure
  - Storage decommissioning, host operating system (OS) access logging, and auditing
- Network infrastructure
  - Intrusion detection
- Virtualization infrastructure
  - Instance isolation

Customer responsibility: Security in the cloud

- Customer responsibilities:
  - Amazon Elastic Compute Cloud (Amazon EC2) instance operating system
    - Including patching, maintenance
  - Applications and services
    - Passwords, role-based access, etc.
  - Security group configuration
  - OS or host-based firewalls
    - Including intrusion detection or prevention systems
  - Complete responsibilities for the content


Customer data
Applications, IAM
Operating system, network, and firewall configuration
Client-side data encryption and data integrity authenticatio n
Server-side encryption (file system or data)
Network traffic protection (encryption, integrity, identity)
Customer-configurable

- Network configurations
- Account management
  - Login and permission settings for each user

Service characteristics and security responsibility

- Examples

Example services managed by the customer

Amazon EC2

Amazon Elastic Block Store (Amazon EBS)

Amazon Virtual Private Cloud (Amazon VPC)

- **Infrastructure as a service (IaaS)**
  - Provides basic building blocks for cloud IT => similar to on-premise
  - Customer has more flexibility over configuring networking and storage settings
  - Customer is responsible for managing more aspects of the security
  - Customer configures the access controls
  - Provides the customer with the highest level of flexibility and management control over IT resources

Service characteristics and security responsibility

- Examples

Example services managed by AWS

AWS Lambda

Amazon Relational Database Service (Amazon RDS)

AWS Elastic Beanstalk

- **Platform as a service (PaaS)**
  - Customer does not need to manage the underlying infrastructure (WH, OS, etc.)
  - AWS handles
    - the operating system, database patching, firewall configuration, and disaster recovery
  - Customer can focus on managing code or data

Service characteristics and security responsibility

- Examples

SaaS examples

AWS Trusted Advisor

AWS Shield

Amazon Chime

- **Software as a service (SaaS)**
  - Software is centrally hosted
  - Licensed on a subscription model or pay-as-you-go basis.
  - Services are typically accessed via web browser, mobile app, or application programming interface (API)
  - Customers do not need to manage the infrastructure that supports the service

Ak chcete pridať obrázok, kliknite na ikonu

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)

- IAM
  - Allows to control access to compute, storage, database, and application services
  - Manages access to AWS resources, ie.. launching, configuring, managing, and terminating resources
    - A resource is an entity in an AWS account that you can work with
    - Example: Control who can terminate Amazon EC2 instances

- Define fine-grained access rights
  - Who can access the resource
  - Which resources can be accessed and what can the user do to the resource
  - How resources can be accessed
- IAM is a no-cost AWS account feature

AWS Identity and Access Management (IAM)

IAM: Essential components

IAM user

A **person** *or* **application** that can authenticate with an AWS account.

IAM group

A **collection of IAM users** that are granted identical authorization.

IAM policy

The document that defines **which resources can be accessed** and the **level of access** to each resource.

IAM role

Useful mechanism to grant a set of permissions for making AWS service requests.

Authenticate as an IAM user to gain access

- When you define an IAM user, you select what types of access the user is permitted to use.
- Programmatic access
  - Authenticate using:
    - Access key ID
    - Secret access key
  - Provides AWS CLI and AWS SDK access
- AWS Management Console access
  - Authenticate using:
    - 12-digit Account ID or alias
    - IAM user name
    - IAM password
  - If enabled, multi-factor authentication (MFA) prompts for an authentication code.

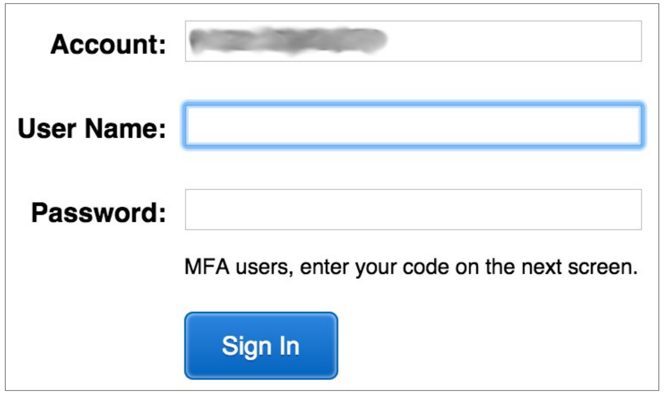
AWS CLI

AWS Tools and SDKs

AWS Management Console

IAM MFA

- MFA provides increased security.
- In addition to **user name** and **password**, MFA requires a unique authentication code to access AWS services.



Account: [redacted]

User Name:

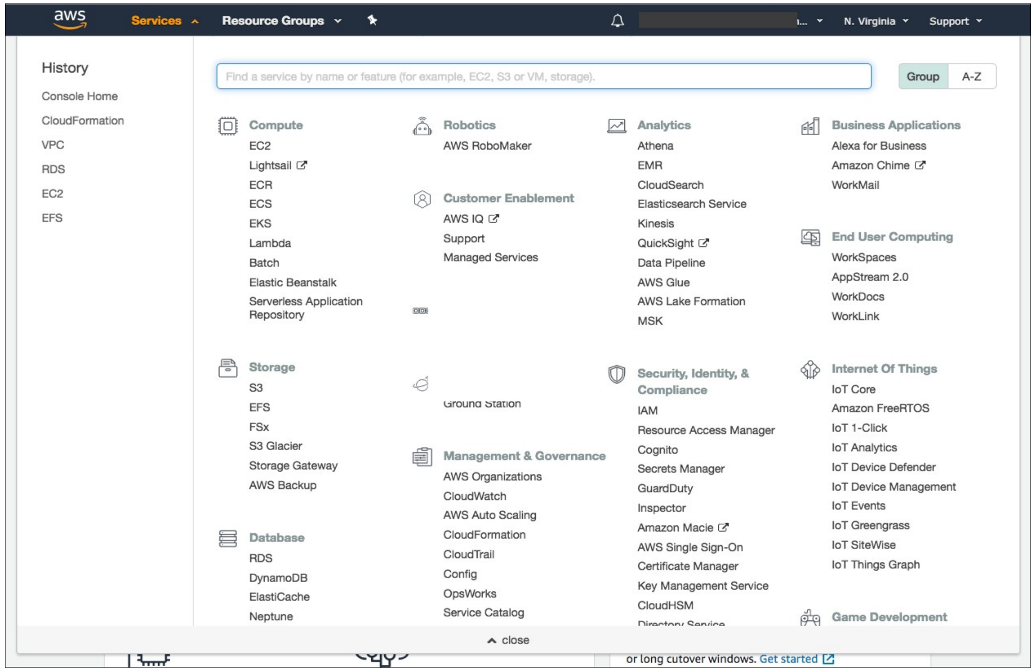
Password:

MFA users, enter your code on the next screen.

User name and password

MFA

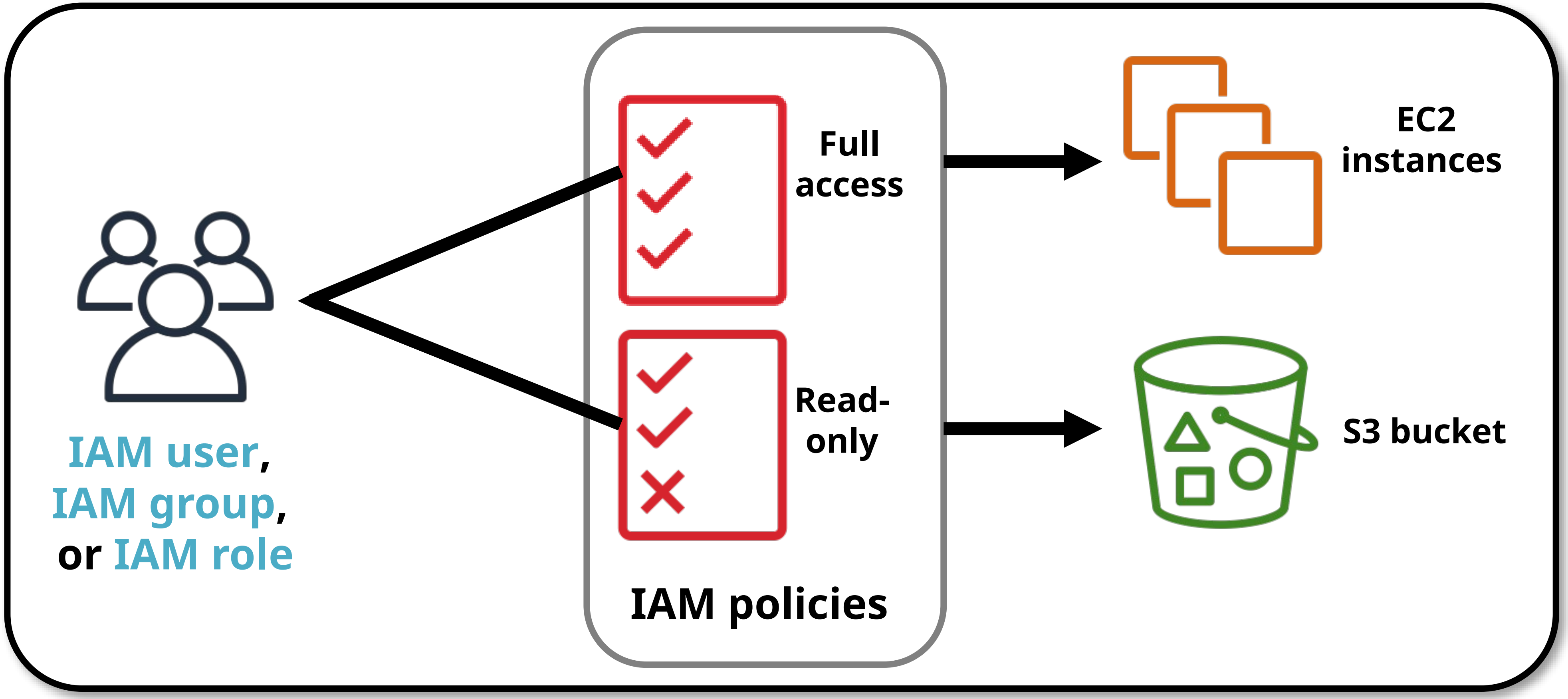
MFA token



AWS Management Console

Authorization: What actions are permitted

After the user or application is connected to the AWS account, what are they allowed to do?



- By default, IAM users do not have permissions to access any resources or data in an AWS account => must be explicitly granted permissions to a user, group, or role by creating a *policy*,

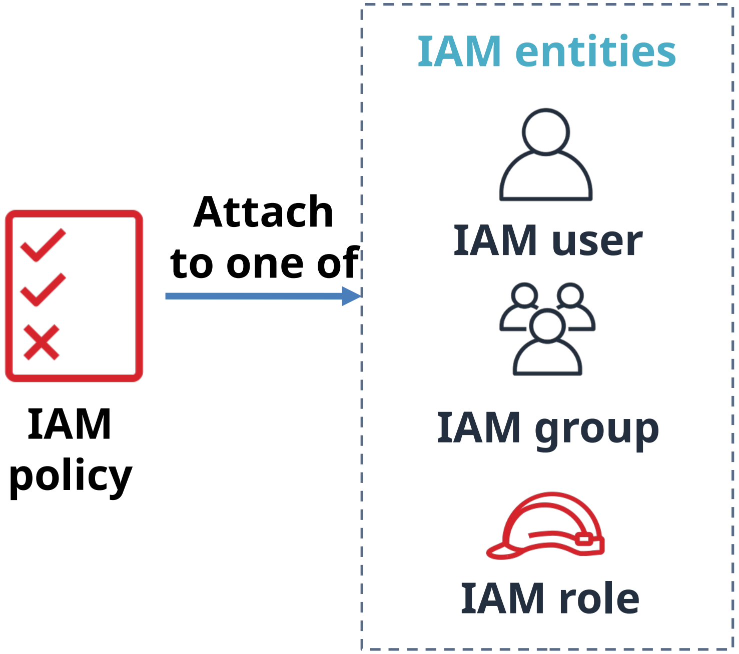
IAM: Authorization

- Assign permissions by creating an IAM policy.
- Permissions determine which resources and operations are allowed:
  - All permissions are implicitly denied by default.
  - If something is explicitly denied, it is never allowed.
- Best practice: Follow the principle of least privilege.
- ***Note****: The scope of IAM service configurations is global. Settings apply across all AWS Regions.*

IAM permissions

IAM policies

- **An IAM policy is a document that defines permissions**
  - Enables fine-grained access control
- Two types of policies – *identity-based* and *resource-based*
- **Identity-based** policies –
  - Attach a policy to any IAM entity
    - An IAM user, an IAM group, or an IAM role
  - Policies specify:
    - Actions that ***may*** be performed by the entity
    - Actions that ***may not*** be performed by the entity
  - A single *policy* can be attached to multiple *entities*
  - A single *entity* can have multiple *policies* attached to it
- **Resource-based** policies
  - Attached to a resource (such as an S3 bucket)



IAM policy example

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["DynamoDB:*","s3:*"],
    "Resource":[
          "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name”,
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Explicit allow gives users access to a specific DynamoDB table and…

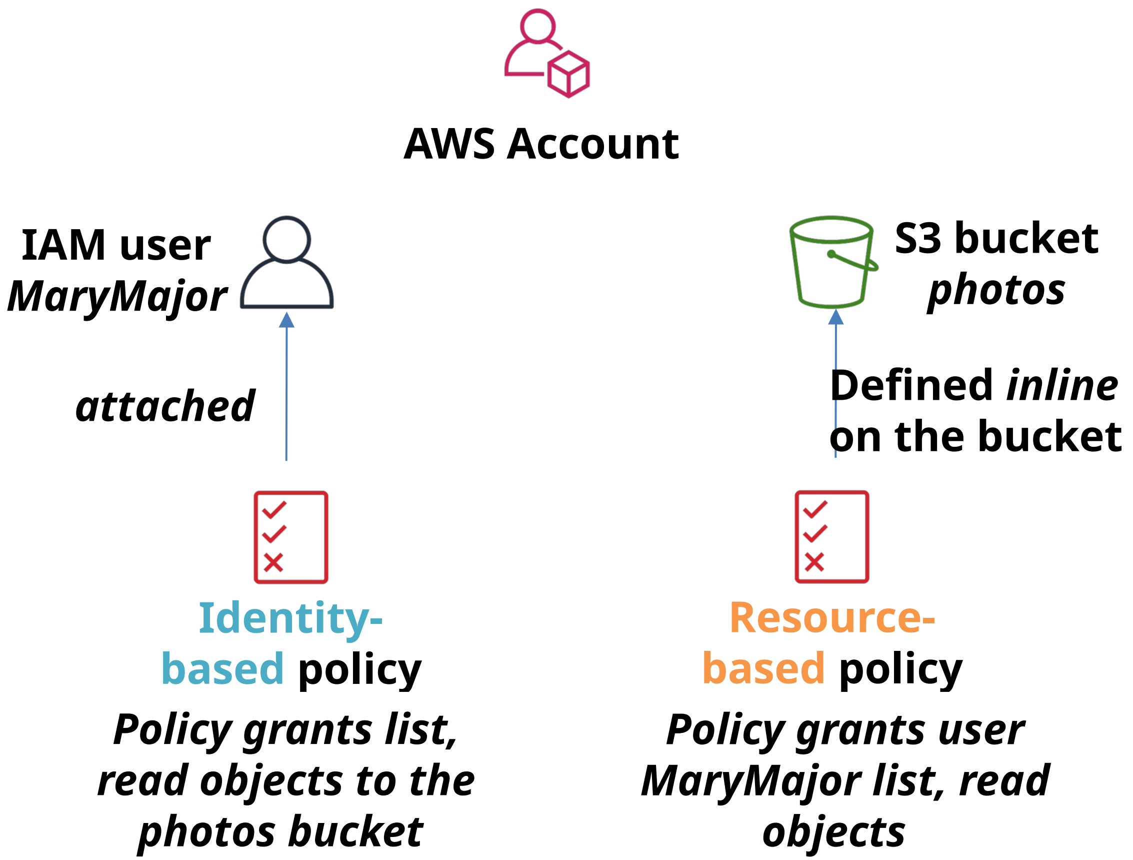
…Amazon S3 buckets.

Explicit deny ensures that the users cannot use any other AWS actions or resources other than that table and those buckets.

An explicit deny statement takes precedence over an allow statement.

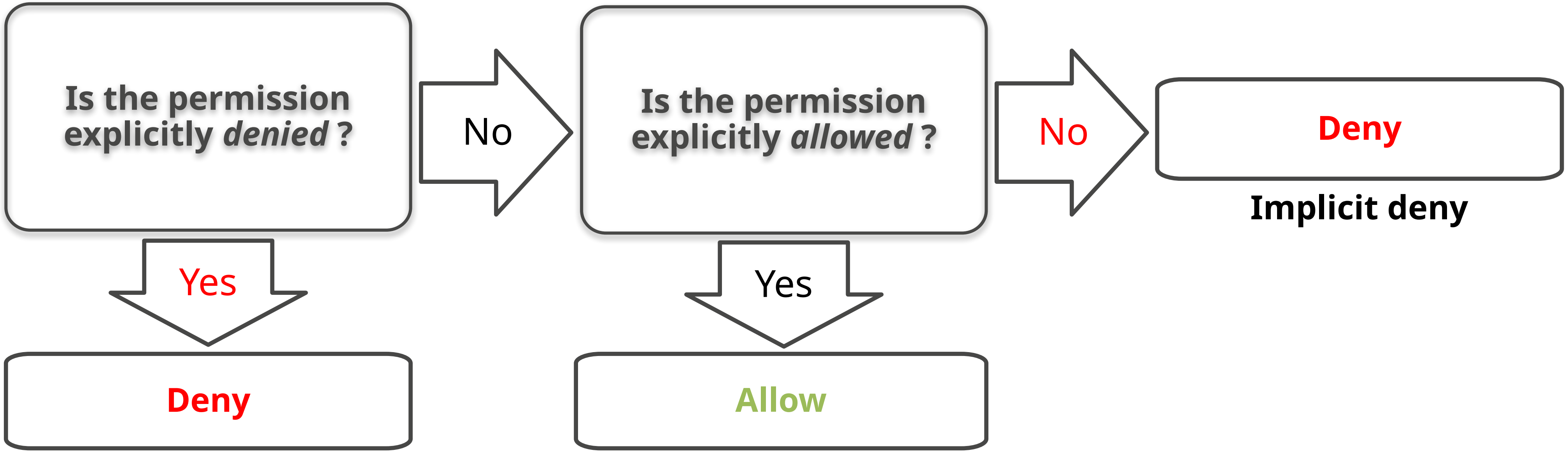
Resource-based policies

- *Identity-based policies* are attached to a user, group, or role
- **Resource-based policies** are attached to a resource (*not* to a user, group or role)
- Characteristics of resource-based policies –
  - Specifies who has access to the resource and what actions they can perform on it
  - The policies are *inline* only, not managed
- Resource-based policies are supported only by some AWS services


AWS Account
IAM user
MaryMajor
attached
S3 bucket
photos
Defined *inline* on the bucket
Identity-based policy
Policy grants list, read objects to the photos bucket
Resource-based policy
Policy grants user MaryMajor list, read objects

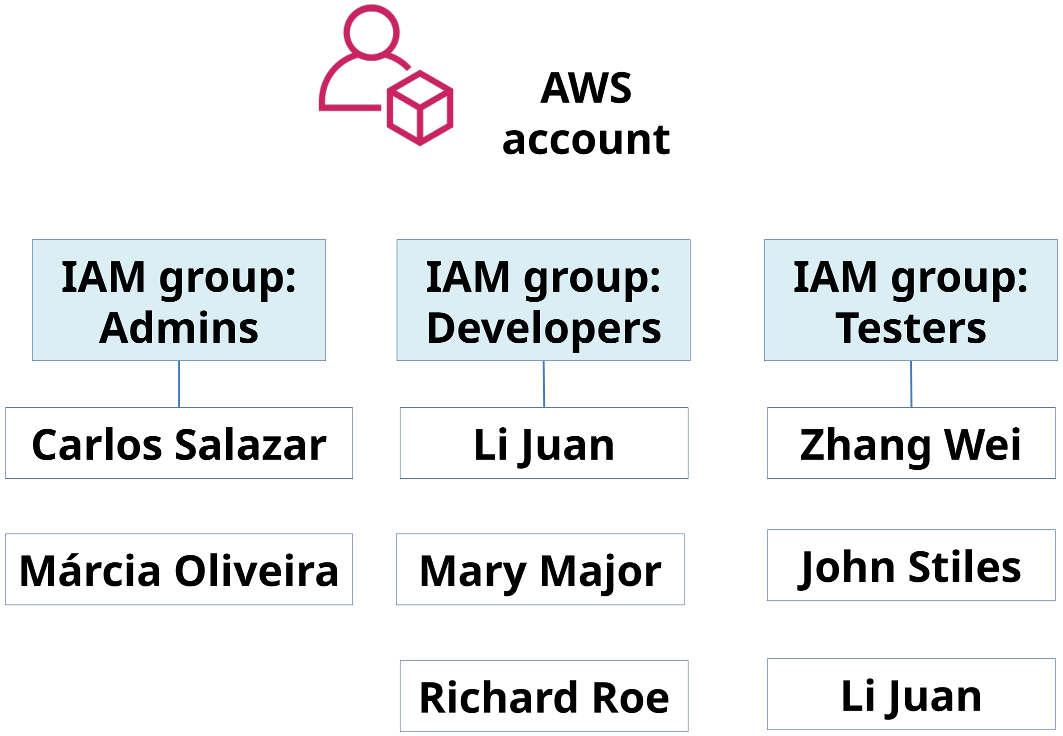
IAM permissions

How IAM determines permissions:


Is the permission explicitly *denied* ?
No
Is the permission explicitly *allowed* ?
No
Deny
Implicit deny
Yes
Deny
Yes
Allow

IAM groups

- An IAM group is a collection of IAM users
- A group is used to grant the same permissions to multiple users
    - Permissions granted by attaching IAM policy or policies to the group
- A user can belong to multiple groups
- There is no default group
- Groups cannot be nested



AWS account

IAM group: Admins	IAM group: Developers	IAM group: Testers
Carlos Salazar	Li Juan	Zhang Wei
Márcia Oliveira	Mary Major	John Stiles
	Richard Roe	Li Juan

IAM roles

- An **IAM role** is an IAM identity with specific permissions
- Similar to an IAM user
  - Attach permissions policies to it
- Different from an IAM user
  - Not uniquely associated with one person
  - Intended to be *assumable* by a **person**, **application**, or **service**
- Role provides *temporary* security credentials
- Examples of how IAM roles are used to **delegate** access –
  - Used by an IAM user in the same AWS account as the role
  - Used by an AWS service—such as Amazon EC2—in the same account as the role
  - Used by an IAM user in a different AWS account than the role

IAM role

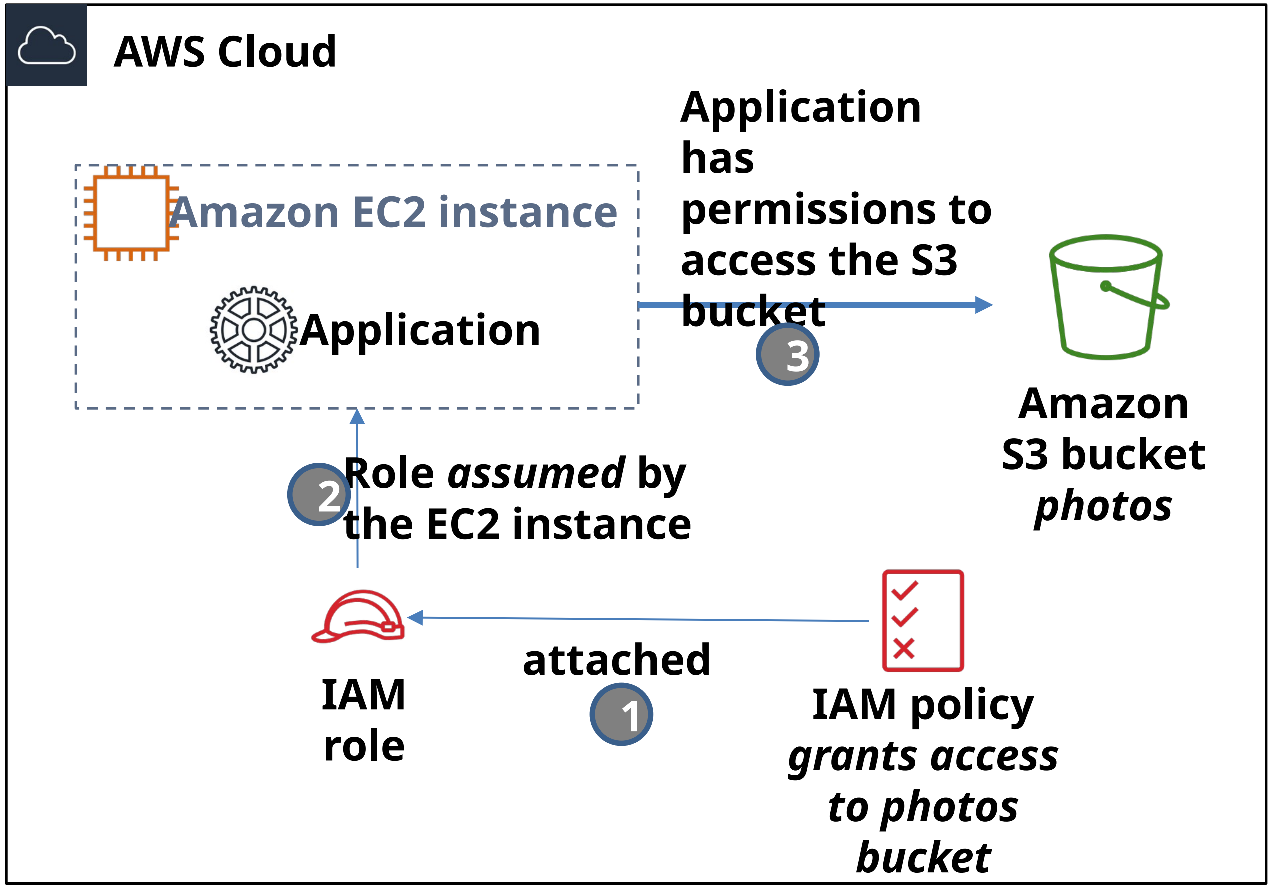
Example use of an IAM role

Scenario:

- An application that runs on an EC2 instance needs access to an S3 bucket

Solution:

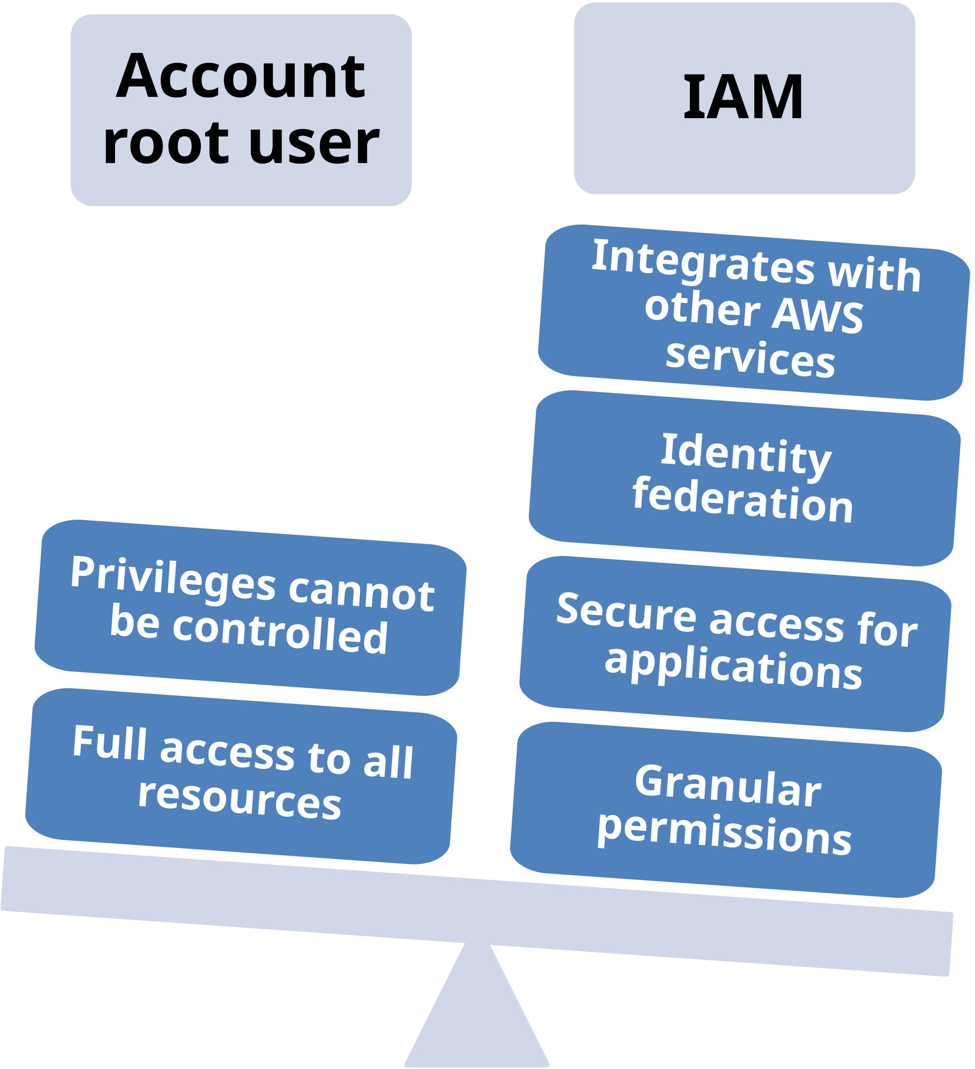
- Define an IAM policy that grants access to the S3 bucket.
- Attach the policy to a role
- Allow the EC2 instance to assume the role


AWS Cloud
Application has permissions to access the S3 bucket
Amazon EC2 instance
Application
3
Amazon S3 bucket *photos*
2
Role *assumed* by the EC2 instance
attached
1
IAM role
IAM policy *grants access to photos bucket*

Ak chcete pridať obrázok, kliknite na ikonu

Securing a new AWS account

AWS account root user access versus IAM access


Account root user
IAM
Integrates with other AWS services
Identity federation
Privileges cannot be controlled
Secure access for applications
Full access to all resources
Granular permissions

- Creating a first AWS account **= AWS account root user**
  - **full** access to all AWS services and resources !!!
  - **Best practice**: Do not use the AWS account root user except when necessary.
    - Access to the **account root user**
      - logging in with the *email address* (and password) that you used to create the account
    - Create an additional accounts
- Example actions that can only be done with the account root user:
  - Update the account root user password
  - Change the AWS Support plan
  - Restore an IAM user's permissions
  - Change account settings (for example, contact information, allowed Regions)

Securing a new AWS account: Account root user

Step 1: Stop using the account root user as soon as possible.

  - The account root user has unrestricted access to all your resources.

- To stop using the account root user:
  1. While you are logged in as the account root user, create an IAM user for yourself. Save the access keys if needed.
  2. Create an IAM group, give it full administrator permissions, and add the IAM user to the group.
  3. Disable and remove your account root user access keys, if they exist.
  4. Enable a password policy for users.
  5. Sign in with your new IAM user credentials.
  6. Store your account root user credentials in a secure place.

Securing a new AWS account: MFA

Step 2: Enable multi-factor authentication (MFA).

- Require MFA for your account root user and for all IAM users.
- You can also use MFA to control access to AWS service APIs.

- Options for retrieving the MFA token –
  - Virtual MFA-compliant applications:
    - Google Authenticator.
    - Authy Authenticator (Windows phone app).
  - U2F security key devices:
    - For example, YubiKey.
  - Hardware MFA options:
    - Key fob or display card offered by Gemalto.

MFA

MFA token

Securing a new AWS account: AWS CloudTrail

Step 3: Use AWS CloudTrail.

- CloudTrail tracks user activity on your account.
  - Logs all API requests to resources in all supported services your account.
- Basic AWS CloudTrail event history is enabled by default and is free.
  - It contains all management event data on latest 90 days of account activity.

- To access CloudTrail
  1. Log in to the **AWS Management Console** and choose the **CloudTrail** service.
  2. Click **Event history** to view, filter, and search the last 90 days of events.
- **To enable logs beyond 90 days and enable specified event alerting, create a trail.**
  1. From the CloudTrail Console trails page, click **Create trail**.
  2. Give it a name, apply it to all Regions, and create a new Amazon S3 bucket for log storage.
  3. Configure access restrictions on the S3 bucket (for example, only admin users should have access).

Securing a new AWS account: Billing reports

Step 4: Enable a billing report, **such as the AWS Cost and Usage Report.**

- Billing reports provide information about your use of AWS resources and estimated costs for that use.
- AWS delivers the reports to an Amazon S3 bucket that you specify.
  - Report is updated at least once per day.
- The **AWS Cost and Usage Report** tracks your AWS usage and provides estimated charges associated with your AWS account, either by the hour or by the day.

Ak chcete pridať obrázok, kliknite na ikonu

Securing accounts

AWS Organizations

AWS Organizations

- **AWS Organizations** enables you to consolidate multiple AWS accounts so that you centrally manage them.
- Security features of AWS Organizations:
  - **Group AWS accounts into organizational units** (OUs) and attach different access policies to each OU.
  - **Integration and support for IAM**
    - Permissions to a user are the intersection of what is allowed by AWS Organizations and what is granted by IAM in that account.
  - **Use service control policies** to establish control over the AWS services and API actions that each AWS account can access

AWS Organizations: Service control policies

- **Service control policies (SCPs)** offer centralized control over accounts.
  - Limit permissions that are available in an account that is part of an organization.

- Ensures that accounts comply with access control guidelines.

- SCPs are *similar* to IAM permissions policies –
  - They use similar syntax.
  - However, an SCP never grants permissions.
  - Instead, SCPs specify the maximum permissions for an organization.

AWS Key Management Service (AWS KMS)

AWS Key Management Service (AWS KMS)

- AWS Key Management Service (AWS KMS) features:
  - Enables you to create and manage encryption keys
  - Enables you to control the use of encryption across AWS services and in your applications.
  - Integrates with AWS CloudTrail to log all key usage.
  - Uses hardware security modules (HSMs) that are validated by Federal Information Processing Standards (FIPS) 140-2 to protect keys

Amazon Cognito

Amazon Cognito

- Amazon Cognito features:
  - Adds user sign-up, sign-in, and access control to your web and mobile applications.
  - Scales to millions of users.
  - Supports sign-in with social identity providers, such as Facebook, Google, and Amazon; and enterprise identity providers, such as Microsoft Active Directory via Security Assertion Markup Language (SAML) 2.0.

AWS Shield

AWS Shield

- AWS Shield features:
  - Is a managed distributed denial of service (DDoS) protection service
  - Safeguards applications running on AWS
  - Provides always-on detection and automatic inline mitigations

  - AWS Shield Standard enabled for at no additional cost. AWS Shield Advanced is an optional paid service.
- Use it to minimize application downtime and latency.

Ak chcete pridať obrázok, kliknite na ikonu

Securing data on AWS

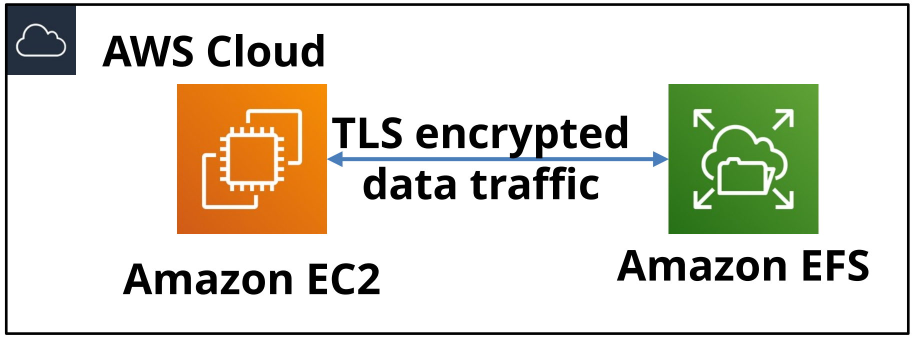
Encryption of data *at rest*

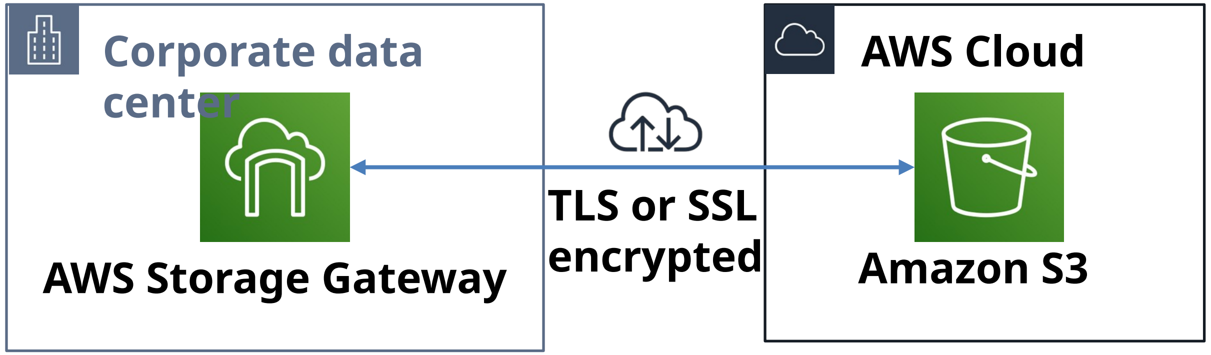
- **Encryption** encodes data with a secret key, which makes it unreadable
  - Only those who have the secret key can decode the data
  - AWS KMS can manage your secret keys

- AWS supports encryption of **data at rest**
  - Data at rest = Data stored physically (on disk or on tape)
  - You can encrypt data stored in any service that is supported by AWS KMS, including:
    - Amazon S3
    - Amazon EBS
    - Amazon Elastic File System (Amazon EFS)
    - Amazon RDS managed databases

Encryption of data *in transit*

- Encryption of **data in transit** (data moving across a network)
  - **Transport Layer Security (TLS)**—formerly SSL—is an open standard protocol
  - **AWS Certificate Manager** provides a way to manage, deploy, and renew TLS or SSL certificates
- Secure HTTP (HTTPS) creates a secure tunnel
  - Uses TLS or SSL for the bidirectional exchange of data
- **AWS services support data in transit encryption**.
  - Two examples:





Securing Amazon S3 buckets and objects

- Newly created S3 buckets and objects are private and protected by default.
- When use cases require sharing data objects on Amazon S3
  - It is essential to manage and control the data access.
  - Follow the **permissions that follow the principle of least privilege** and consider using Amazon S3 encryption.
- Tools and options for controlling access to S3 data include
  - Amazon S3 Block Public Access feature: Simple to use.
  - IAM policies: A good option when the user can authenticate using IAM.
  - Bucket policies
  - Access control lists (ACLs): A legacy access control mechanism.
  - AWS Trusted Advisor bucket permission check: A free feature.

Ak chcete pridať obrázok, kliknite na ikonu

Working to ensure compliance

AWS compliance programs

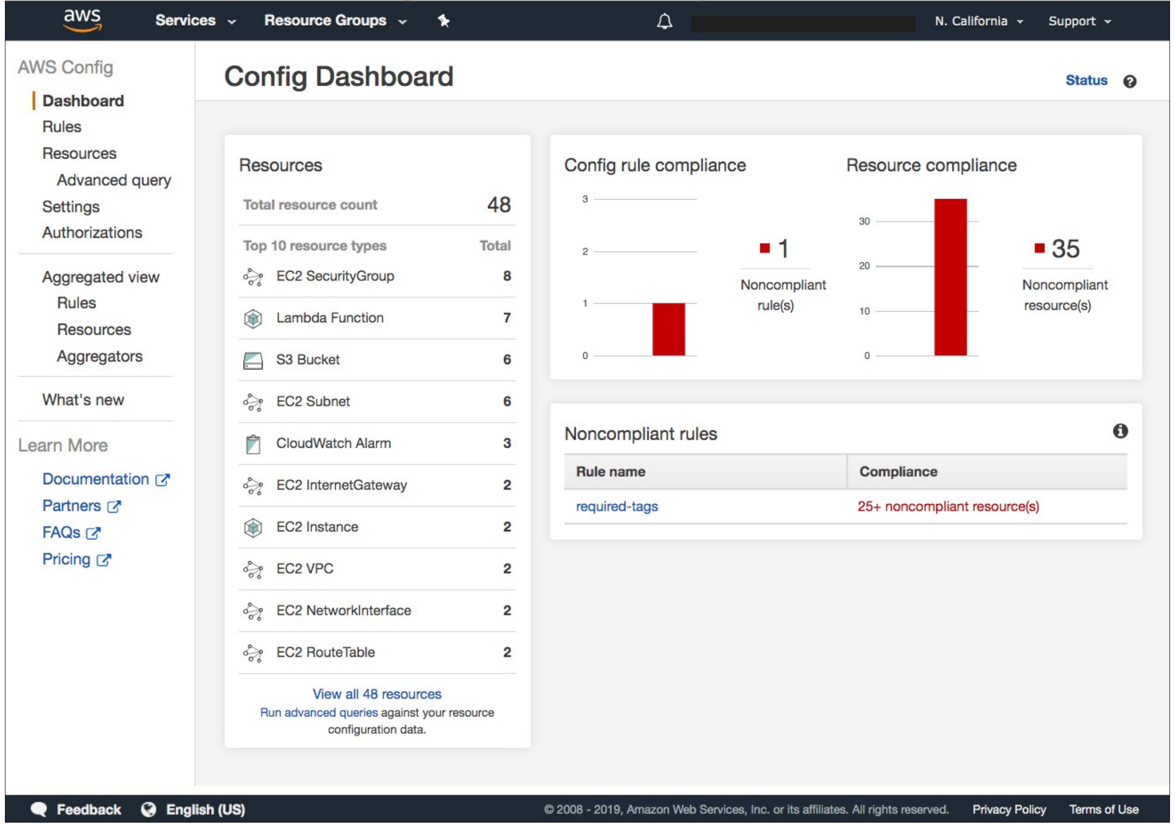
- Customers are subject to many different security and compliance regulations and requirements.
- **AWS engages with certifying bodies and independent auditors to provide customers with detailed information about the policies, processes, and controls that are established and operated by AWS.**

- Compliance programs can be broadly categorized –
  - **Certifications and attestations**
    - Assessed by a third-party, independent auditor
    - Examples: ISO 27001, 27017, 27018, and ISO/IEC 9001
  - **Laws, regulations, and privacy**
    - AWS provides security features and legal agreements to support compliance
    - Examples: EU General Data Protection Regulation (GDPR), HIPAA
  - **Alignments and frameworks**
    - Industry- or function-specific security or compliance requirements
    - Examples: Center for Internet Security (CIS), EU-US Privacy Shield certified

AWS Config

AWS Config

Example AWS Config Dashboard view



[redacted]

AWS Config

- Dashboard
- Rules
- Resources
  - Advanced query
- Settings
- Authorizations
- Aggregated view
  - Rules
  - Resources
  - Aggregators
- What's new

Learn More

- Documentation
- Partners
- FAQs
- Pricing

Config Dashboard

Status

Resources

Total resource count 48

Top 10 resource types	Total
EC2 SecurityGroup	8
Lambda Function	7
S3 Bucket	6
EC2 Subnet	6
CloudWatch Alarm	3
EC2 InternetGateway	2
EC2 Instance	2
EC2 VPC	2
EC2 NetworkInterface	2
EC2 RouteTable	2

View all 48 resources

Run advanced queries against your resource configuration data.

Config rule compliance

🟥 1

Noncompliant rule(s)

Resource compliance

🟥 35

Noncompliant resource(s)

Noncompliant rules

Rule name	Compliance
required-tags	25+ noncompliant resource(s)

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- **Assess, audit, and evaluate the configurations of AWS resources.**
- Use for continuous monitoring of configurations.
- Automatically evaluate *recorded* configurations versus *desired* configurations.
- Review configuration changes.
- View detailed configuration histories.
- **Simplify compliance auditing and security analysis.**

AWS Artifact

AWS Artifact

- Is a resource for compliance-related information
- Provide access to security and compliance reports, and select online agreements
- Can access example downloads:
  - AWS ISO certifications
  - Payment Card Industry (PCI) and Service Organization Control (SOC) reports
- Access AWS Artifact directly from the AWS Management Console
  - Under **Security, Identify & Compliance**, click **Artifact**.

UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Thank you for your attention.

Vytvorené v rámci projektu **026TUKE-4/2021**