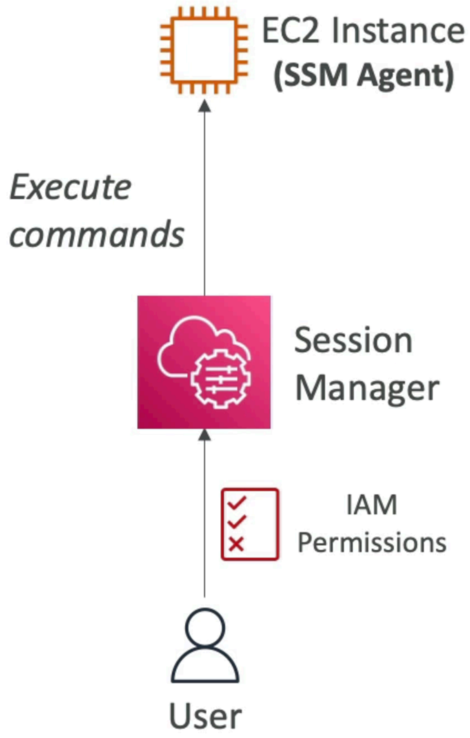
Amazon Web Services (Security)

Agenda

- System Manger – SSM Session Manger
- CloudWatch logs
- CloudTrail
- Config
- Trusted Advisor

System Manger – SSM Session Manger

- Allows you to start a secure shell on your EC2 and on-premises servers.
- **No SSH access, Bastion hosts, or SSH keys needed**
- **No port 22 needed (better security)**
- Supports Linux, MacOS, and Windows
- Send session log tata to S3 or CloudWatch Logs



- Create EC2 instance without SSH – 22, and go to advanced setting
- Select “IAM profile ” create IAM role and attach or go to running EC2 instance and attach IAM role (role : for EC2, “SSMManagedinstancecore” create. & attach
- Now got to ”AWS System Manager ” left panel “fleet manager” (we can check all SSM register instance details) wait for some time then it will show you all instance list with online SSM agent.
- Now left panel select “session Manger” start session.select EC2 and start session you will connect with ssh (secure shell) now any commands like … ping google.com, host, hostname etc.
- Left panel select “Run Command” and select instances and execute commands.

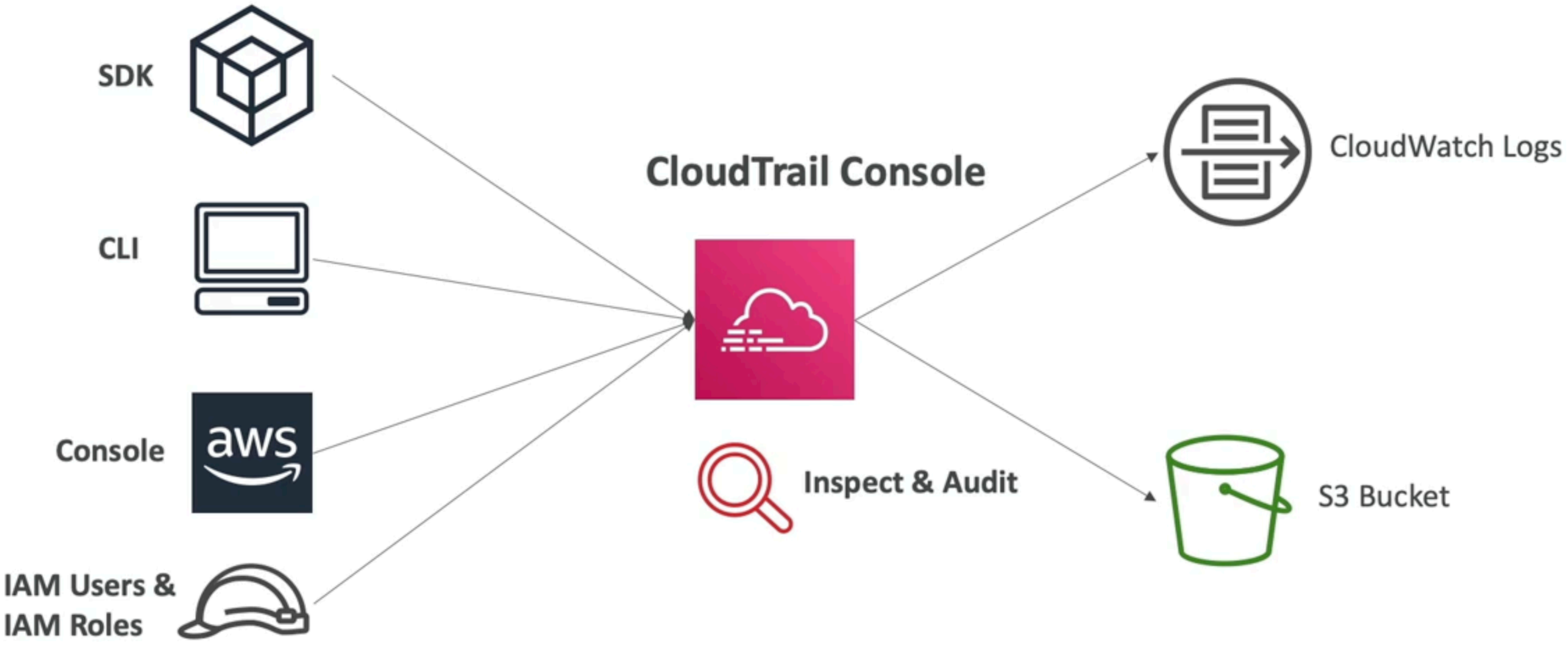
CloudWatch Logs

- Log groups: usually representing and application
- Log stream: instances within application / log files / containers
- Can define log expiration policies (never expire, 1 day to 10 years)
- Logs are encrypted by default
- Cloudwatch logs can send logs to:
  - Amazon S3
  - Kinesis data streams
  - AWS Lambda… etc

AWS CloudTrail (Tracking user activity and API usage)

- Provides governance, compliance and audit for your AWS Account
- CloudTrail is enabled by default!
- Get an history of events / API calls made within your AWS Account by:
  - Console
  - Clli
  - SDK
- Can put logs from CloudTrail into CloudWatch Logs or S3
- A trail can be applied to all region (default) or a single region.
- If a resource is deleted in AWS, investigate CloudTrail first!

CloudTrail Diagram



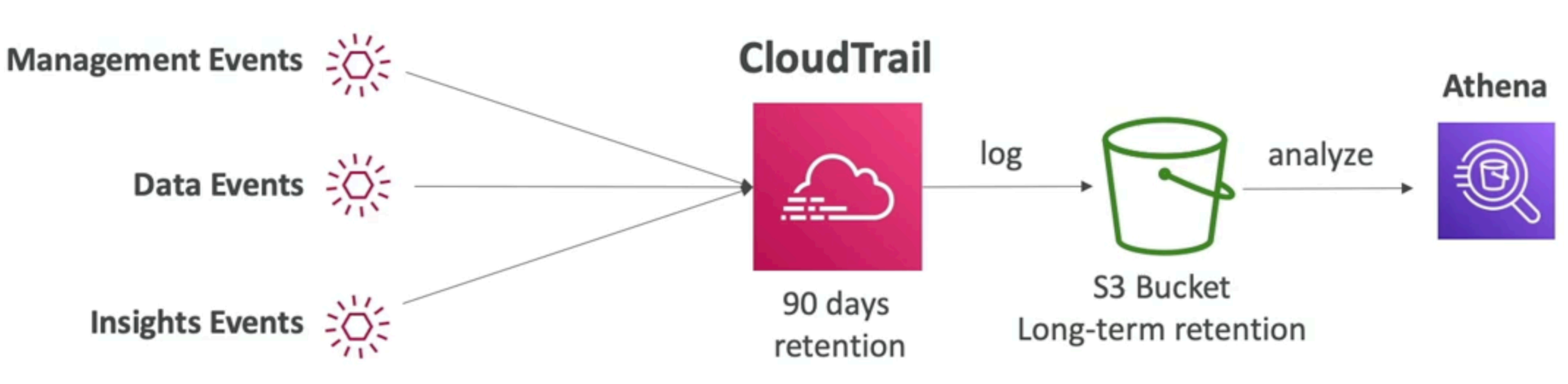
CloudTrail Events

- Management Events:
  - Operations that are performed on resources in your AWS account
  - Examples:
    - Configuring security (IAM attachRolePolicy)
    - Configuring rules for routing data (AWS EC2 create subnet)
    - Setting up logging (Aws Trail createTrail)
- Data Events:
  - By default dta events are not logged (because high volume operations)
  - AWS S3 object-level activity
  - AWS Lambda function execution activity
- CloudTrial Insights Events: Unusual activity in your account (hitting service limit, gaps in maintenance activity etc)

CloudTrail Events Retention

- Events are stored for 90 days in CloudTrail
- To keep events beyond this period, log them to s3 and use Athena

(Athena: serverless service to query data in S3)



AWS Config

- Helps with auditing and recording compliance of your AWS resources
- Helps record configurations and changes over time
- You can receive alerts (SNS notifications) for any changes
- AWS config is a per-region service

- Questions that can be solved by AWS Config?

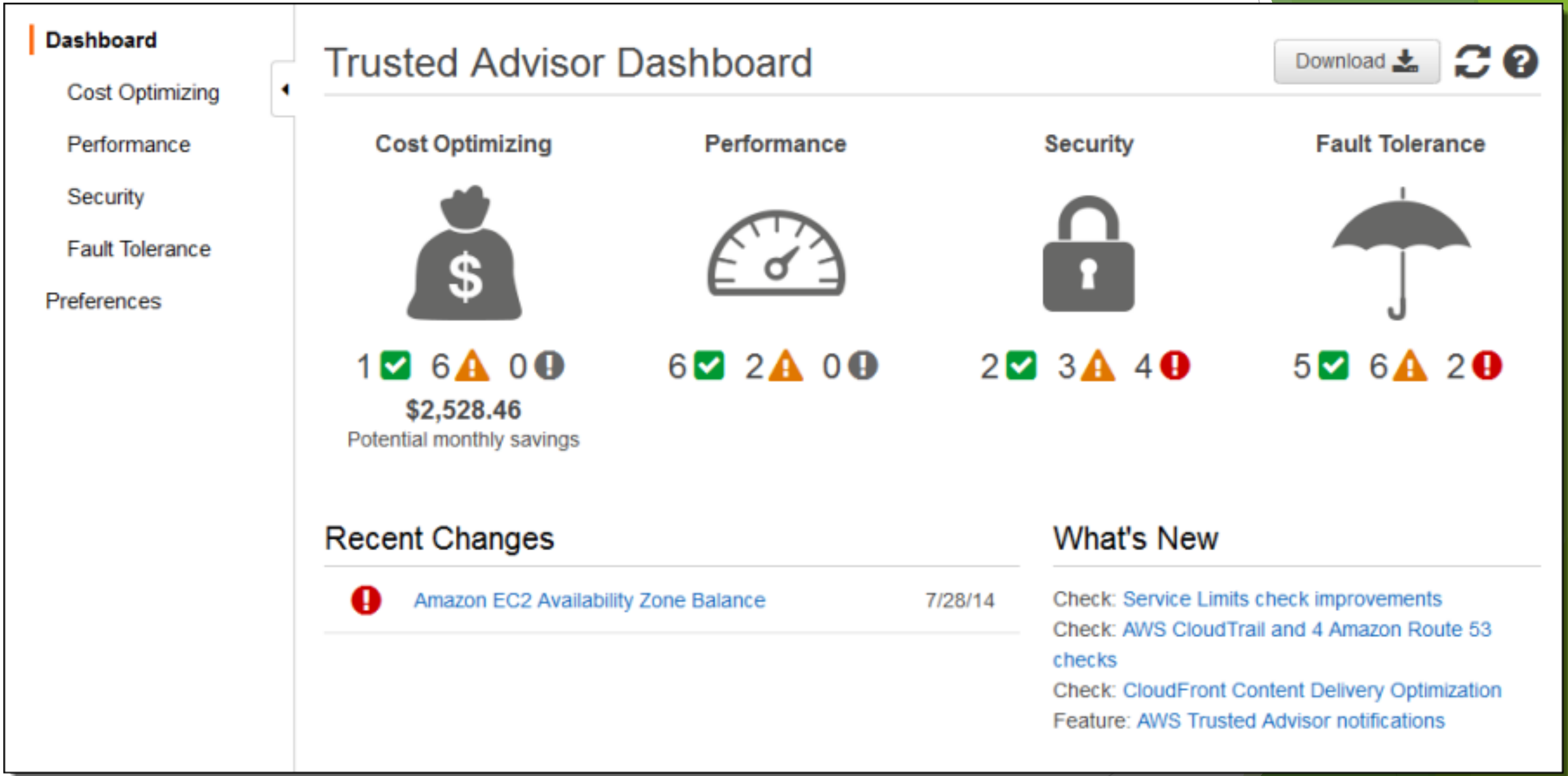
- You can receive alerts (SNS notifications) for any changes
  - Is there unrestricted SSH access to my security groups?
  - Do my buckets have any public access?

CloudWatch vs CloudTrail vs Config

- Cloud Watch
  - Performance monitoring (metrics, CPU, network, etc)
  - Events & Alerting
  - Log Aggregation & Analysis
- CloudTrail
  - Record API calls made within your account by everyone
  - Global service
  - Can define trails for specific resources
- Config
  - Record configuration changes
  - Evaluate resources against compliance rules
  - Get timeline of changes and compliance

Trusted Advisor

- No need to install anything – high level
- Aws account assessment
- Business & Enterprise support plan
- Analyze your AWS accounts and provides recommendation on 6 Categories:
  - Cost optimization
  - Performance
  - Security
  - Fault tolerance
  - Service limits
  - Operational excellence



Trusted Advisor Dashboard

Cost Optimizing	Performance	Security	Fault Tolerance
1 ✓ 6 ⚠ 0 ❗	6 ✓ 2 ⚠ 0 ❗	2 ✓ 3 ⚠ 4 ❗	5 ✓ 6 ⚠ 2 ❗
$2,528.46 Potential monthly savings			

Recent Changes

❗ Amazon EC2 Availability Zone Balance 7/28/14

What's New

Check: Service Limits check improvements

Check: AWS CloudTrail and 4 Amazon Route 53 checks

Check: CloudFront Content Delivery Optimization

Feature: AWS Trusted Advisor notifications