AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

COP313

Inside Amazon operations: Operations automated at scale

Eric Westfall (he/him)
Principal Enterprise Architect
Amazon Web Services

Glen Miglin (he/him)
Software Development Manager
Amazon

Agenda

Intro to AWS Systems Manager service

Intro to Host Agent Installation Manager

How Amazon leverages Systems Manager

- Scalability
- Security

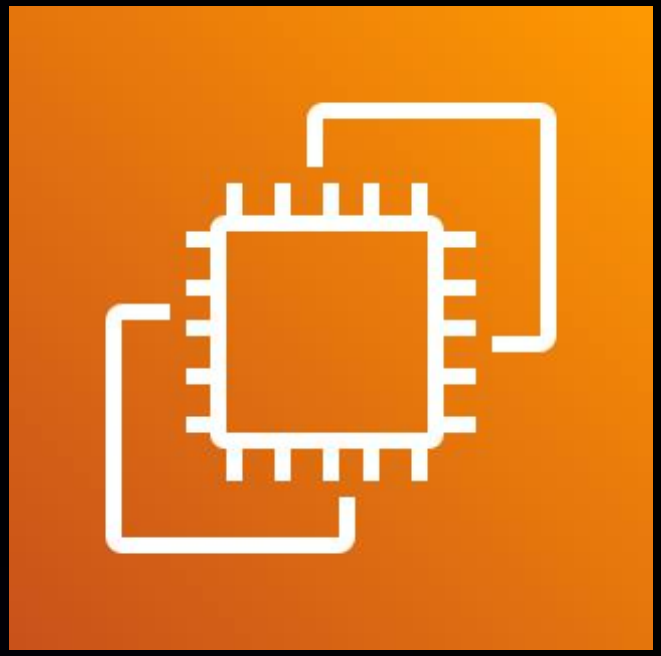
Current operating scale

Q&A

Growth opportunity

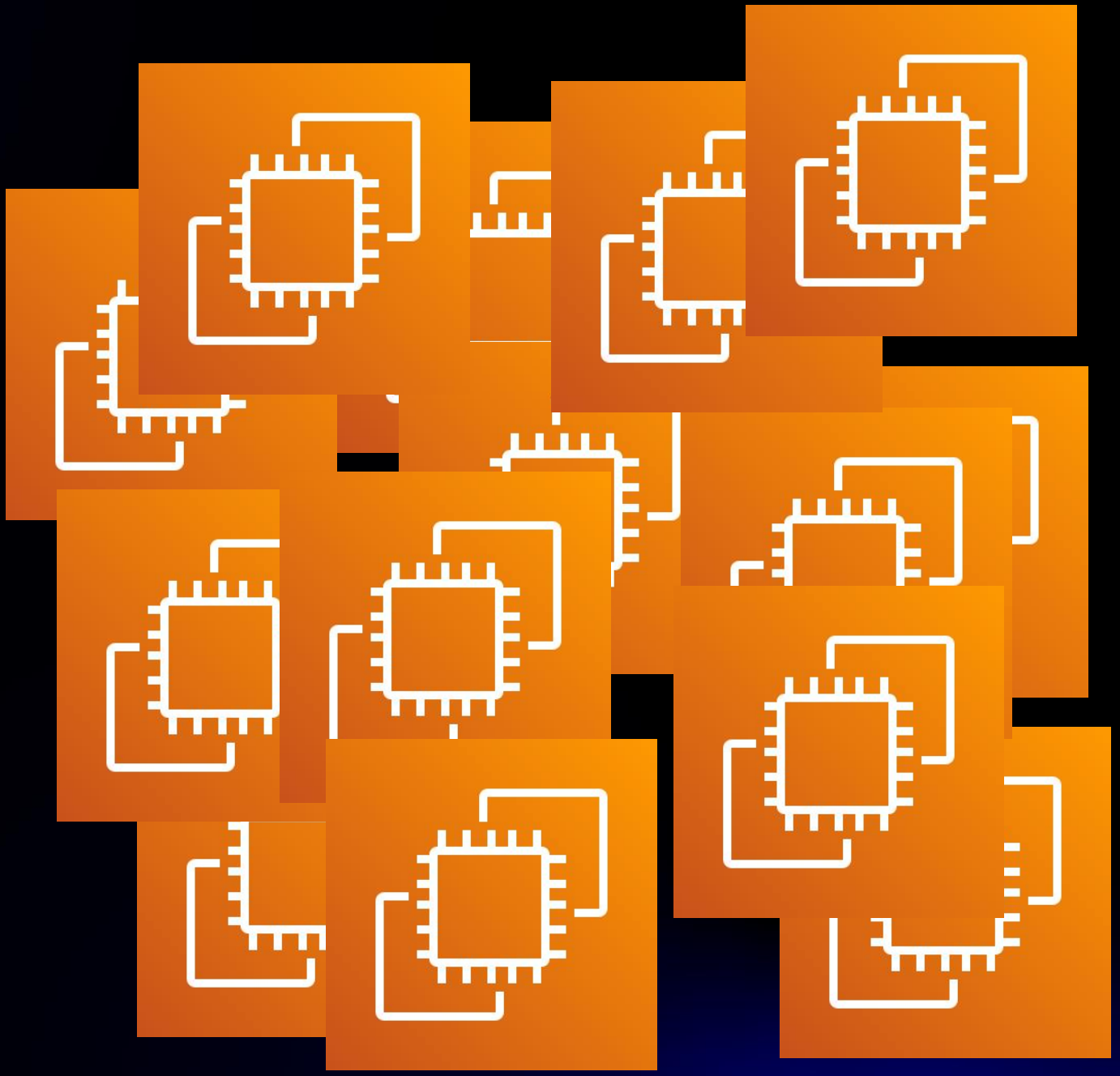
Growth opportunity

information security
amazon



Growth opportunity

information security
amazon



Growth opportunity

- Unable to reliably deploy security agents on internal hosts
- Campaigns were attempted but did yielded the desired results
  - Emails
  - Tickets
  - Default configuration

Introduction to AWS Systems Manager

AWS Systems Manager

Shorten the time to detect problems

Automate tasks to increase efficiency

Improve visibility and control

Manage hybrid environments

Maintain security and compliance

aws

AWS Systems Manager features

Operations management


OpsCenter


Explorer

Application management


AWS Resource Groups


AWS AppConfig


Parameter Store

Action and change


Automation


Maintenance Windows


Change Calendar

Instances and nodes


Inventory


Run Command


Patch Manager


Distributor


State Manager

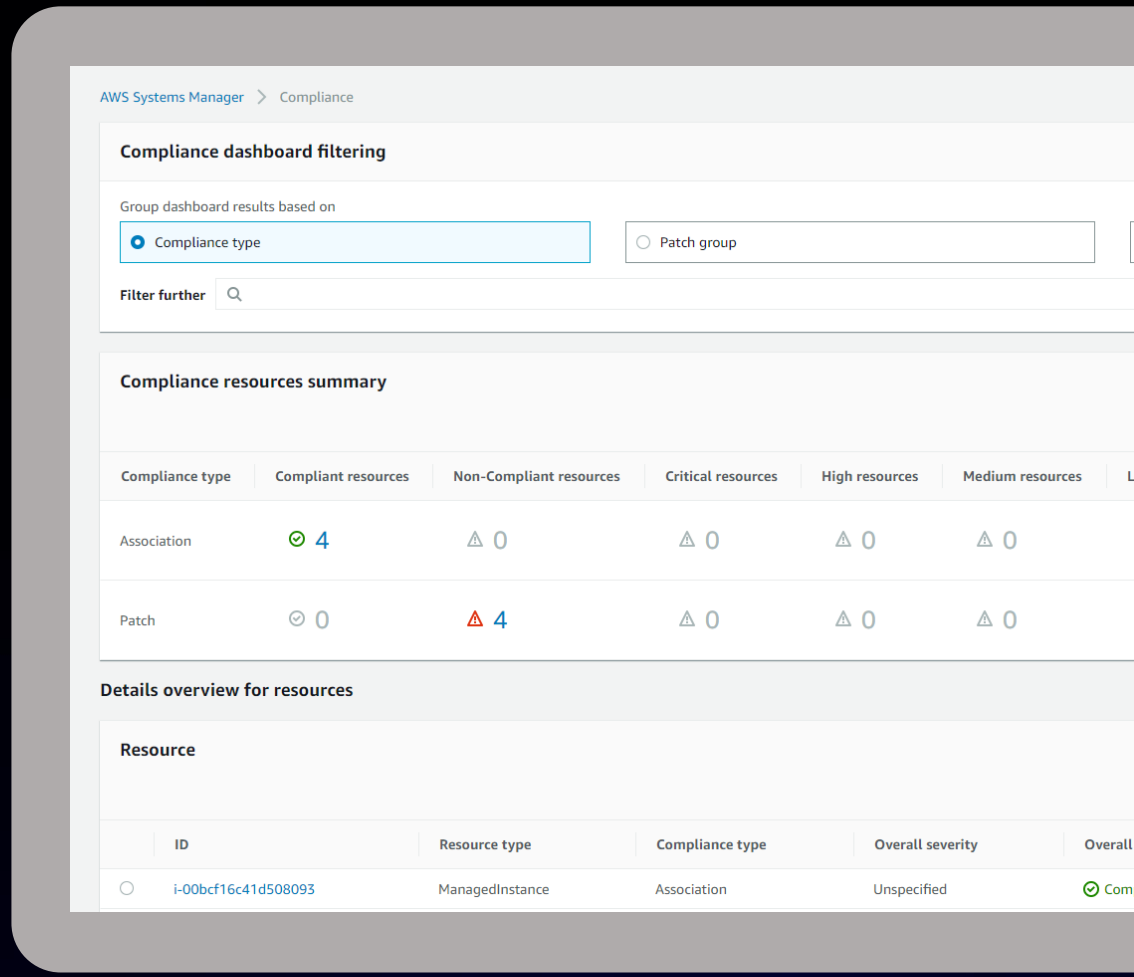

Session Manager

State Manager

SECURE AND SCALABLE CONFIGURATION MANAGEMENT

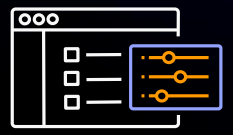
- Simplifies the process of keeping your Amazon EC2 and hybrid infrastructure in the desired state that you define
- Provides flexibility by enabling Chef recipes, PowerShell modules, or Ansible playbooks for configuration management
- Fixes configuration drift by periodically checking and remediating changes
- Bootstraps instances with in-guest configuration at startup

  Example: use State Manager with AWS CloudFormation to install software on instances upon provisioning

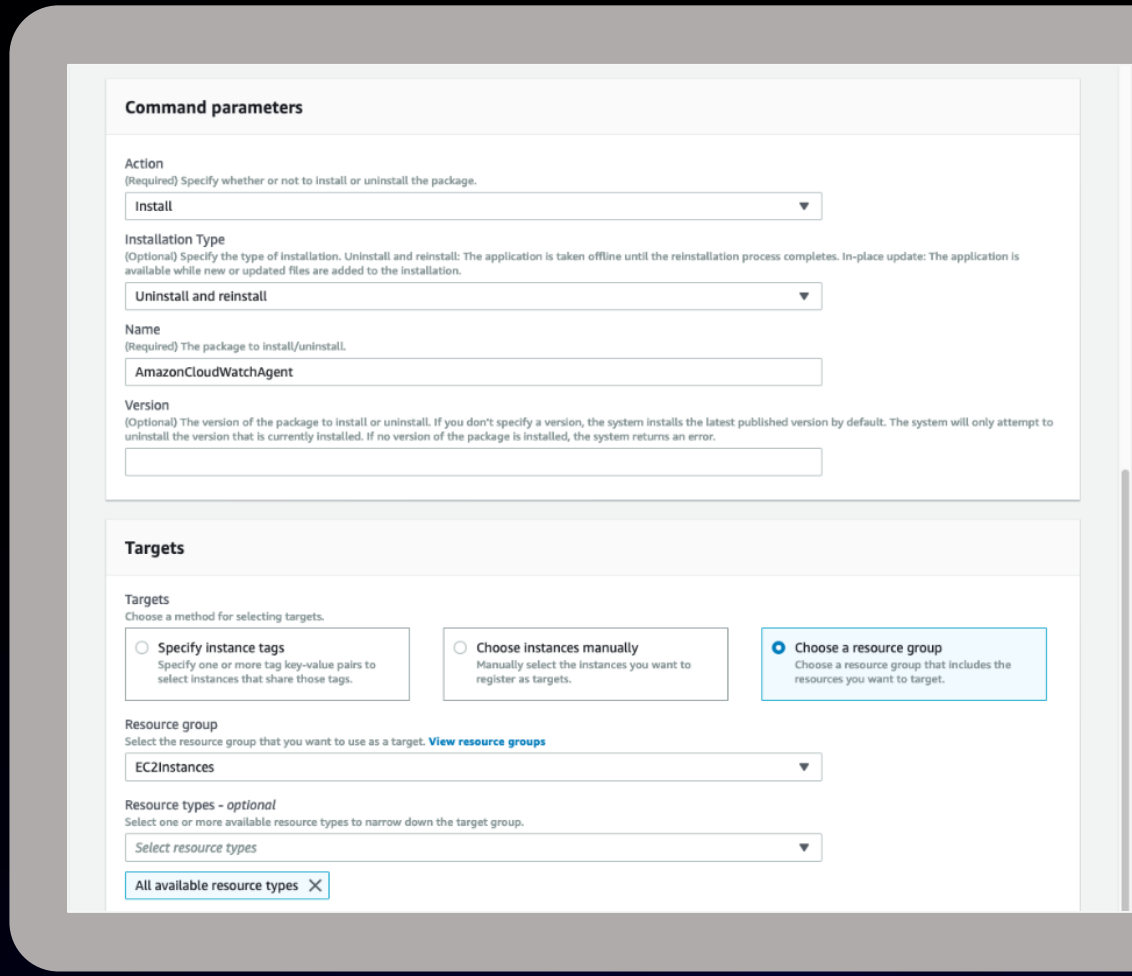


Run Command

SAFE AND SECURE REMOTE ADMINISTRATION OF YOUR COMPUTE NODES AT SCALE

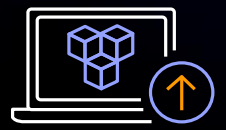


- Execute controlled actions across any or all selected nodes in your fleet
- Install or bootstrap applications
- Track inventory and capture log files
- Apply software updates and edit system settings
- Enable custom uses such as predefined failure injections for chaos testing
- Control access via AWS Identity and Access Management (IAM), and record command activity for troubleshooting and auditability
- All without the need for bastion hosts, open inbound ports, or SSH key management

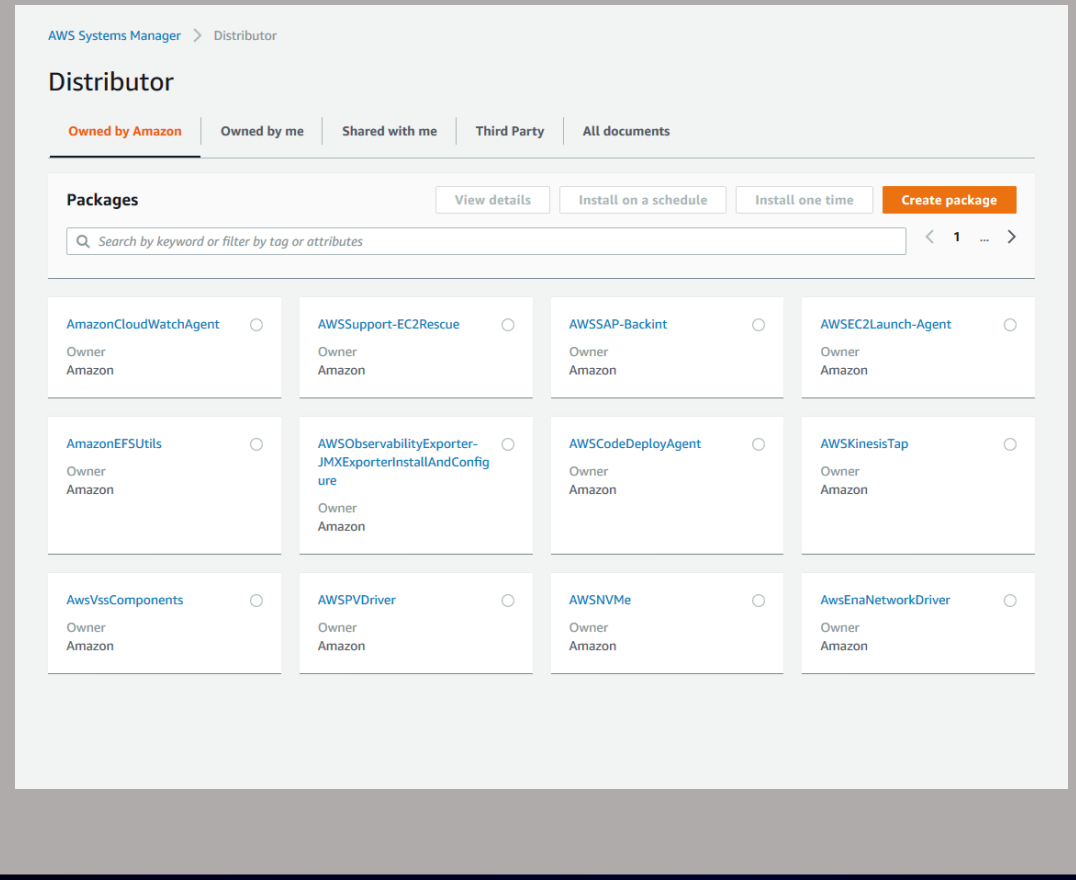


Distributor

SECURELY DISTRIBUTE AND INSTALL SOFTWARE PACKAGES



- Create new or deploy existing software packages, including AWS-published and third-party packages, to multiple managed instances at one time
- Simplifies installing packages via Run Command and State Manager
- Deploy to multiple platforms and architectures with a single package
- Control deployment across groups of instances
- Centralize packages in a single AWS account and share across your AWS Organizations



Introduction to the Host Agent Installation Manager

Growth opportunity

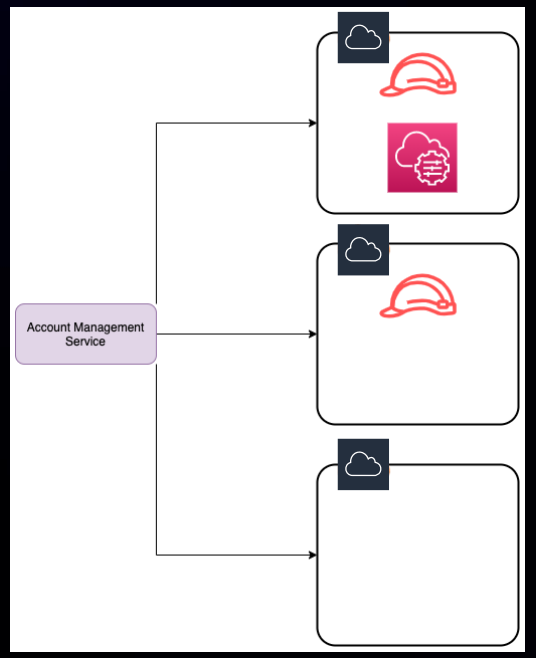
Solution: Host Agent Installation Manager

Solution requirements

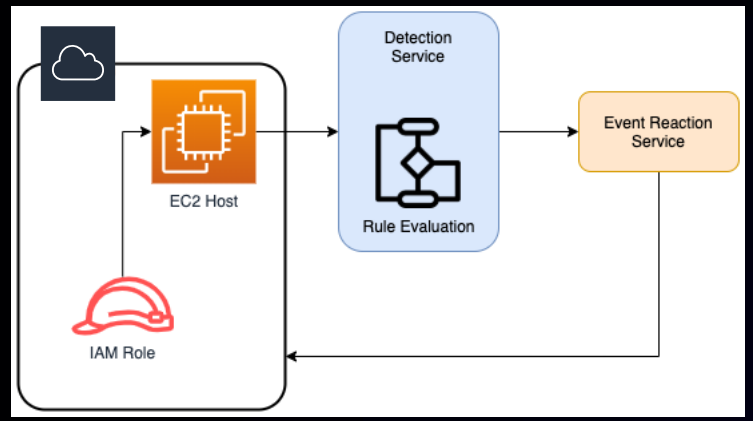
- Scalable
- Safe
- Reactive
- Communicative

High-level architecture

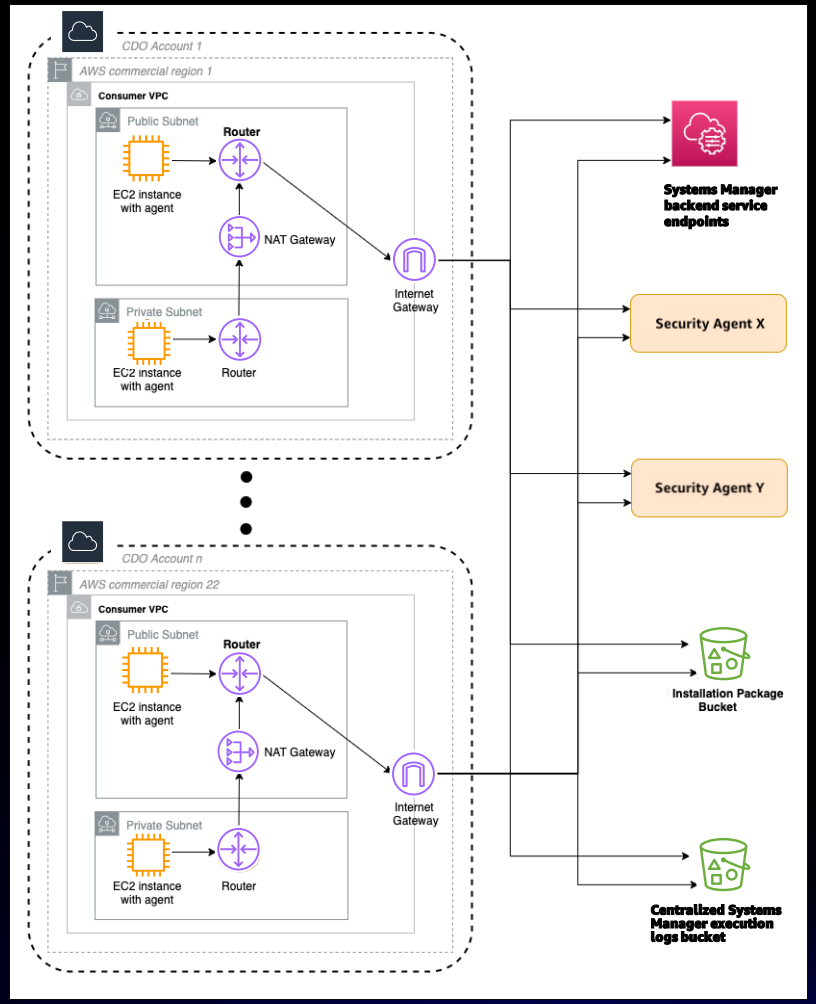
Resource creation



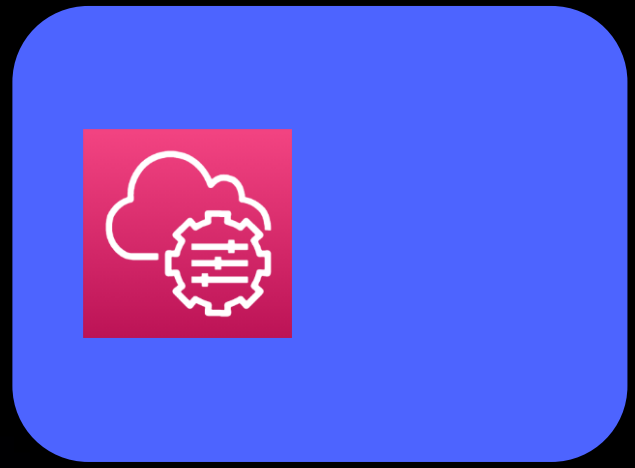
Event reaction

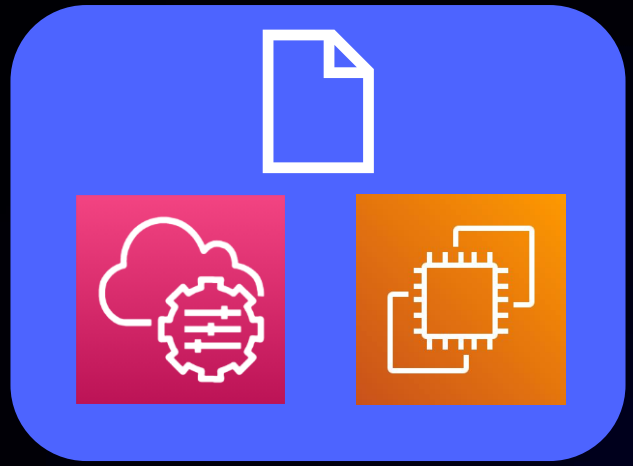


Agent installation



High-level architecture





High-level architecture

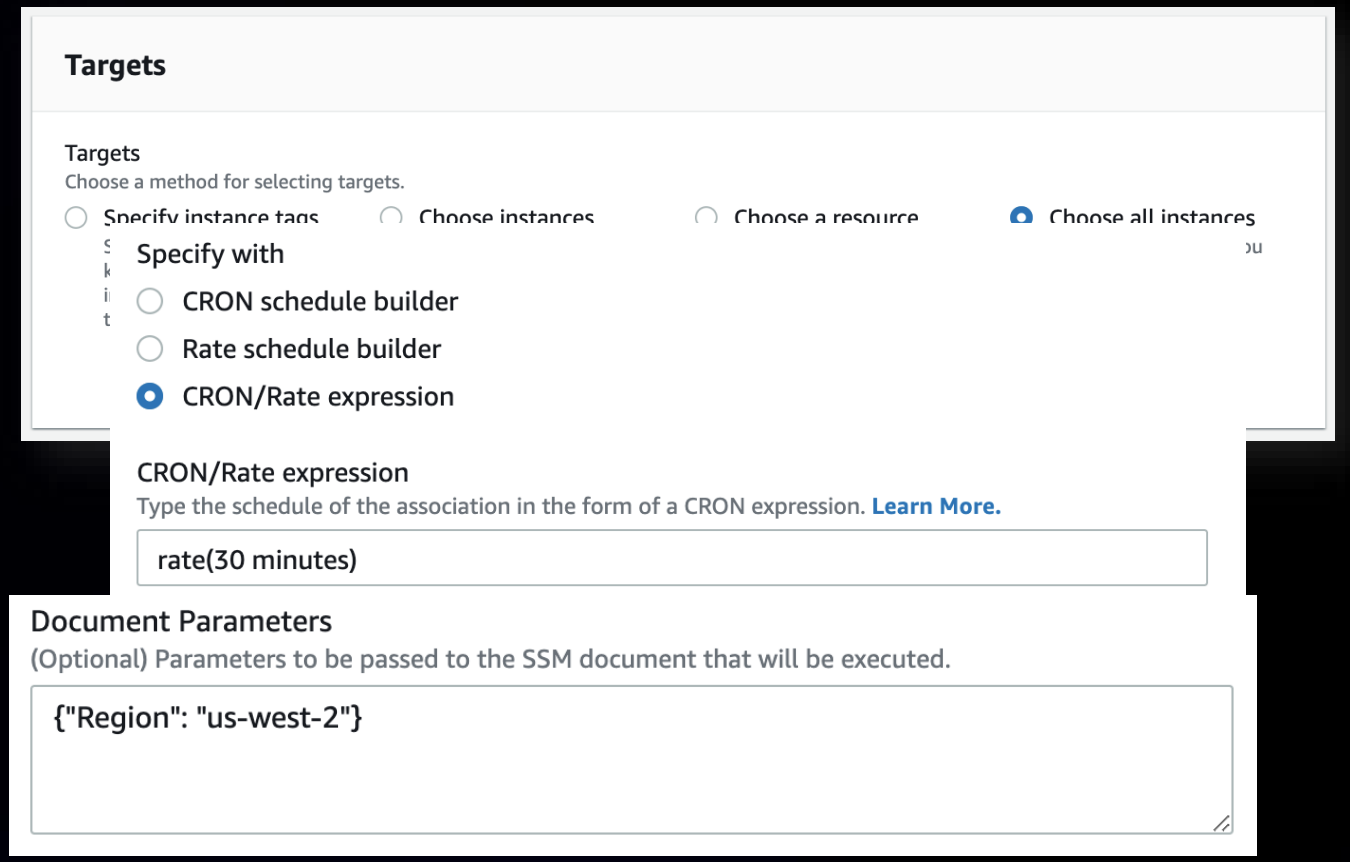
getAgentConfig

installAgentPackage

isAgentHealthy

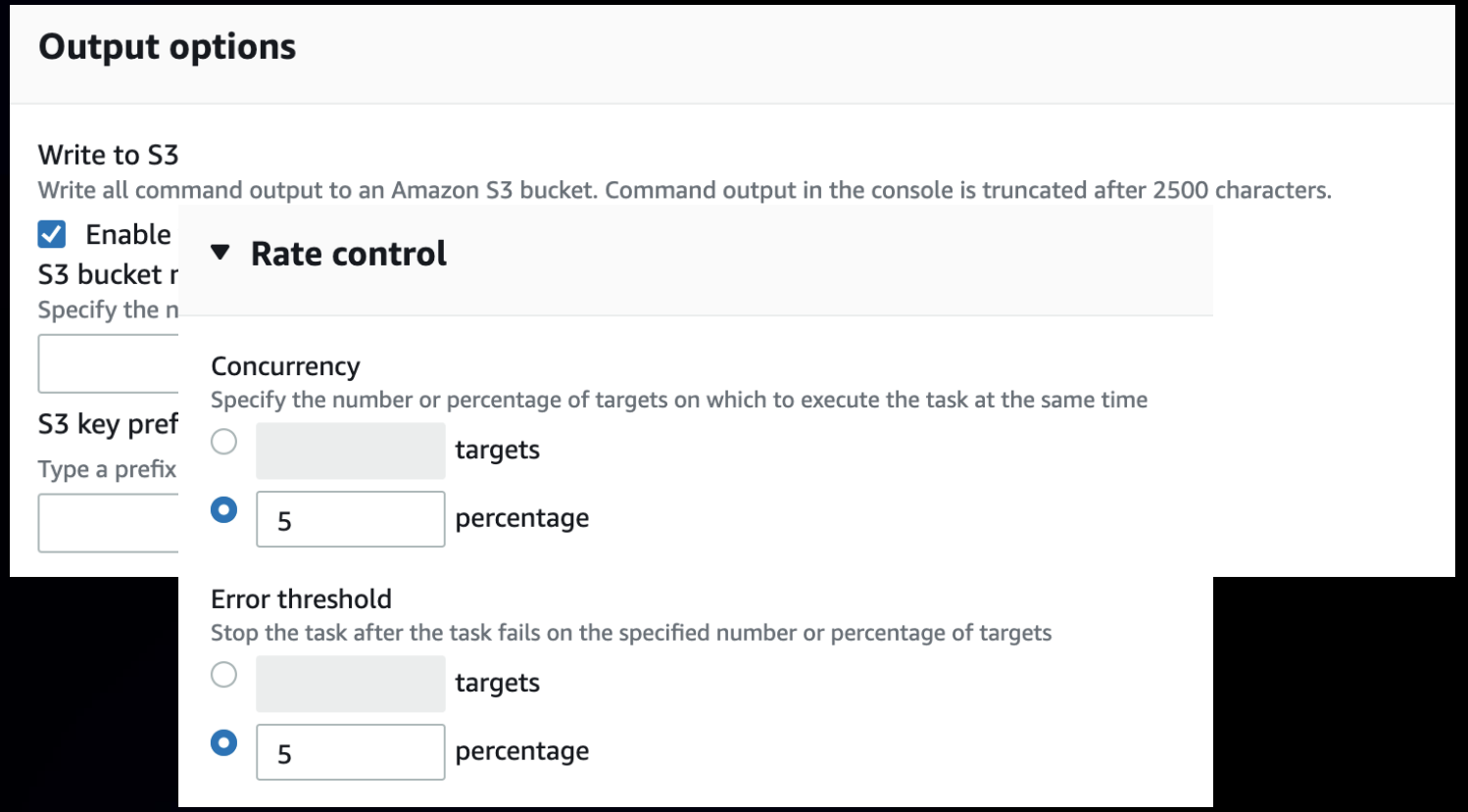
Key Systems Manager features utilized

- Star (*) instances
- Reactive and scheduled run
- Intake parameters



Key Systems Manager features utilized

- Logging to Amazon S3
- Max error limit
- Max concurrency



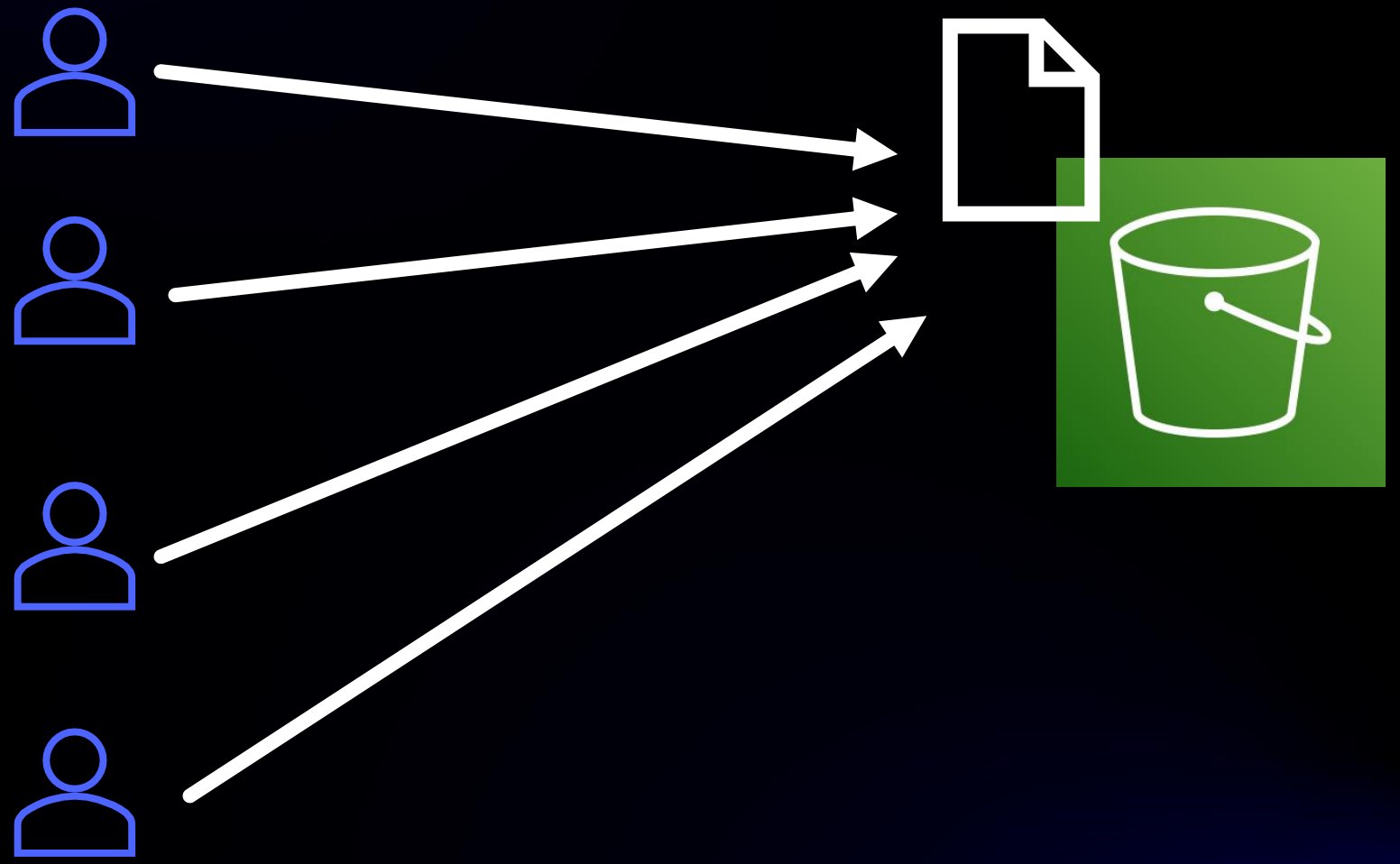
Additional effort required

- Creating Systems Manager associations
- Creating IAM resources
- Hooking up permissions
- Maintaining created resources

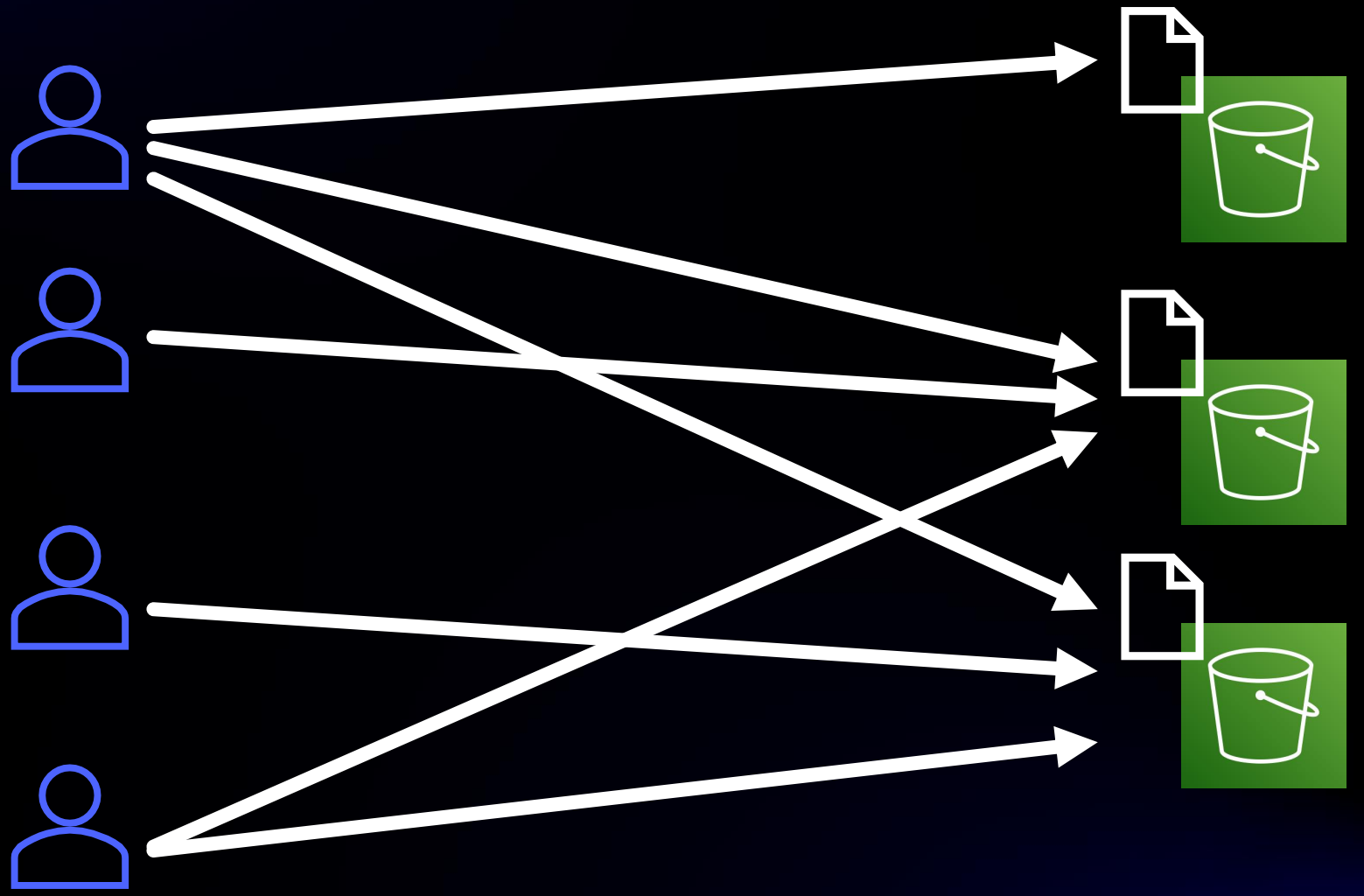
Other options considered

- Internal tools
  - Not intended for this scale
  - Required granting broad permissions
- AWS Systems Manager Distributor
  - Well suited to our use case
  - We would have had to make security agent package public

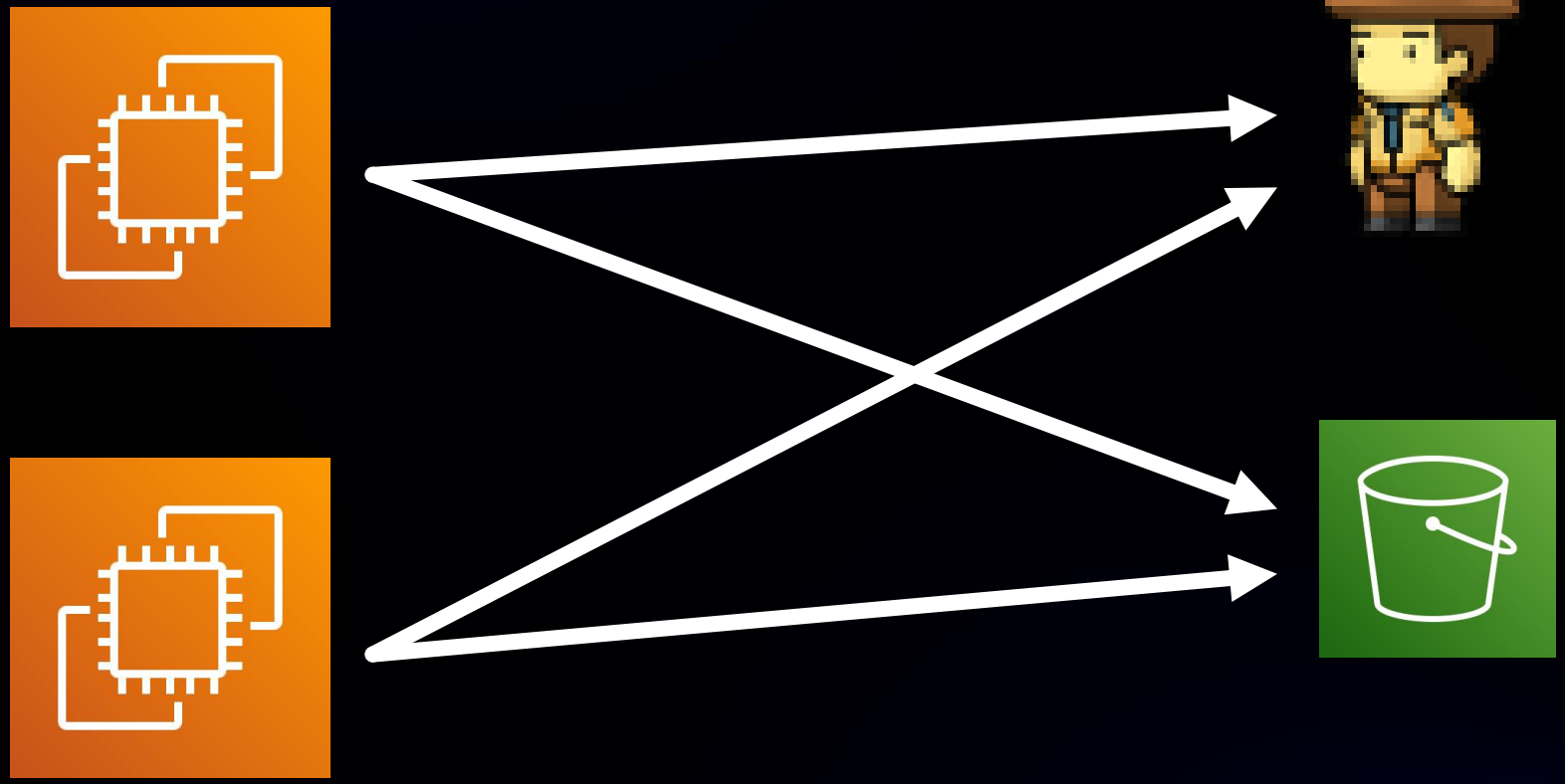
Scalability



Scalability



Scalability

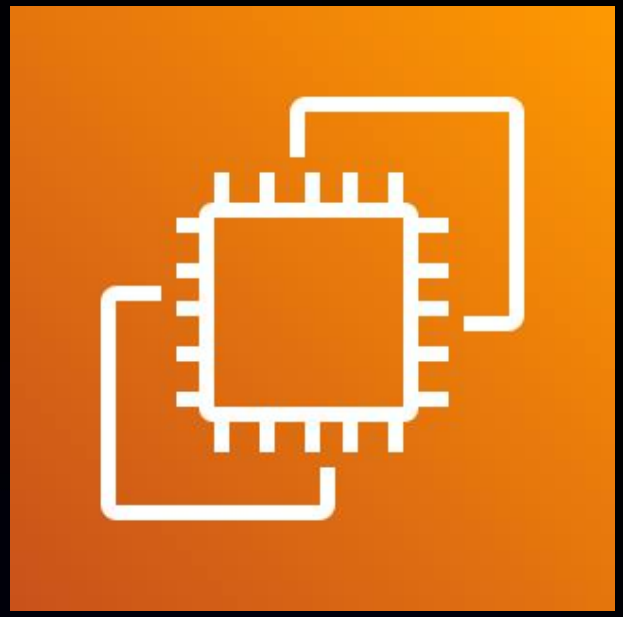


Security considerations

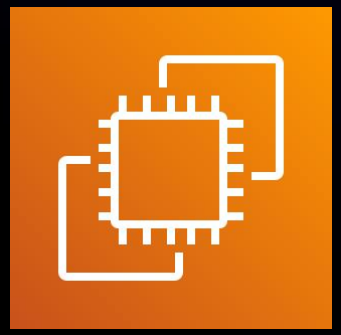
- Encryption at rest and in transit
- Auditing and alarming
- Amazon S3 versioning
- Digital signature verifications
- Least permissions
- Safety switch

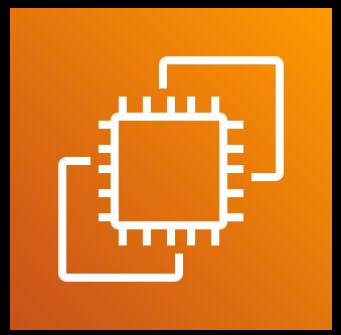
User experience

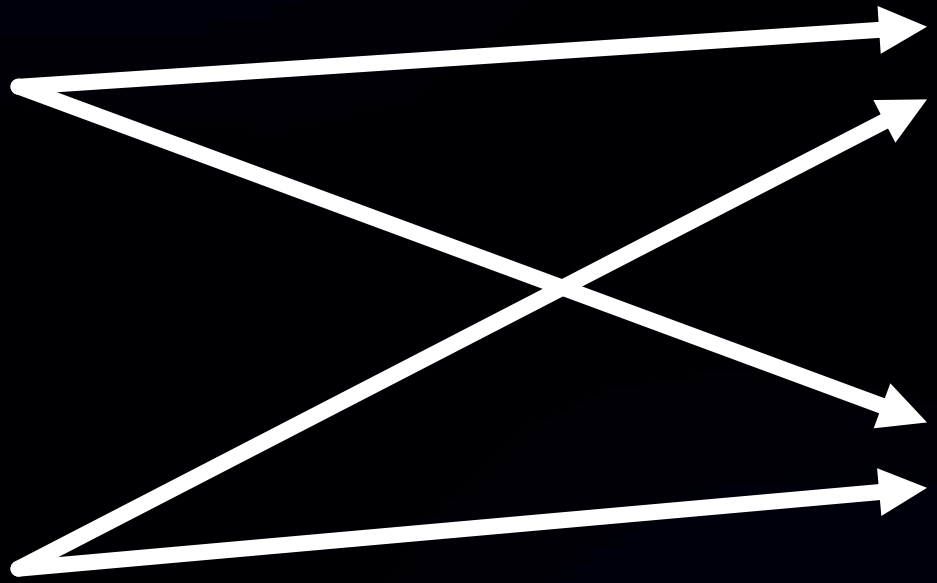
information security
amazon



Grouping



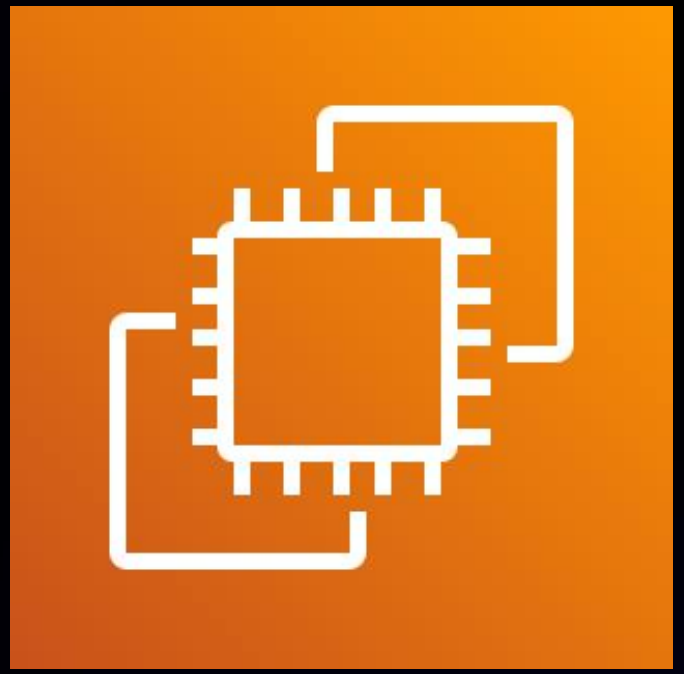




Current state

- Installed on hundreds of thousands of accounts
- Millions of Amazon EC2 instances scanned daily
- Security agent compliance target hit

What's remaining?



Thank you!

Eric Westfall
erwestfa@amazon.com

Glen Miglin
glenmigl@amazon.com