

The background features a dark blue gradient with abstract geometric shapes. On the left, a large triangle is formed by a vertical orange line and a diagonal orange line. On the right, a large curved shape in shades of blue and orange sweeps across the frame. The text is positioned in the upper right area.

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

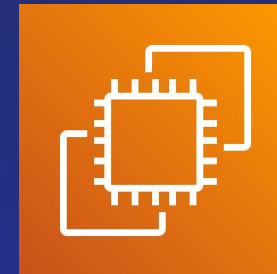
- Scalability
- Security

Current operating scale

Q&A

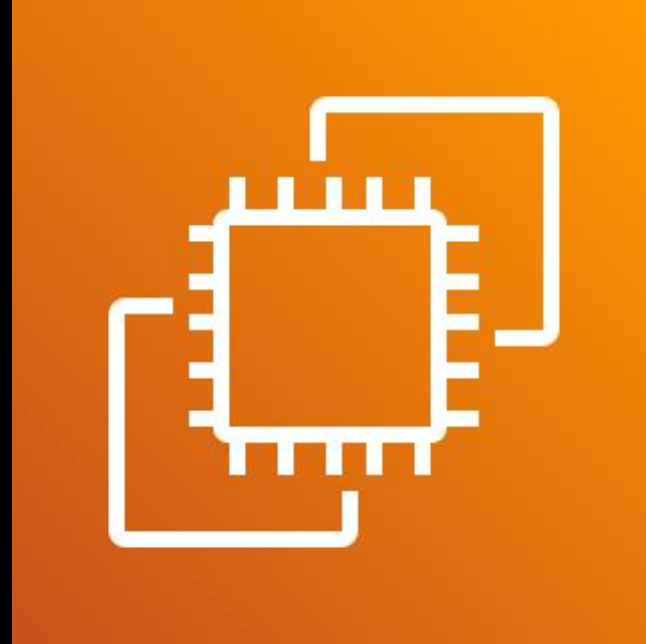


Growth opportunity

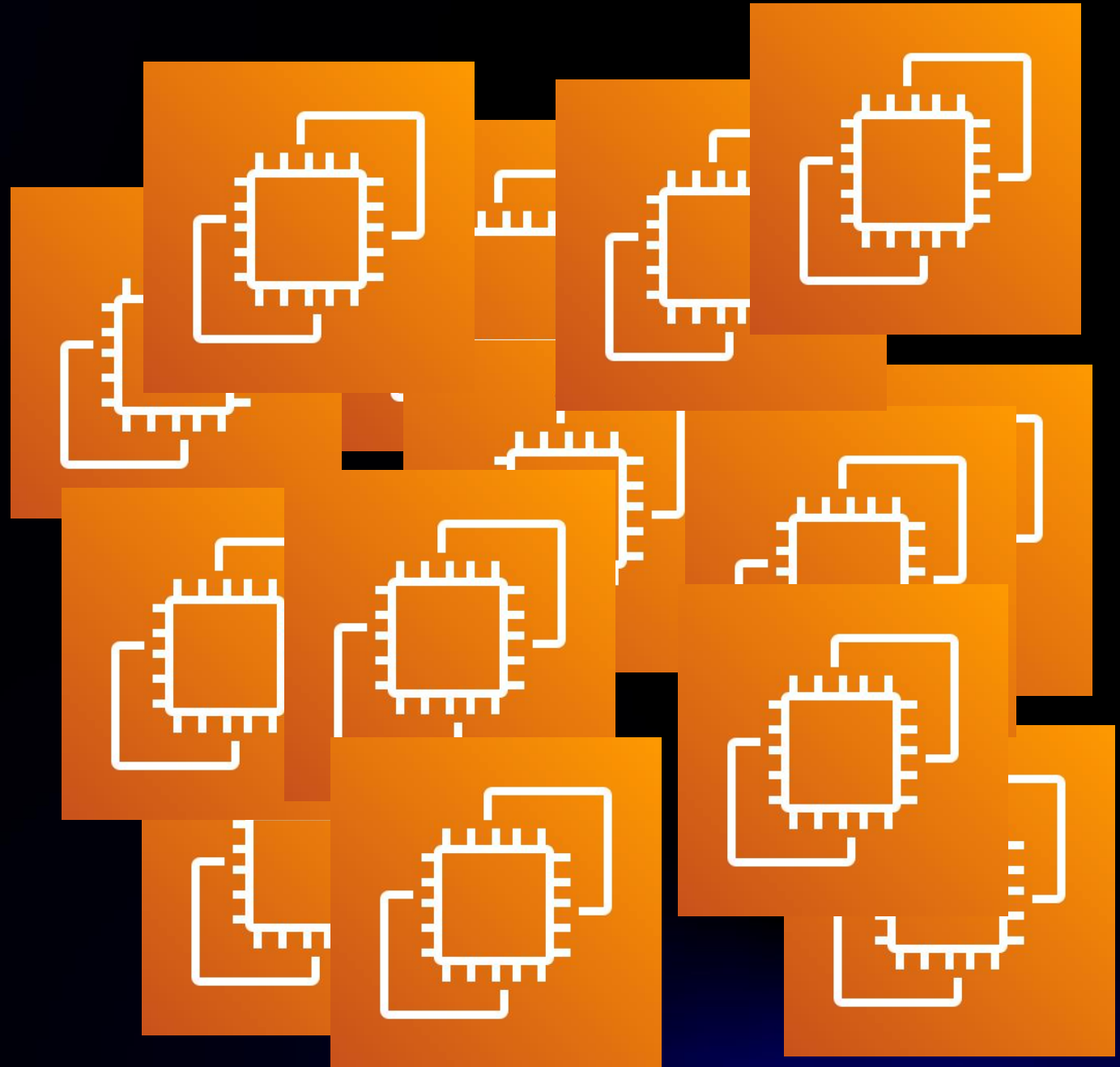


?

Growth opportunity



Growth opportunity



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 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

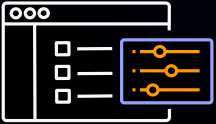
The screenshot displays the AWS Systems Manager Compliance dashboard. At the top, it shows the breadcrumb 'AWS Systems Manager > Compliance'. Below this is the 'Compliance dashboard filtering' section, which includes a dropdown menu set to 'Compliance type' and a search bar labeled 'Filter further'. The main section is 'Compliance resources summary', which contains a table with columns for 'Compliance type', 'Compliant resources', 'Non-Compliant resources', 'Critical resources', 'High resources', and 'Medium resources'. The table shows two rows: 'Association' with 4 compliant and 0 non-compliant resources, and 'Patch' with 0 compliant and 4 non-compliant resources. Below the summary table is the 'Details overview for resources' section, which includes a table with columns for 'ID', 'Resource type', 'Compliance type', 'Overall severity', and 'Overall status'. The table shows one resource with ID 'i-00bcf16c41d508093', resource type 'ManagedInstance', compliance type 'Association', overall severity 'Unspecified', and overall status 'Compliant'.

Compliance type	Compliant resources	Non-Compliant resources	Critical resources	High resources	Medium resources
Association	4	0	0	0	0
Patch	0	4	0	0	0

ID	Resource type	Compliance type	Overall severity	Overall status
i-00bcf16c41d508093	ManagedInstance	Association	Unspecified	Compliant

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



Command parameters

Action
(Required) Specify whether or not to install or uninstall the package.

Install ▼

Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.

Uninstall and reinstall ▼

Name
(Required) The package to install/uninstall.

AmazonCloudWatchAgent

Version
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

Targets

Targets
Choose a method for selecting targets.

☐ Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

☐ Choose instances manually
Manually select the instances you want to register as targets.

☒ Choose a resource group
Choose a resource group that includes the resources you want to target.

Resource group
Select the resource group that you want to use as a target. [View resource groups](#)

EC2Instances ▼

Resource types - optional
Select one or more available resource types to narrow down the target group.

Select resource types ▼

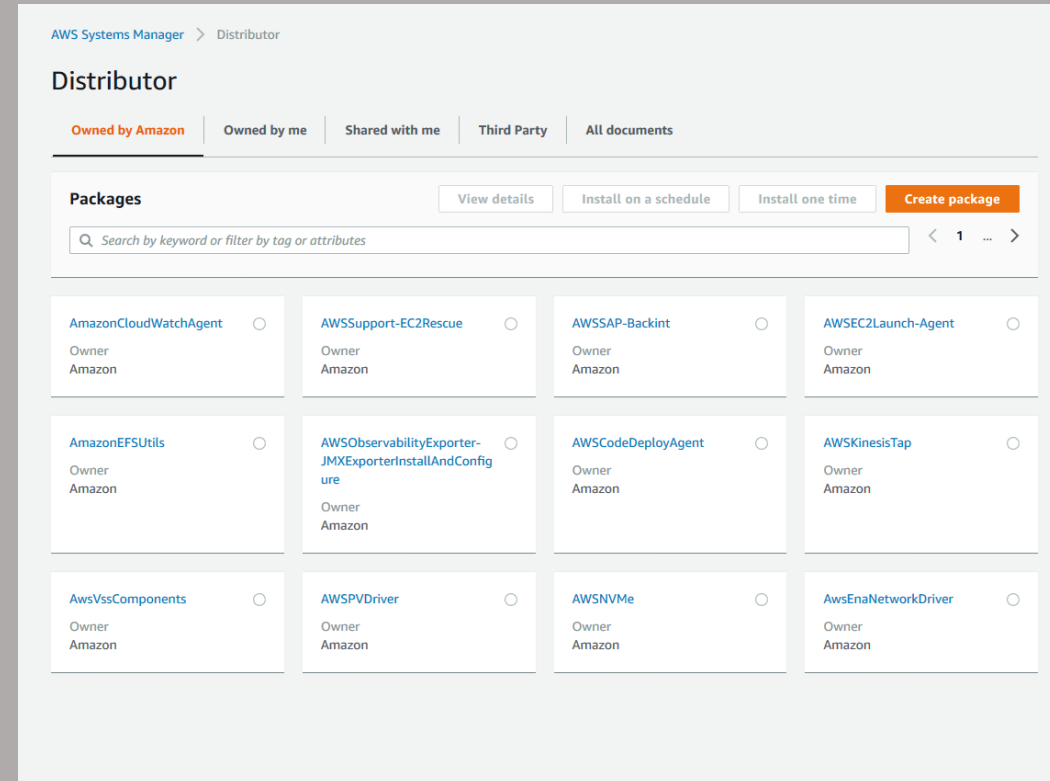
All available resource types X

Distributor

SECURELY DISTRIBUTE AND INSTALL SOFTWARE PACKAGES

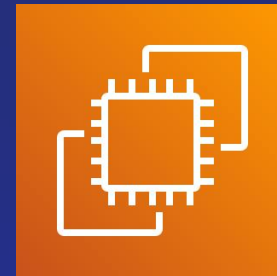
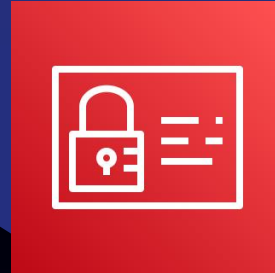


- ➔ Create new or deploy existing software packages, including AWS-published and third-party packages, to multiple managed instances at one time
- ➔ Simplifies installing packages via Run Command and State Manager
- ➔ Deploy to multiple platforms and architectures with a single package
- ➔ Control deployment 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



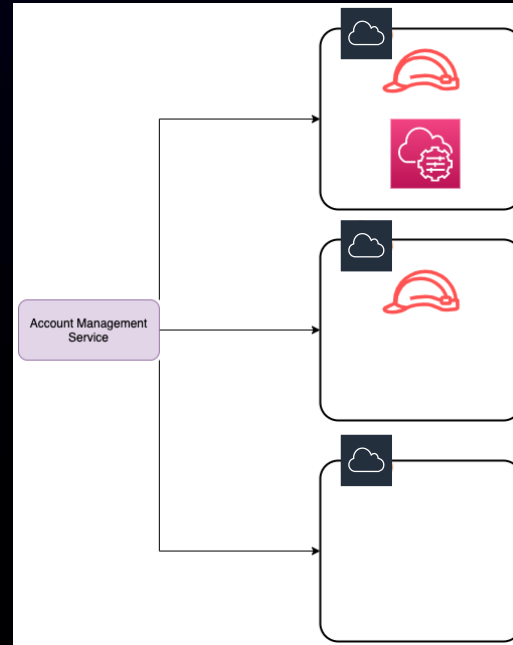
Solution requirements

- Scalable
- Safe
- Reactive
- Communicative

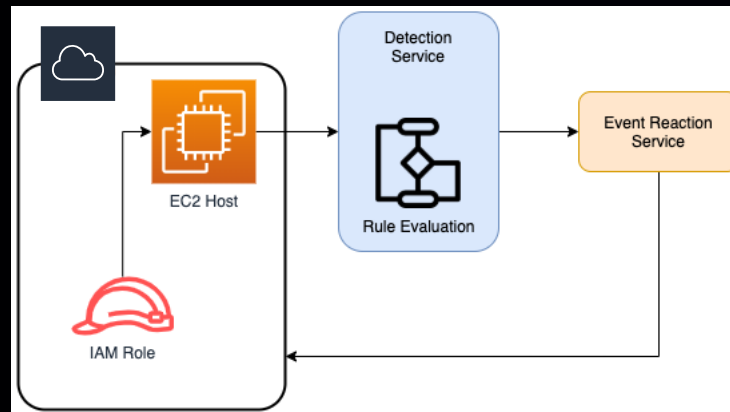
High-level architecture



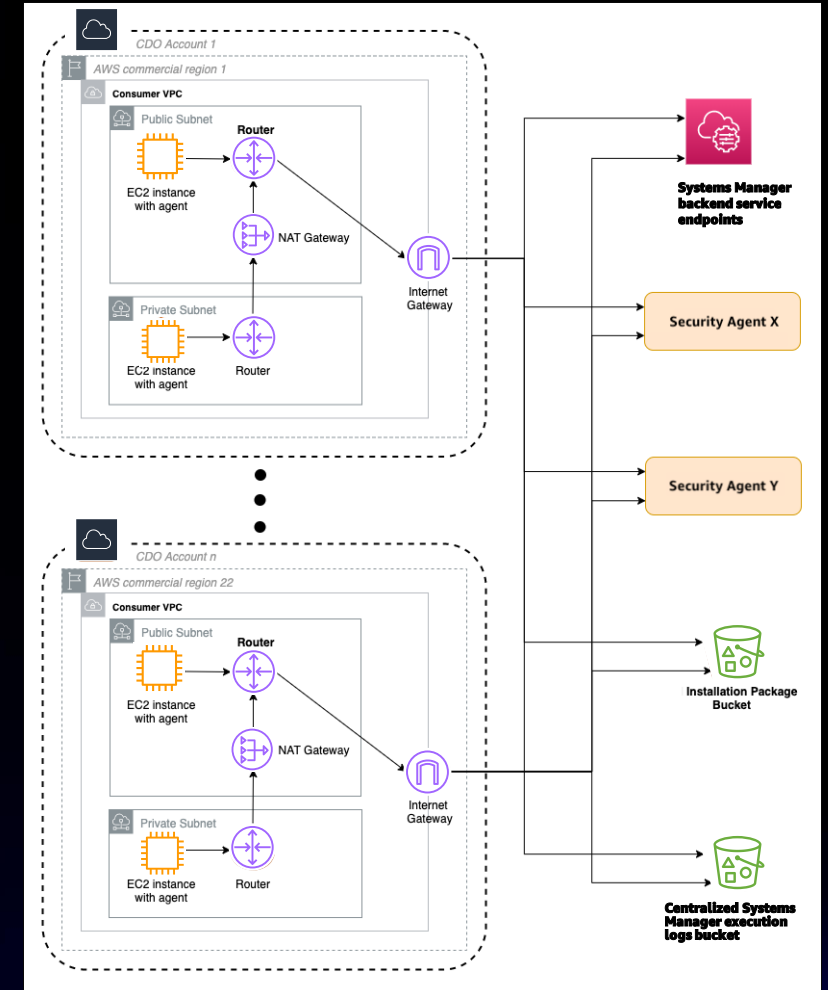
Resource creation



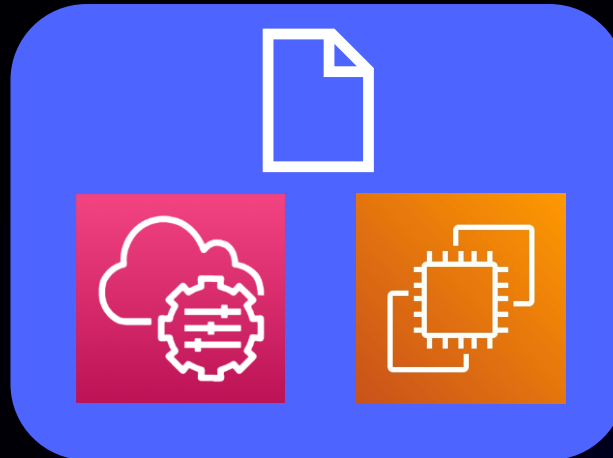
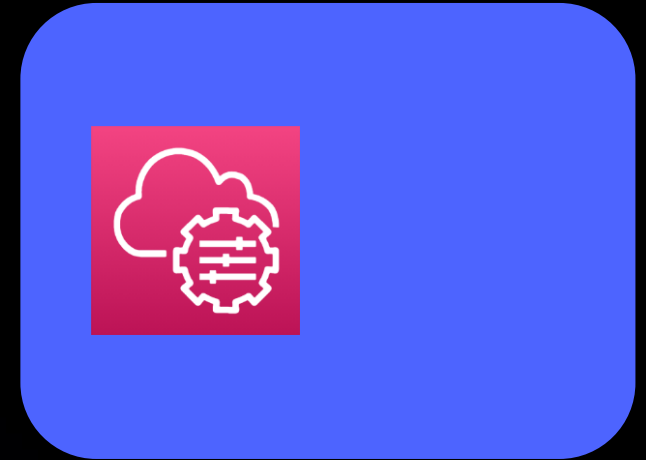
Event reaction



Agent installation



High-level architecture



High-level architecture



getAgentConfig

installAgentPackage

isAgentHealthy

Key Systems Manager features utilized



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

Targets

Targets

Choose a method for selecting targets.

☐ Specify instance tags ☐ Choose instances ☐ Choose a resource ☒ Choose all instances

Specify with

☐ CRON schedule builder

☐ Rate schedule builder

☒ CRON/Rate expression

CRON/Rate expression

Type the schedule of the association in the form of a CRON expression. [Learn More.](#)

rate(30 minutes)

Document Parameters

(Optional) Parameters to be passed to the SSM document that will be executed.

{"Region": "us-west-2"}

Key Systems Manager features utilized



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

Output options

Write to S3
Write all command output to an Amazon S3 bucket. Command output in the console is truncated after 2500 characters.

☒ **Enable**
S3 bucket r
Specify the n

S3 key pref
Type a prefix

▼ **Rate control**

Concurrency
Specify the number or percentage of targets on which to execute the task at the same time

☐ targets

☒ percentage

Error threshold
Stop the task after the task fails on the specified number or percentage of targets

☐ targets

☒ percentage

Additional effort required



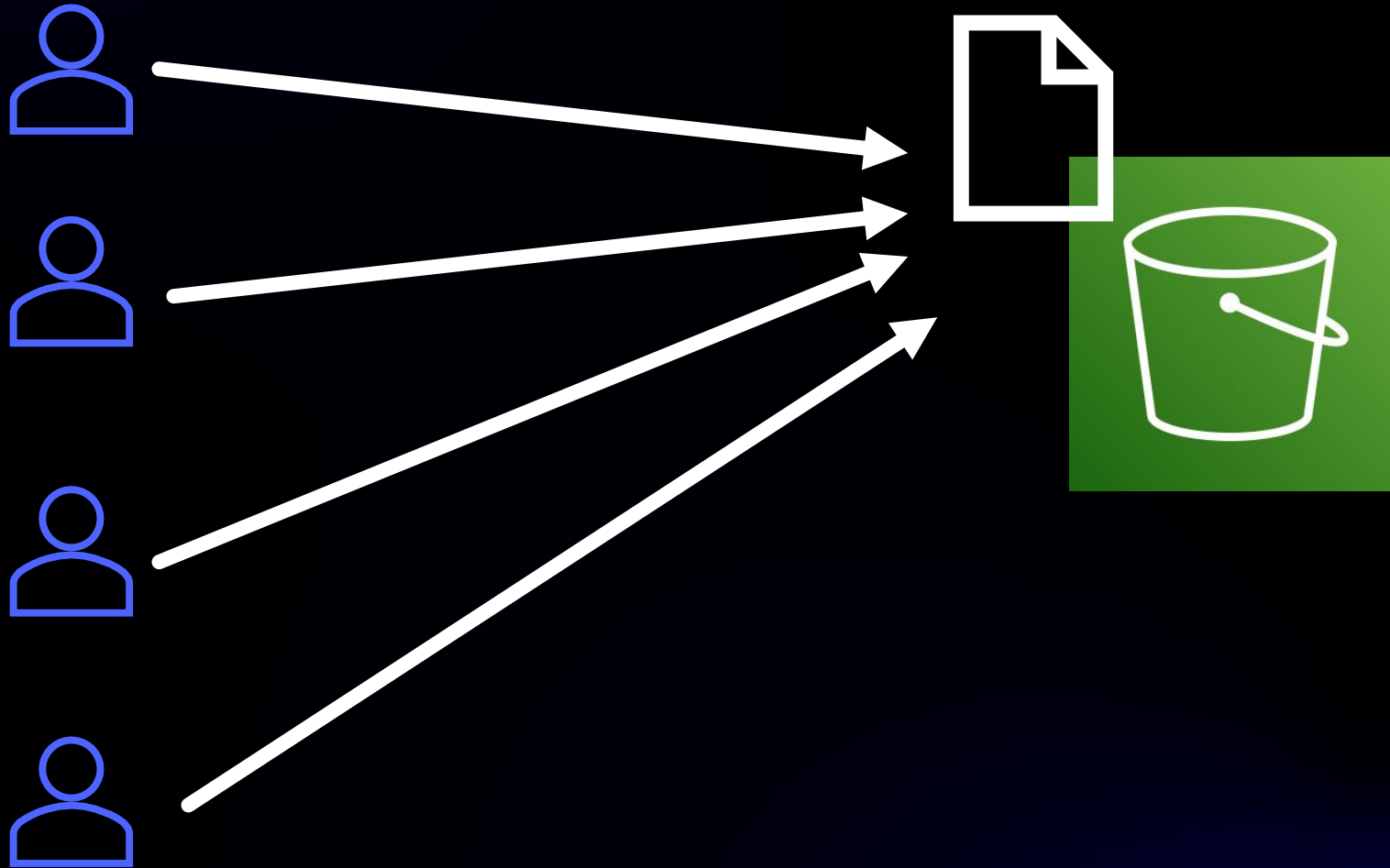
- Creating Systems Manager associations
- Creating IAM resources
- Hooking up permissions
- Maintaining created resources

Other options considered

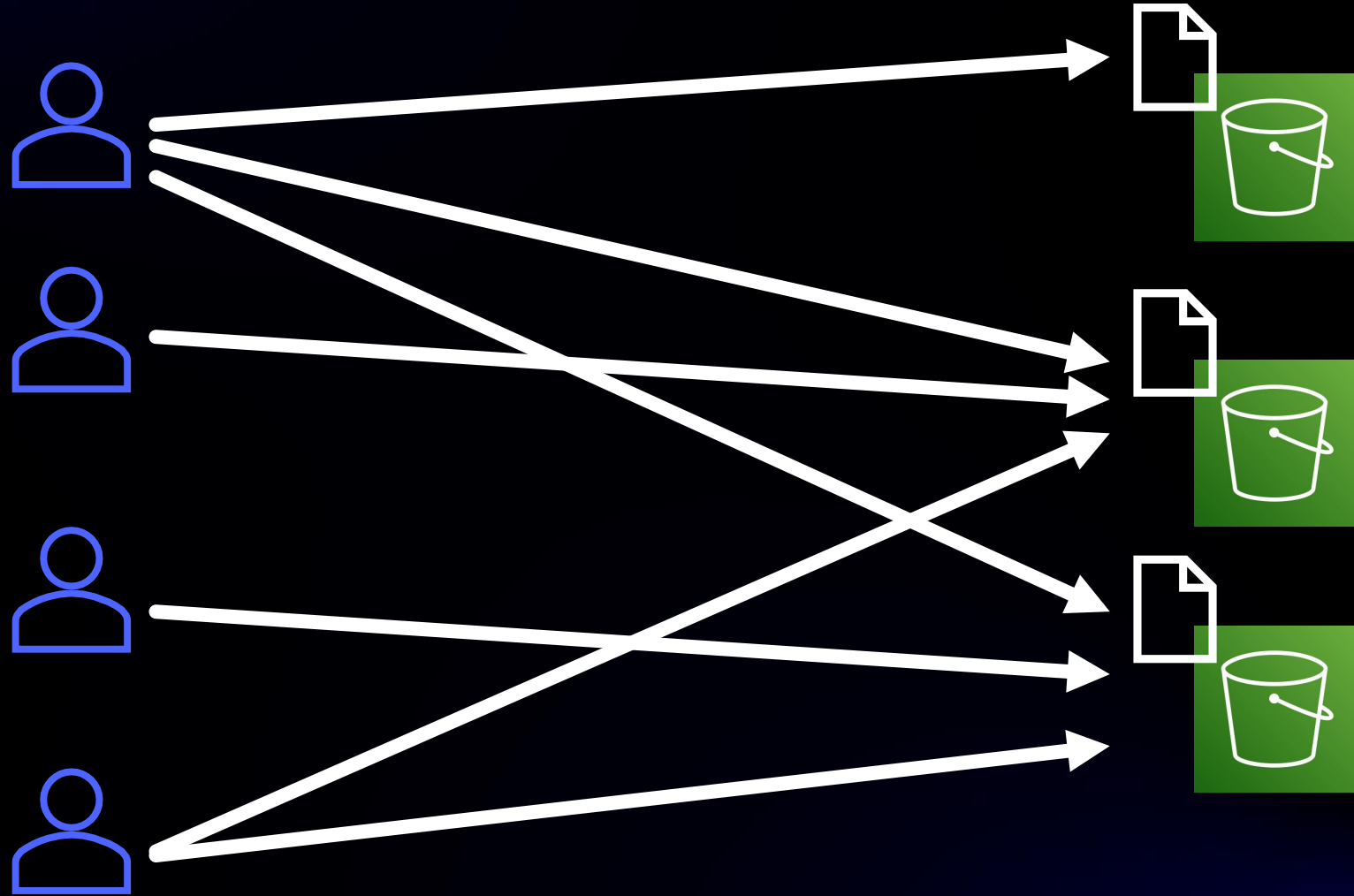


- Internal tools
 - Not intended for this scale
 - Required granting broad permissions
- AWS Systems Manager Distributor
 - Well suited to our use case
 - We would have had to make security agent package public

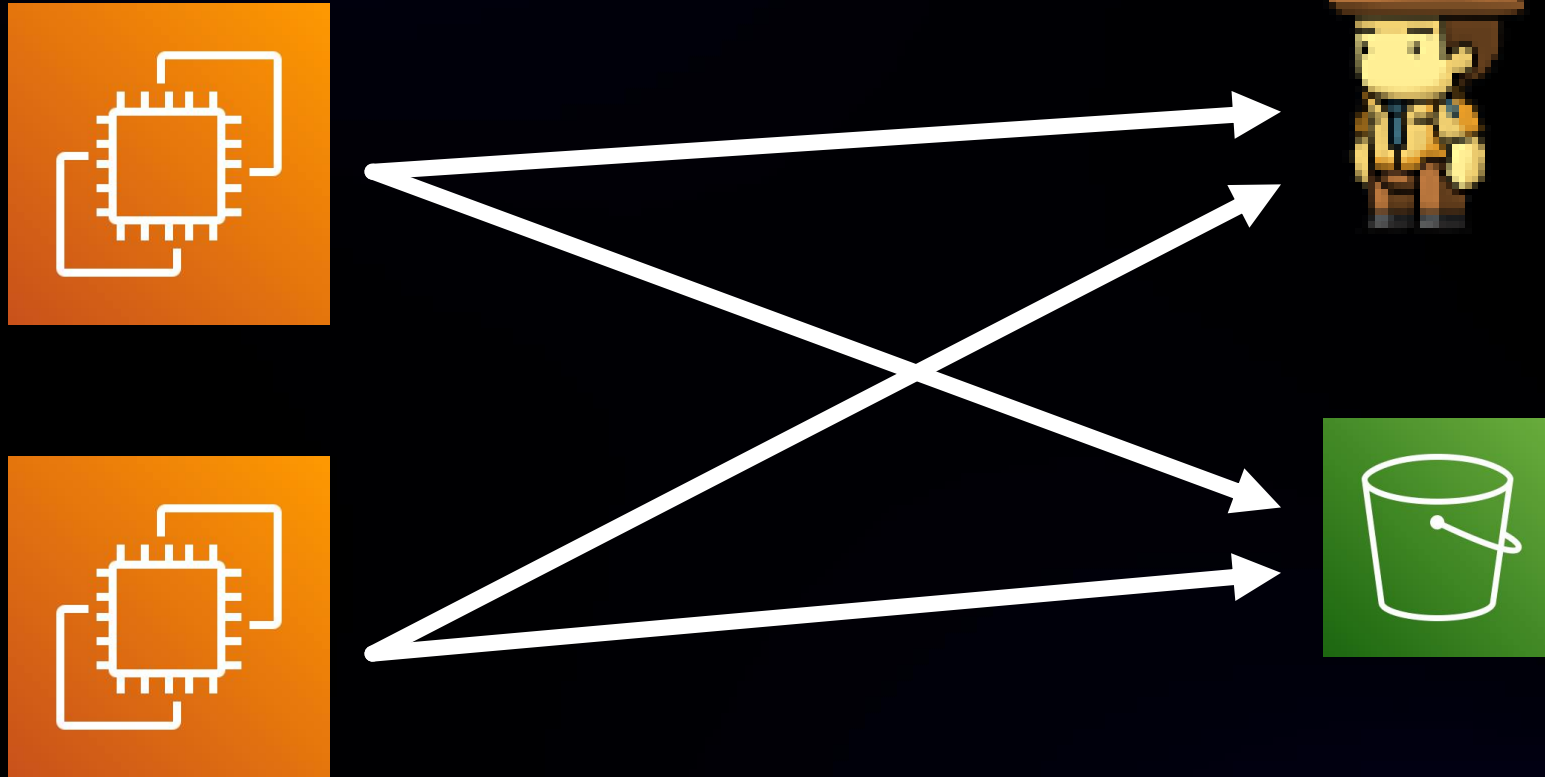
Scalability



Scalability



Scalability

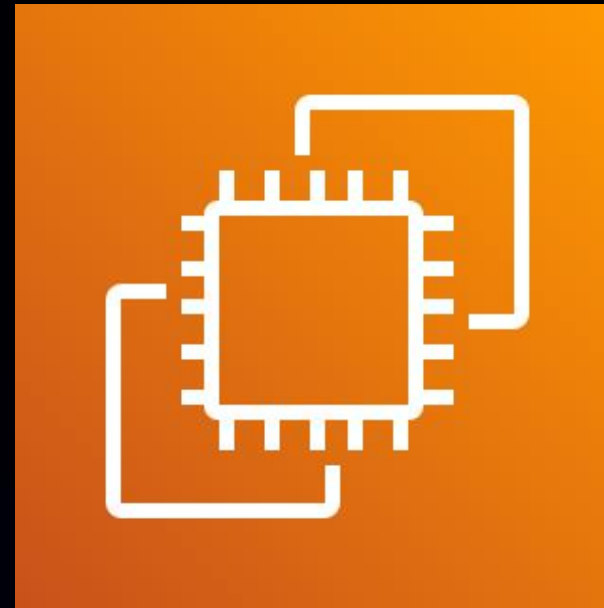
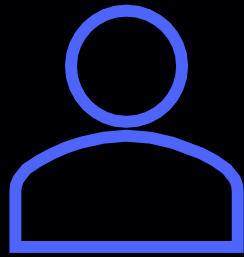


Security considerations

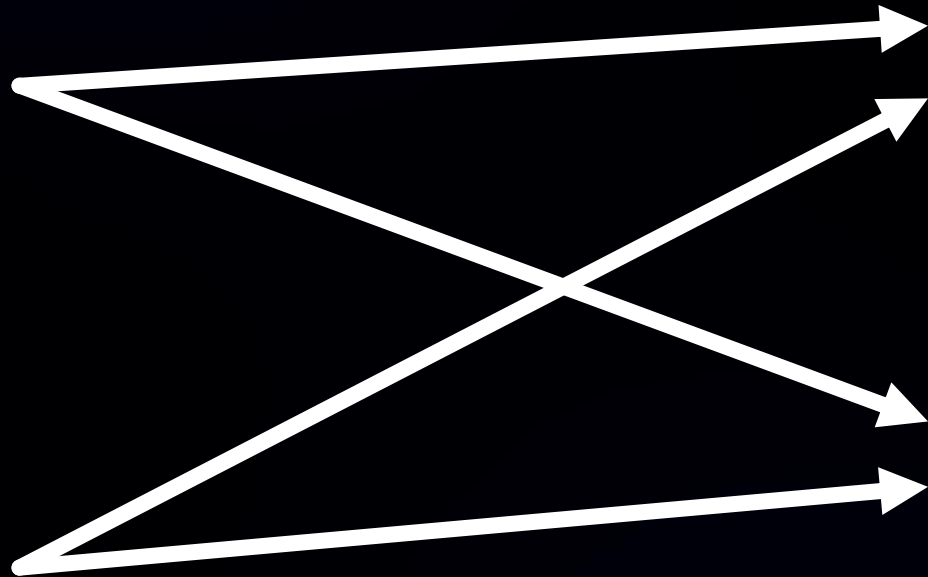
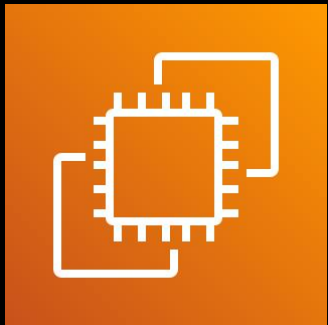
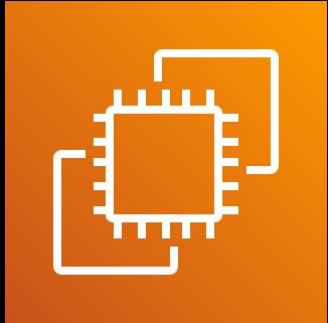


- Encryption at rest and in transit
- Auditing and alarming
- Amazon S3 versioning
- Digital signature verifications
- Least permissions
- Safety switch

User experience



Grouping

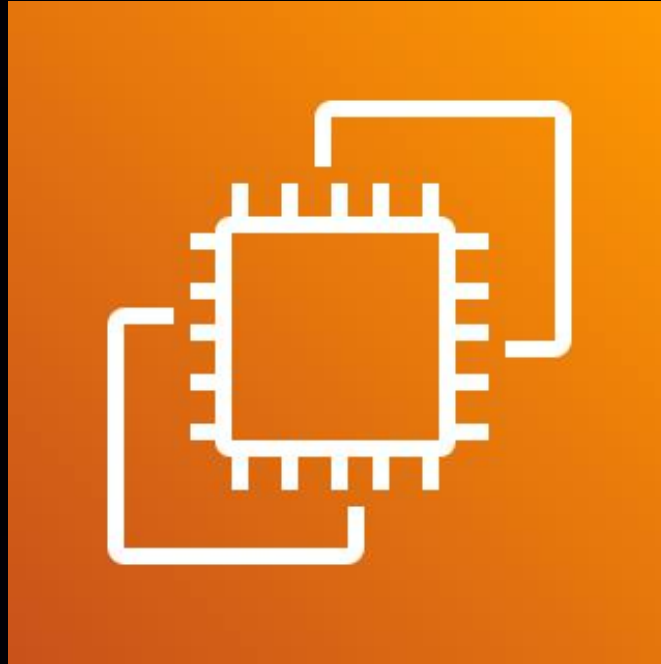


Current state



- 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

