AWS re:Invent

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

WIN302

Managing and governing Microsoft workloads on AWS

Aaron Lima
Principal Solutions Architect
AWS

Jonathan Lozano
Security Consultant
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab info

WIN302: Managing and governing Microsoft workloads on AWS

Lab access: https://dashboard.eventengine.run

Event hash: c3f5-1c57593ed4-ee

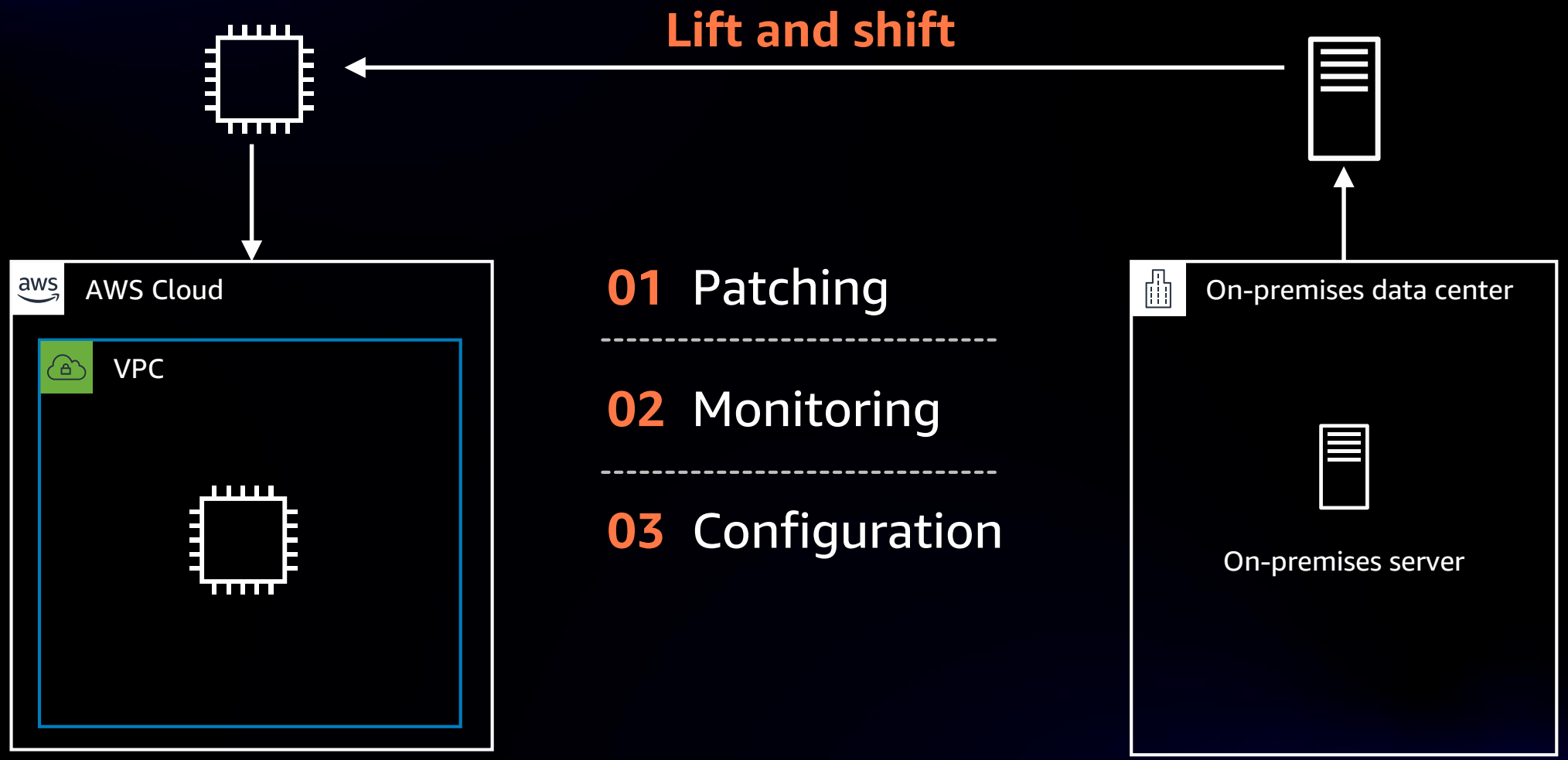
Lab guide: https://ms-immersionday.workshop.aws

SSID: @reInventWorkshops
Password: Exper1ment21

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What's next?



01 Patching

02 Monitoring

03 Configuration

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

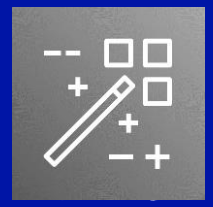
Simple, integrated Ops experience for Windows



Amazon EC2 Image Builder

Build

a compliant enterprise image



AWS Launch Wizard

Deploy

and configure applications simply



Amazon CloudWatch

Monitor

applications with automatic setup and alerting



AWS Systems Manager

Manage

and troubleshoot your fleet of servers

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Systems Manager

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build the foundation



- Quick setup
- Inventory
- Automation
- Parameter store
- State manager

Set up service configurations and collect IT asset inventory

Enable operational best practices

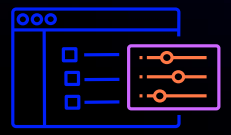
Codify runbooks

Enable continuous compliance

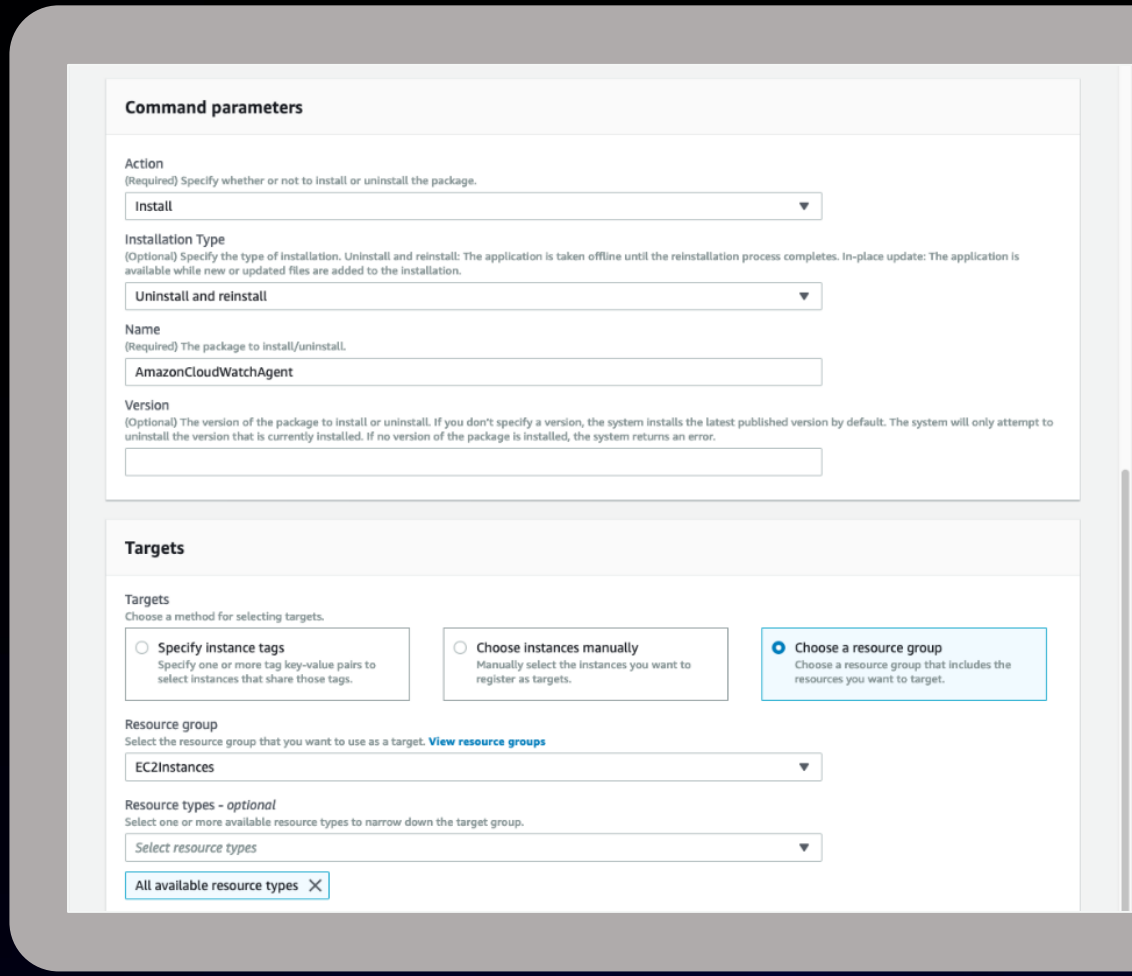
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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 pre-defined failure injections for chaos testing
- Control access via AWS IAM, and record command activity for troubleshooting and auditability
- All without the need for bastion hosts, open inbound ports, or managing SSH keys



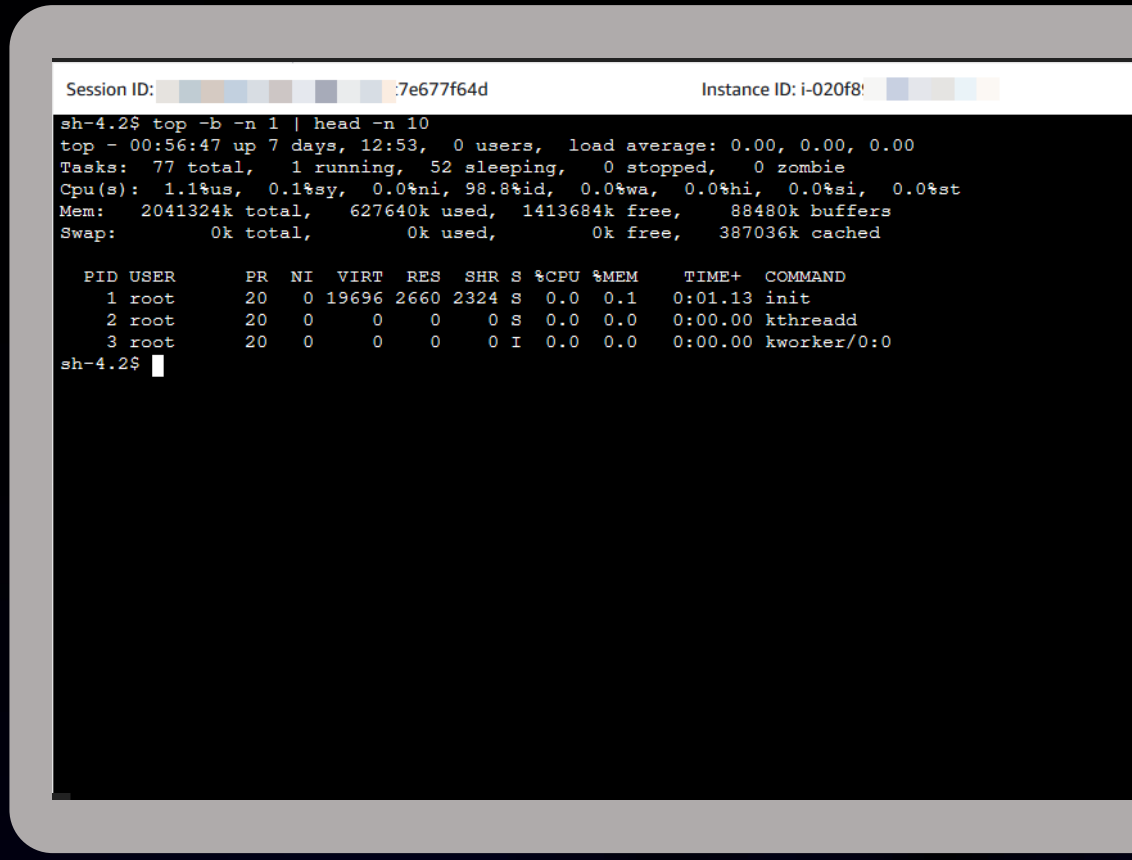
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Session Manager

Secure and auditable privileged access to your compute nodes



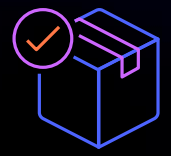
- Single solution for privileged access across Linux and Windows compute nodes
- Enables DevOps and break-glass investigation and remediation
- Eliminates the need for bastion hosts, inbound firewall exceptions, and managing SSH keys
- Centralized access controls via AWS IAM
- Allows detailed activity and session logging to Amazon CloudWatch, Amazon S3 and/or AWS CloudTrail
- Improve the security posture of your managed instances by using interface VPC endpoints



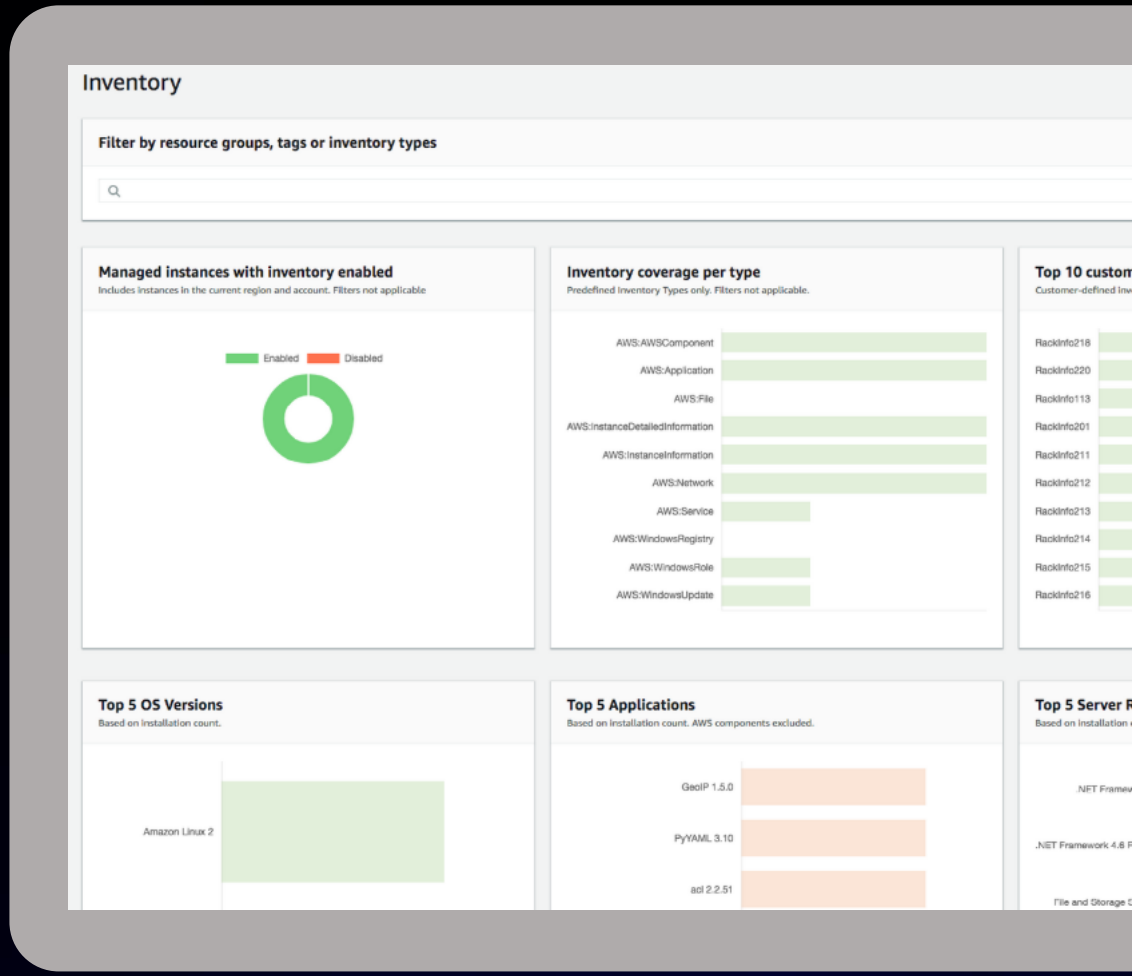
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inventory

Improve visibility of your EC2 and on-premises computing environments



- Collects data about applications, files, network configuration, instance details, Windows Registry and roles
- Gain actionable insights by analyzing aggregated data from multiple AWS Regions and accounts by storing data in S3 bucket and querying it using services like Amazon Athena and Amazon QuickSight
- Integrates with AWS Config for change tracking, compliance, auditing, assessing security risks, and tracking license usage
- Flexibility to create custom inventory to collect non-preconfigured datatypes



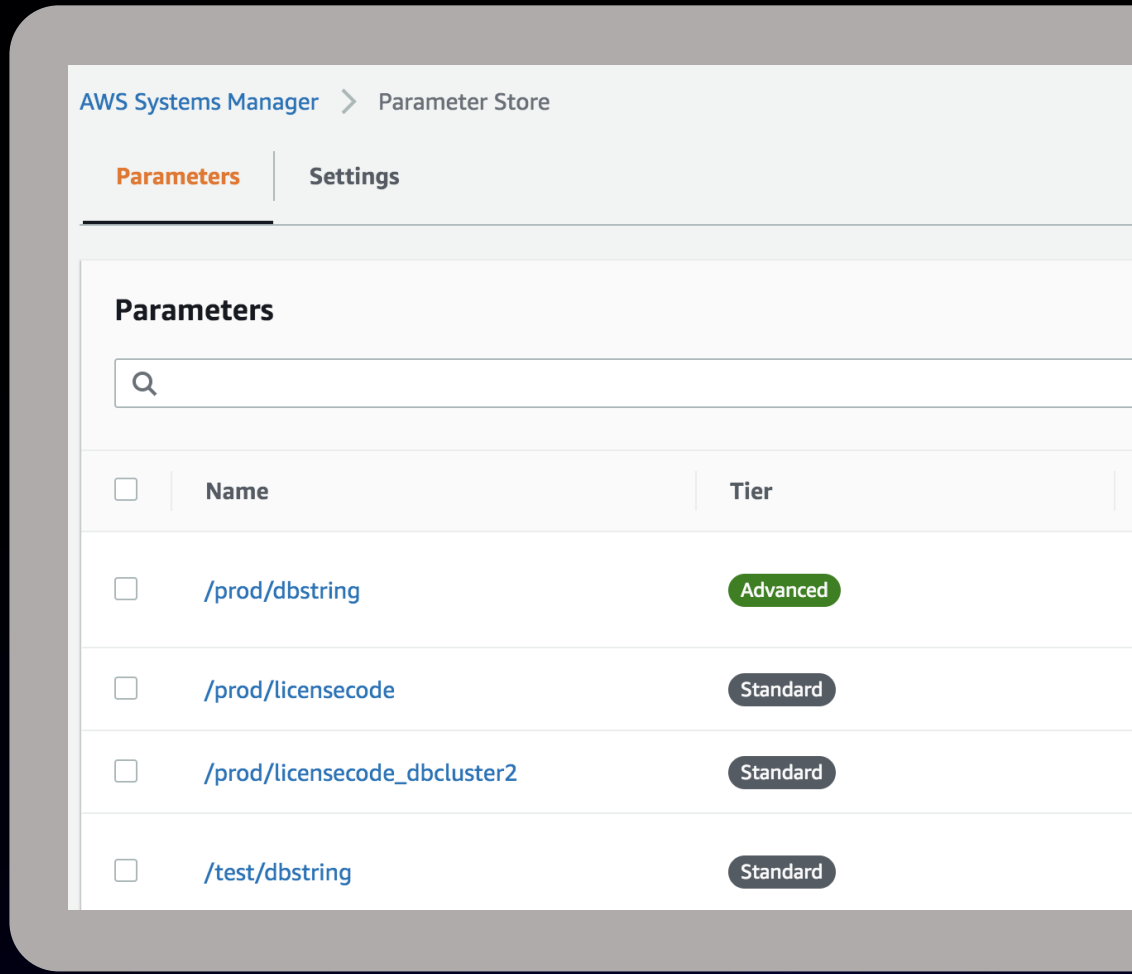
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Parameter Store

Central store for application configuration values



- A secure, scalable managed service to externalize your application configuration values and secrets
- Simplify maintenance of code and automation by updating all parameters centrally in one location
- Eliminates application errors due to hardcoding of variables
- Organize parameters into hierarchies based on environment or application component hierarchy (e.g., /config/prod/fleethealth)
- Control and audit access at individual parameter level



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

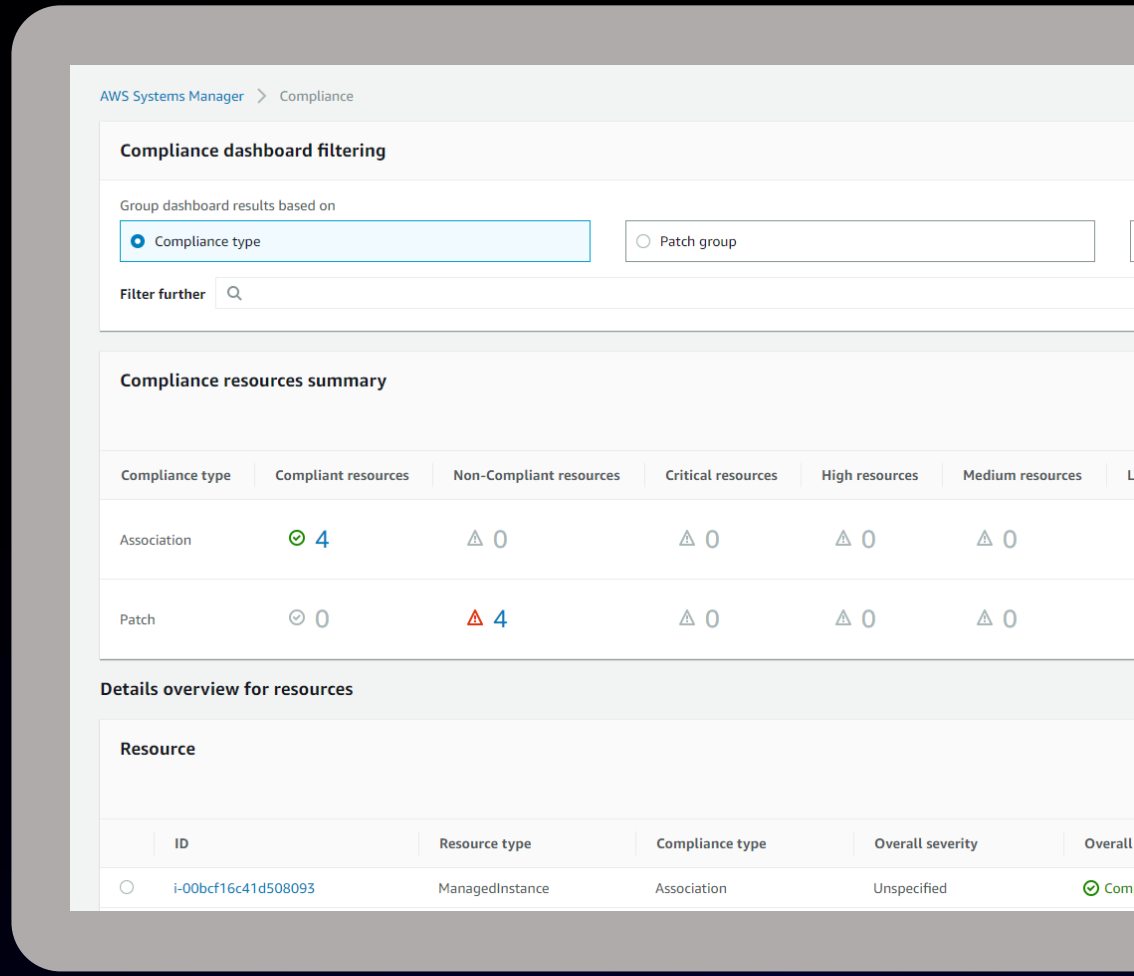
State Manager

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

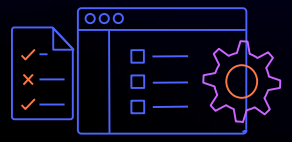
Example: Use State Manager with AWS CloudFormation to install software on instances upon provisioning



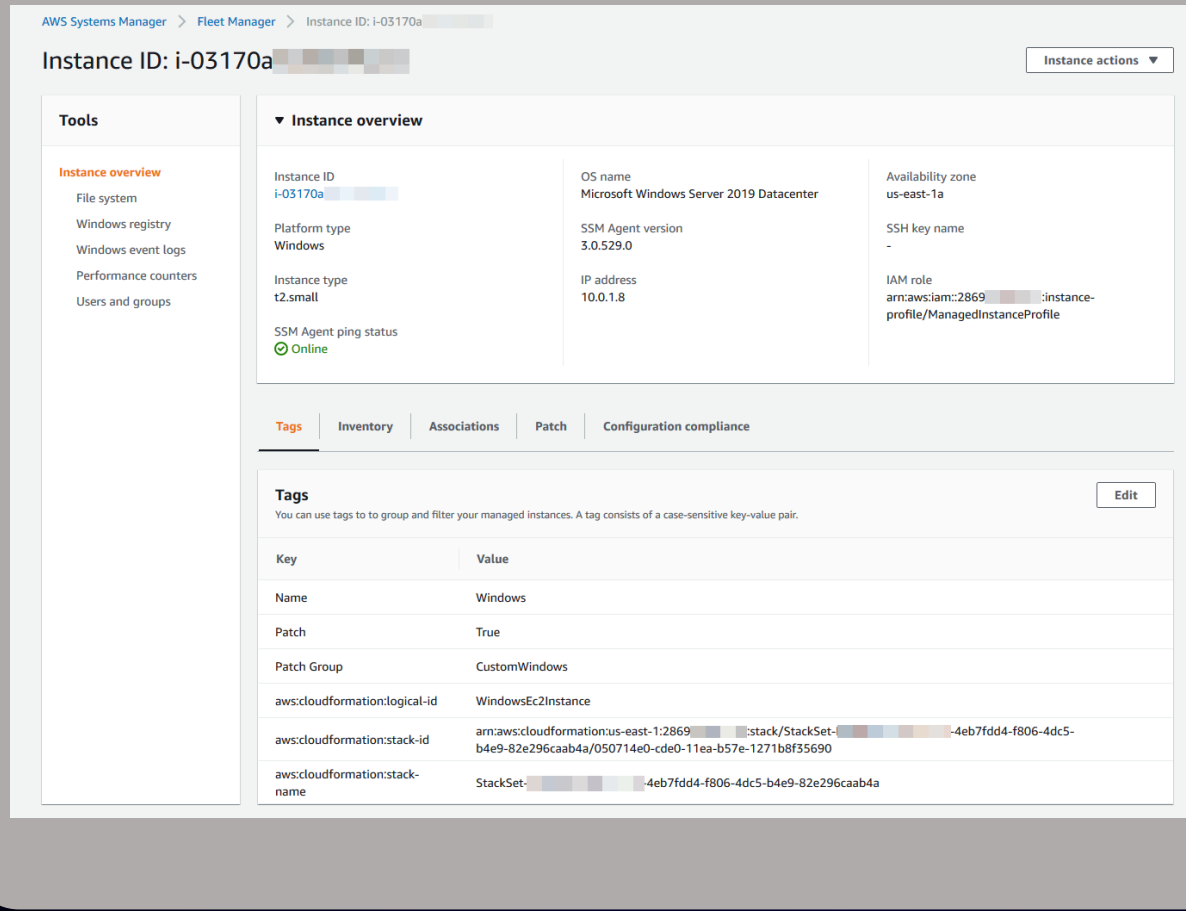
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fleet Manager

Consistent administration across server fleet



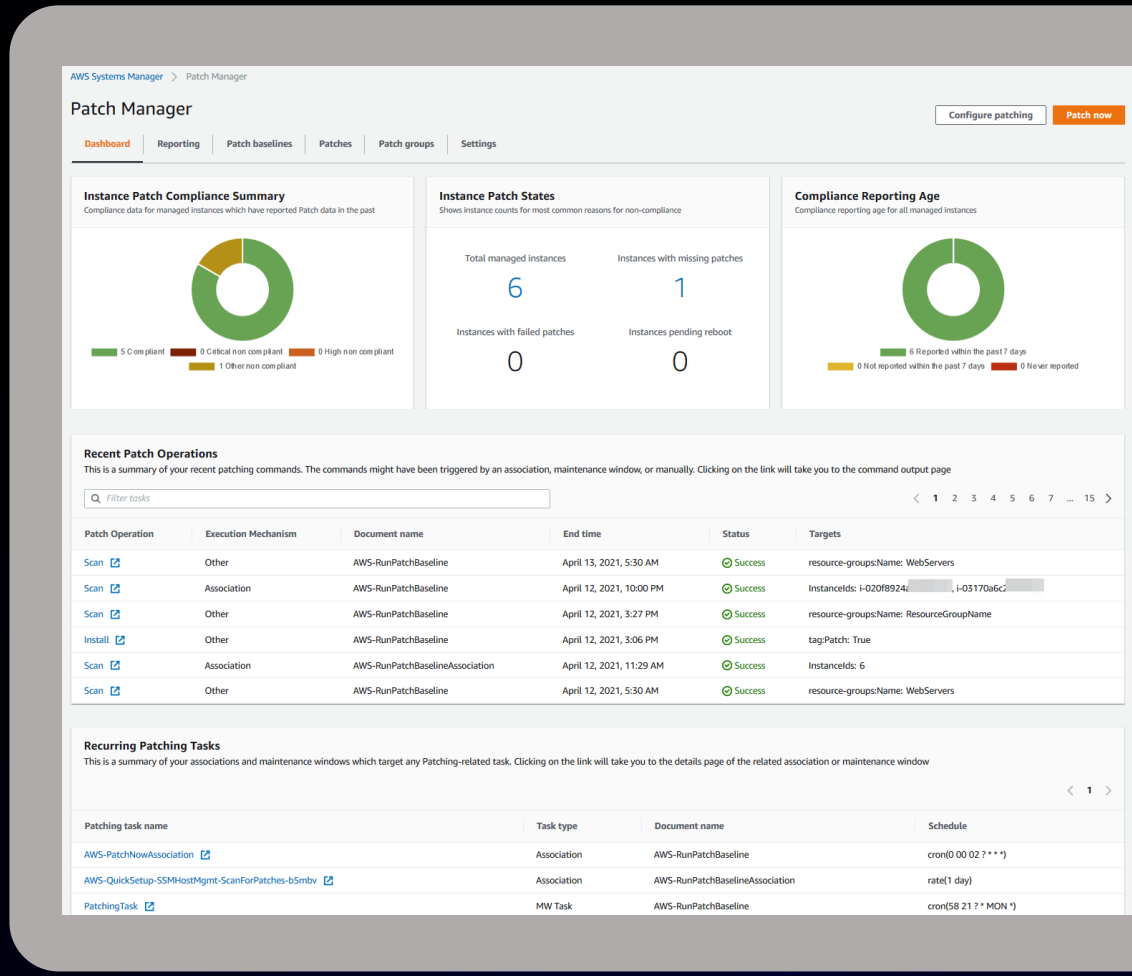
- Manage and troubleshoot your fleet of servers running on AWS and on-premises
- Administer VM fleet without needing to remotely connect with RDP or SSH
- Perform common administrator tasks from a single integrated console



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Patch Manager

Automate the process of patching your instances



- Automate patching by defining rules for auto approval
- Scan and install patches on a regular basis by scheduling maintenance windows
- Shorten the time to install zero-day vulnerability patches
- View aggregate patch compliance using Explorer
- Supported OS include Windows Server, Amazon Linux/2, CentOS, Debian, Oracle Linux, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Ubuntu Server

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Other features



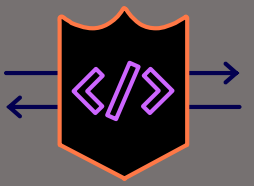
Available in all AWS Regions including GovCloud *



SSM Agent is installed on AWS Windows Server, Amazon Linux, Amazon Linux 2, and Ubuntu AMIs



Accessible through AWS PrivateLink



Systems Manager is SOC, ISO, FedRAMP (JAB/Agency authorized) and PCI compliant, HIPAA enabled

Integrated with AWS services such as

AWS Config
Configuration history

Amazon EventBridge
Notification and remediation

AWS CloudTrail
Audited actions

AWS IAM
RBAC

aws

* Some features are not available in all regions

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab activities

- **Module 1.1** Use Run command to remediate IIS on Windows EC2 instances (Console)
- **Module 1.2** Use Patch Manager to manage patches on Windows EC2 instances (Console)
- **Module 1.3** Use State Manager to ensure Windows instances are joined to a domain (Console)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudWatch

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is observability?

In control theory, **observability** is a measure of how well internal states of a system can be inferred from knowledge of its external outputs

Source: Wikipedia, “Observability.” https://en.wikipedia.org/wiki/Observability

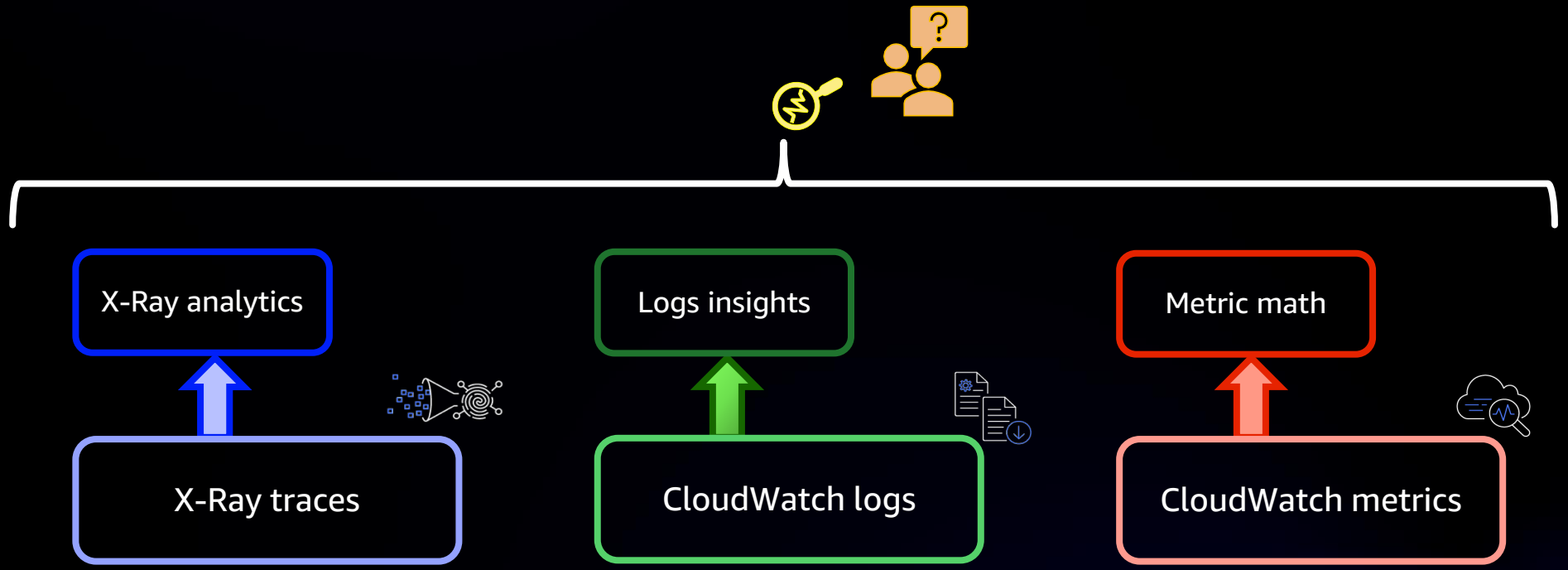
Monitoring tells you whether a system is working; observability lets you understand why it isn't working

Good observability allows you to answer the questions you didn't know that you needed to ask

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

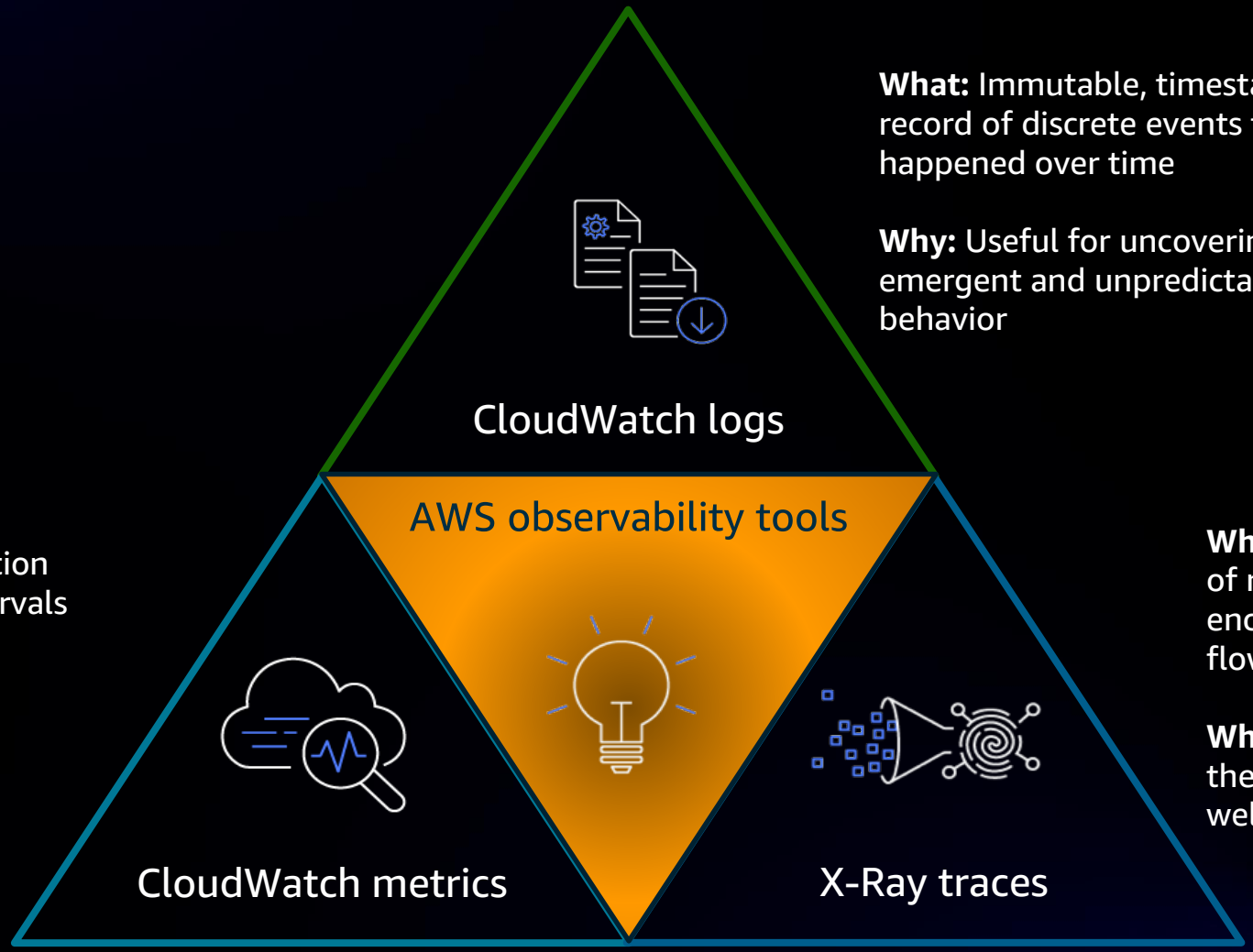
Tools and challenges

- Want to be able to get a 360^0 view of a problem
- Need to correlate logs, metrics and traces to get deeper insights
- Repetitive troubleshooting process
- Data introspection



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS observability tools



What: Immutable, timestamped record of discrete events that happened over time

Why: Useful for uncovering emergent and unpredictable behavior

What: Numeric representation of data measured over intervals of time

Why: Useful for identifying trends, mathematical modeling, and prediction

What: Representation of a series of related distributed events that encode the end-to-end request flow through a distributed system

Why: Provides visibility into both the path traversed by a request as well as the structure of a request

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab activities

- **Module 2.1** Create CloudWatch agent configuration (Console)
- **Module 2.1** Install and configure Amazon CloudWatch to capture metrics and logs on our EC2 instances (Console)
- **Module 2.2** Configure automated response to CloudWatch events (optional - Console)

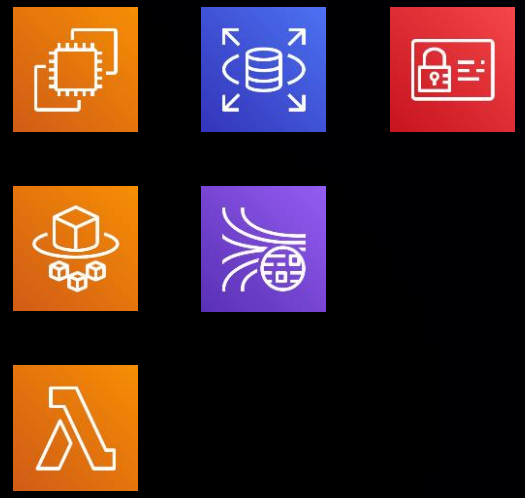
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

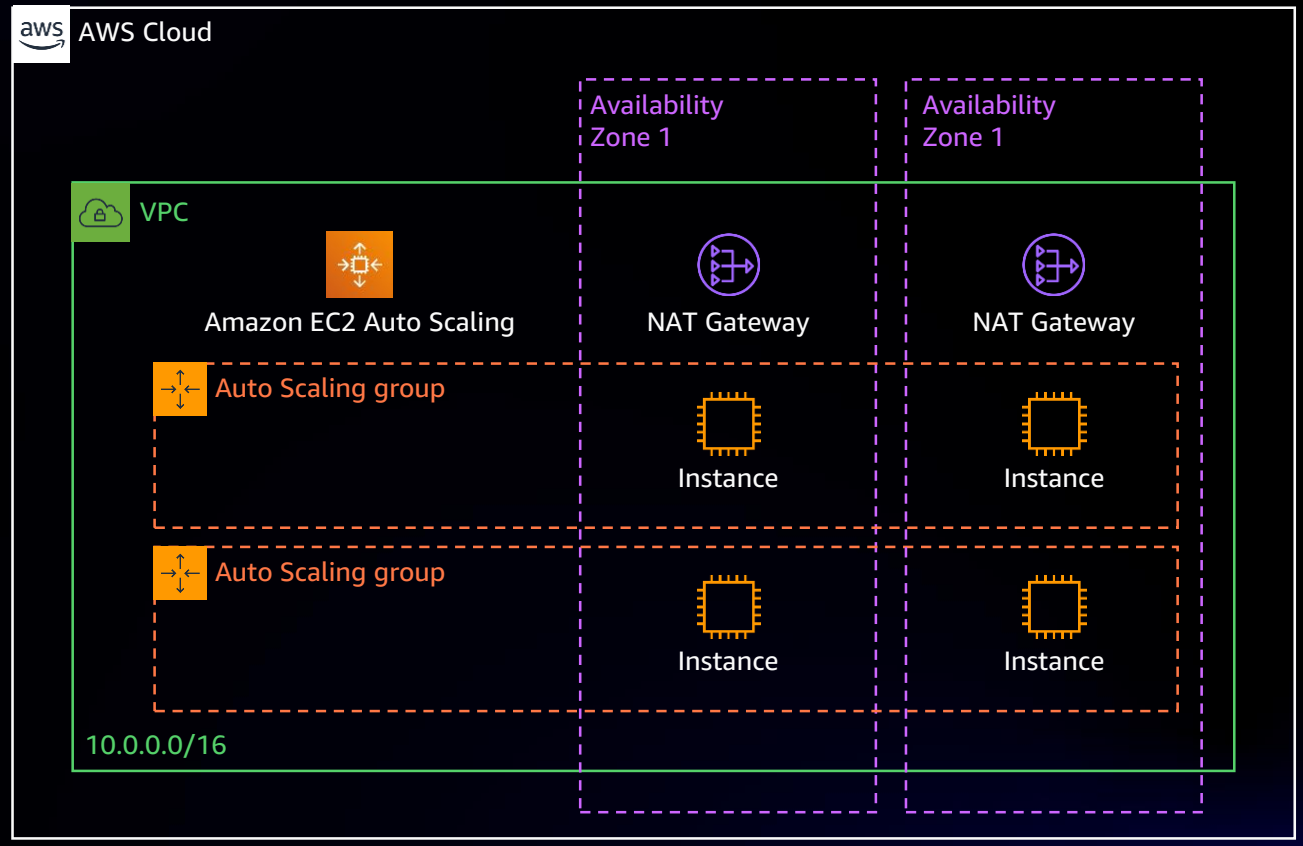
AWS CloudFormation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introduction

Managing a cloud application involves managing the lifecycle of its resources





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

Resources are the building blocks, or components, of cloud applications

Several ways of managing cloud resource lifecycle (creation, update, deletion)



AWS Management Console



AWS Command Line Interface



AWS Tools and SDKs



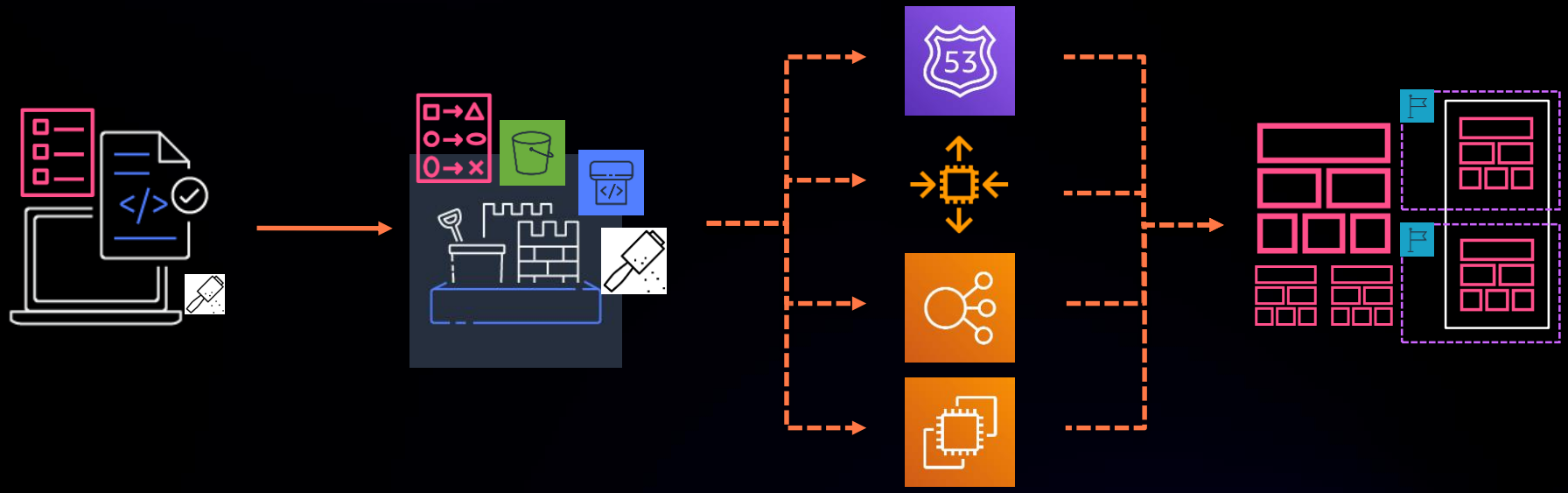
AWS CloudFormation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudFormation

At a high level, the template describes the intended state of your resources

CloudFormation then translates that intention to API calls, providing abstraction



1. Code your template
2. Upload, test, & review changes
3. Execution of changes creates a stack
4. Manage stacks and stack sets

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab activities

- **Module 3.1** Use AWS CloudFormation to create AWS Systems Manager automation runbooks (CLI)
- **Module 3.1** Run AWS Systems Manager automation runbooks to configure Windows instances (CLI)
- **Module 3.2** Use AWS CloudFormation and AWS Systems Manager automation to configure Windows instances in an autoscaling group (CLI)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab info

WIN302: Managing and governing Microsoft workloads on AWS

Lab access: https://dashboard.eventengine.run

Event hash: c3f5-1c57593ed4-ee

Lab guide: https://ms-immersionday.workshop.aws

SSID: @reInventWorkshops
Password: Exper1ment21

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.