Patching VMs with SSM Patch Management

David O'Brien

MICROSOFT MVP, SENIOR DEVOPS CONSULTANT

@david_obrien   https://david-obrien.net

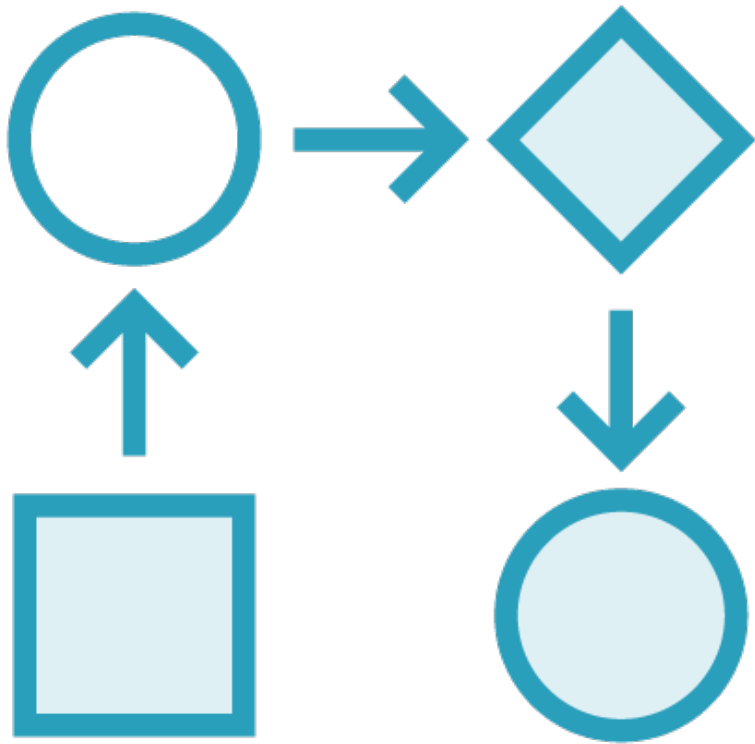# Module Overview

How does Patch Management work

Patch Baselines

Patch Groups

Maintenance Windows

How Does Patch Management Work?

Supported OS:

- Windows Server 2008 – 2016
- Amazon Linux 2012.03 – 2017.03
- RHEL 6.5 – 6.9
- Ubuntu 14.04 / 16.04 LTS

How Does Patch Management work

AWS EC2

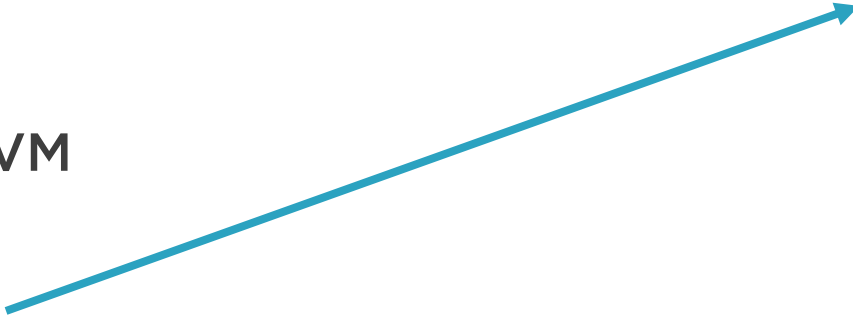**On-prem VM**

AWS

How Does Patch Management work

AWS EC2

On-prem VM

AWS

How Does Patch Management work

AWS EC2

On-prem VM

AWS

Windows Update / yum repo
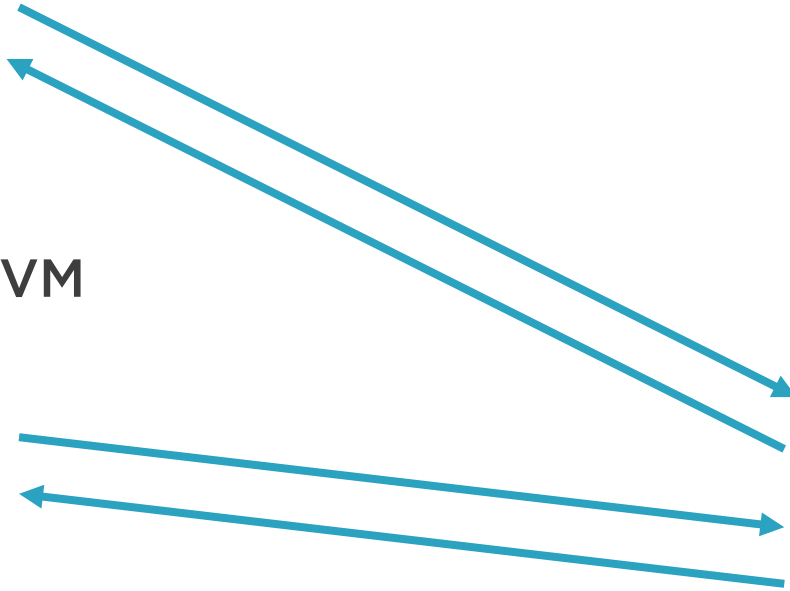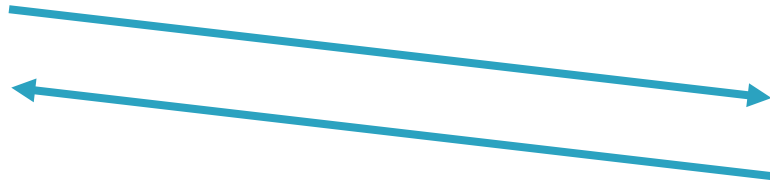
How Does Patch Management work

AWS EC2

**Windows Update /
yum repo**

AWS
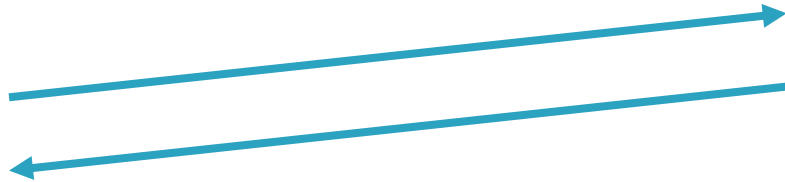
On-prem VM

**WSUS /
Local mirror**

Patch Baselines

AWS provides default baselines for Windows, Amazon Linux, RHEL & Ubuntu

- Define
  - Approved patch classifications
  - Approval delays

Custom baselines for more control

Only one baseline per instance

Patch Groups

Optional, but recommended

Group servers for patching

- Tag
  - Key = Patch Group
  - Value = %any string%

Servers can only be a member of one Patch Group

Attach Patch Groups to Patch Baselines

Maintenance Windows

Optional, but recommended

Schedule for patching operations

Targets = Patch Group

Either "Scan" or "Scan & Install"

Systems Manager reboots after patching

Demo

Create a patching solution

Module Summary

How does SSM Patch Management work

Components that make up Patch Management

- Baselines

- Groups

- Maintenance Windows

How to stitch it all together