Lab – Systems Manager

Configure Systems Manager

Setup roles and permissions

Lab – Systems Manager

Manage instances (EC2, On-premises)

- EC2 - IAM role
- On-premises - TLS + Activation Code + ID
- Systems Manager Agent

Session Manager

- IAM Based access to instance
- Access private instances (with endpoints)
- No need for Bastion hosts

Compliance Monitoring

Lab – Patch Manager

Patch Baselines

Patch Groups

Customize Patching Schedule

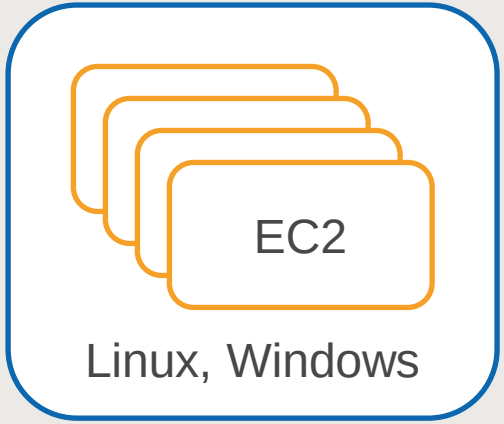
Lab – Monitor failed login attempts to instance

- Monitor `/var/log/secure` log file in the instance
- CloudWatch Agent
    - Monitor log files
    - Publish memory and disk metrics to CloudWatch
    - Install using Systems Manager
- Configuration
    - Use Wizard to generate configuration file

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
```

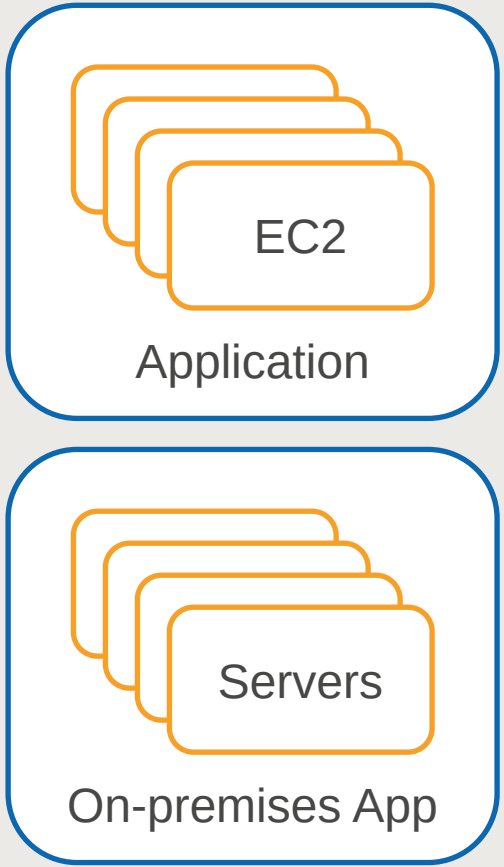
    - Store configuration in Parameter Store

AWS Systems Manager



- Patch Management
- Run Commands across a fleet of instances
- Session Manager - Interactive shell/CLI for Linux and Windows
- IAM based access to servers
- No need for SSH/RDP/Bastion Host
- Inventory – OS, Software, Configuration (AWS Config integration)
- Parameter Store – Configuration data and secrets

AWS Systems Manager



- State Manager – Maintain consistent configuration (anti-virus, firewall, server setting)
- Automation of routine administrative tasks (example: Create AMI, Recover impaired instances, stop instance with approval)
- App Config - Manage application configuration and changes

AWS Config

- Compare current and desired state of resources
- Managed ready to use rules, Create custom rules
- Change history
- Multi-account, multi-region data aggregation
- Systems Manager integration (OS, Application, System level config)
- Alert when changes detected

AWS Config – Managed Rule Checks

- Access key rotated periodically
- ALB HTTP to HTTPS redirection configured
- Unused EBS Volumes, unused Elastic IP
- Check if multi-az is configured for RDS
- Verify is S3 bucket has bucket-level encryption enabled
- Check if EC2 instance is managed by systems manager

Managed Rules: https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html

AWS Config

- Compare current and desired state of resources
- Managed ready to use rules, Create custom rules
- Change history
- Multi-account, multi-region data aggregation
- Systems Manager integration (OS, Application, System level config)
- Alert when changes detected

AWS Best Practices

Compare with Your Implementation

AWS Inspector

Security exposures and vulnerabilities in your EC2 instances

Network Assessment

- Ports reachable from outside the VPC
- Processes reachable on the port (with Inspector agent)

Host Assessment

- Vulnerable software (CVE)
- Host hardening (CIS Benchmarks)
- Security best practices
- Requires Inspector Agent

AWS Trusted Advisor

Scans and compares your infrastructure against AWS best practices

COST OPTIMIZATION

PERFORMANCE

SECURITY

FAULT TOLERANCE

SERVICE LIMITS

Trusted Advisor Core Checks

All Customers have access to seven core checks

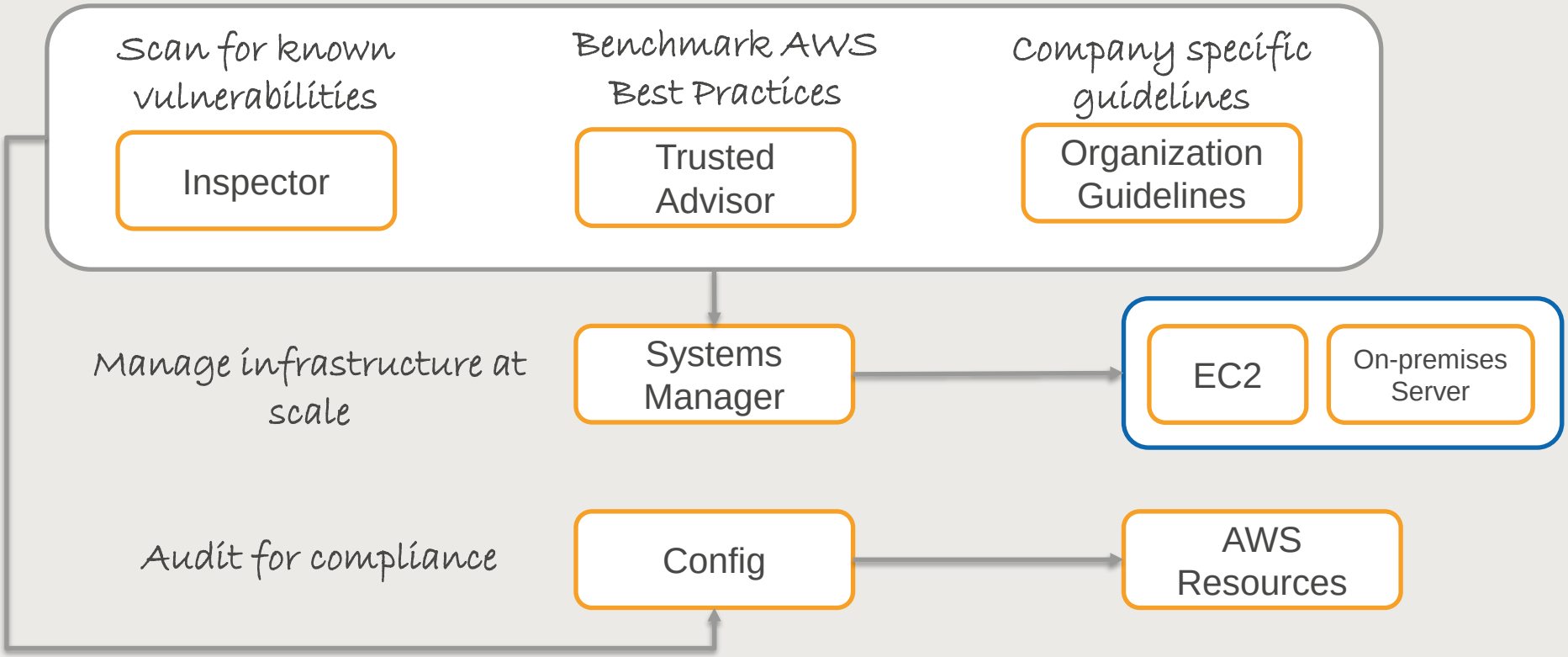
Example:

- S3 bucket permissions
- Security Groups - Specific ports that are unrestricted
- IAM use, MFA on root account
- EBS Public snapshots
- RDS Public snapshots
- Service Limits

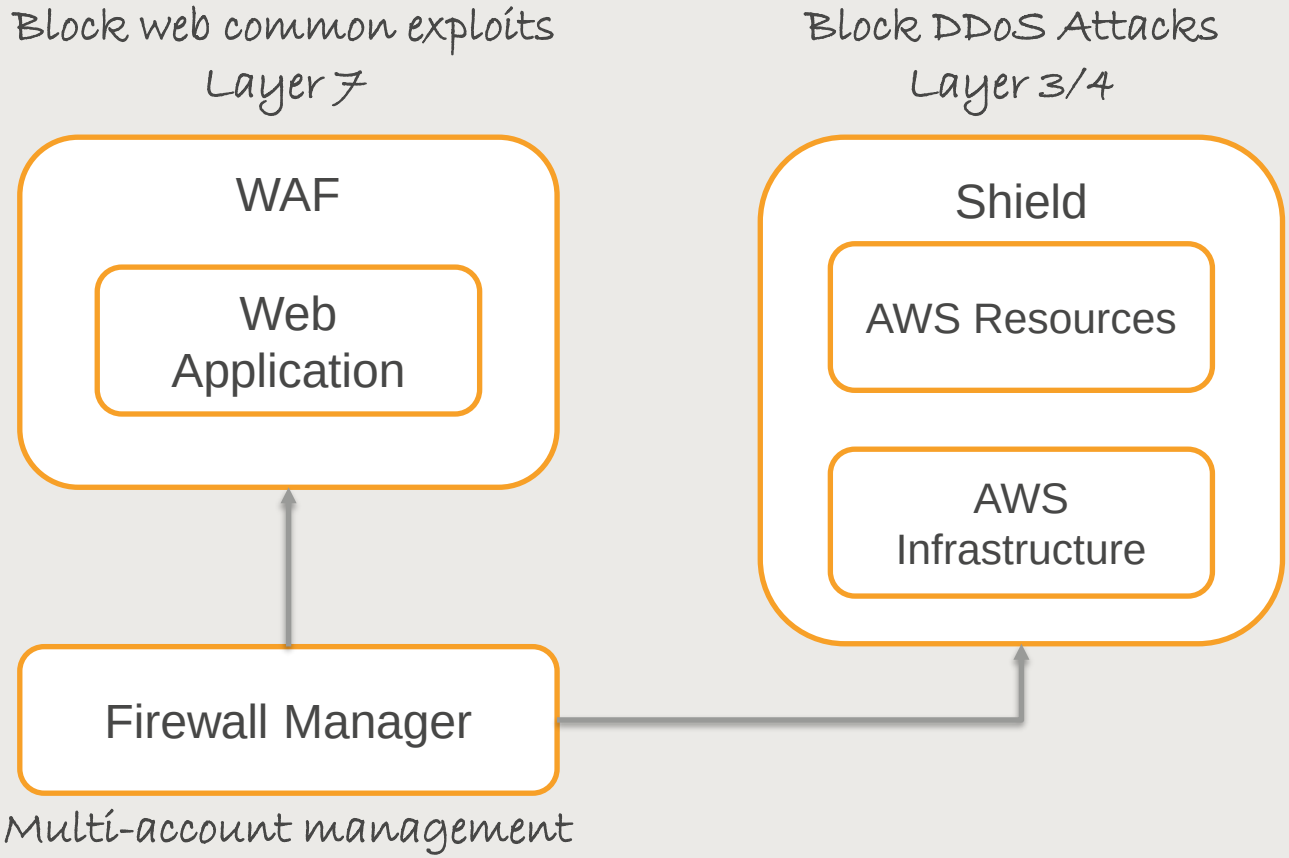
Trusted Advisor – Full Checks

Customers with Business and Enterprise Support have access to full set of trusted advisor checks

Putting it all together



Putting it all together



Chandra Lingam

57,000+ Students

For AWS self-paced video courses, visit:

https://www.cloudwavetraining.com/

Cloud Wave LLC