
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

EUC312

Securing end user computing workloads on AWS end user computing services

Michael Mattes

Enterprise Account Engineer
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Account-level best practices

Securing Amazon WorkSpaces: where to start?

Best security practices for Amazon WorkSpaces

Best security practices for Amazon AppStream 2.0

Additional resources

Making it “real” / whiteboarding customer scenarios

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account-level best practices

- Activate multi-factor authentication (MFA) on the AWS account root user
- Use temporary security credentials (IAM roles) instead of access keys, and disable any AWS account root user access keys
- Use AWS IAM Access Analyzer to analyze your existing permissions
- Use AWS CloudTrail and Amazon CloudWatch in conjunction to monitor credential usage and receive alerts for unusual API calls
- Turn on logging for all AWS Regions, not just the ones you regularly use

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing Amazon WorkSpaces: where to start?

- Securing the endpoint
- Securing the control plane
- Securing the data plane
- Securing the WorkSpace
- Securing the directory

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best security practices for Amazon WorkSpaces

- Ensure your authentication source, Active Directory (AD), is hardened
  - WorkSpaces supports client-side LDAPS
- The streaming connection for PCoIP is encrypted by using AES 128- and 256-bit ciphers, but defaults to 128-bit. Customers can change this to 256-bit, either using PCoIP-specific AD Group Policy settings for Windows WorkSpaces or using the pcoip-agent.conf file for Amazon Linux WorkSpaces
- Use AWS Network Firewall and NAT Gateway together when you do not possess any other means to provide EUC network protections such as Server Name Inspection (SNI) for HTTPS-based websites, Intrusion Detection and Prevention, and an allow and deny list for domain names

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best security practices for WorkSpaces (continued)

- Encrypt WorkSpaces with an AWS Key Management Service (AWS KMS) customer managed key
- Control where users can connect from using a combination of trusted devices and IP access control groups
- Implement MFA for WorkSpaces
- Control clipboard redirection to and from WorkSpaces to mitigate data exfiltration

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best security practices for AppStream 2.0

- Encrypt your persisted user data to a Server Message Block (SMB) share using an AWS KMS customer managed key
- When using antivirus agents with AppStream 2.0, ensure that boot-time scans are disabled
  - Perform antivirus (AV) scans on user data that persists or directories where users will save data
- Use AppLocker from Microsoft to ensure that only the applications that your organization requires can be run
  - For fleet instances joined to an AD domain, use Group Policy Objects (GPOs) to deliver user and system settings to secure the users' application and resource access

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best security practices for AppStream 2.0 (continued)

- Control clipboard redirection to and from AppStream 2.0 to mitigate data exfiltration
  - Disabling this setting does not disable copy and paste within the session. If copying data into the session is required, choose Paste to remote session only to minimize the potential for data leakage

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional resources

EUC204
Creating remote work environments that optimize security and productivity

EUC301-R
Securely stream AWS workloads to your remote workers

EUC310
Streamlining log-on experience for Amazon WorkSpaces and AppStream 2.0

EUC311
Building a secure end user computing environment for power users

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Michael Mattes
mattesm@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.