CIS Benchmarks

CIS AWS End User Compute Services Benchmark

v1.0.0 - 11-13-2020

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Terms of Use 1

Overview 5

Intended Audience 5

Consensus Guidance 5

Typographical Conventions 7

Assessment Status 7

Profile Definitions 8

Acknowledgements 9

Recommendations 10

1 Introduction 10

2 WorkSpaces 12

2.1 Ensure Administrators of WorkSpaces is defined using IAM (Automated) 13

2.2 Ensure MFA is enable for WorkSpaces users (Manual) 16

2.3 Ensure WorkSpace volumes are encrypted. (Automated) 19

2.4 Ensure WorkSpaces are deployed in their own virtual private cloud (VPC) (Manual) 23

2.5 Ensure WorkSpaces traffic is controlled and routed through a NAT Gateway. (Manual) 27

2.6 Ensure Web Access to Workspaces is Disabled (Automated) 30

2.7 Ensure access is limited to trusted devices. (Manual) 32

2.8 Ensure the default IP access control group is disassociated. (Automated) 35

2.9 Ensure CloudWatch is set up for WorkSpaces. (Manual) 38

2.10 Ensure that patches and updates are performed on the operating system for Workstations. (Automated) 41

2.11 Ensure your WorkSpaces image has the appropriate CIS Operating System Benchmark applied (Manual) 44

2.12 Restrict WorkSpaces Bundle options to organization approved versions (Manual) 46

2.13 Ensure Workspaces images are not older than 90 days. (Manual) 49

2.14 Ensure WorkSpaces that are not being utilized are removed. (Automated) . 51

2.15 Ensure primary interface ports for Workspaces are not open to all inbound traffic. (Automated) 54

2.16 Ensure FIPS Endpoint encryption is enabled for WorkSpaces. (Manual) 56

2.17 Ensure WorkSpaces API requests flow through a VPC Endpoint (Automated) 58

2.18 Ensure Radius server is using the recommended security protocol (Automated) 61

3 WorkDocs 63

3.1 Ensure Administrators of WorkDocs is defined using IAM (Automated) 64

3.2 Ensure MFA is enable for WorkDoc users (Manual) 66

3.3 Ensure Workdocs access is limited to a range of allowable IP addresses. (Manual) 70

3.4 Utilize site wide activity feed for monitoring. (Manual) 72

3.5 Ensure new users can only be invited from allowed domains. (Manual) 74

3.6 Ensure only specific users are allowed to invite external users (Manual) 76

3.7 Ensure publicly shareable links is not allowed in WorkDocs (Manual) 78

3.8 Ensure any user that has not accessed WorkDocs in 30 days is set to inactive. (Manual) 80

4 AppStream 2.0 82

4.1 Ensure AppStream is utilizing its own virtual private cloud (VPC) (Manual) . 83

4.2 Ensure a VPC Endpoint is set for AppStream (Manual) 87

4.3 Ensure maximum session duration is no longer than 10 hours. (Automated) 89

4.4 Ensure session disconnect timeout is set to 5 minutes or less. (Automated) .. 91

4.5 Ensure session Idle disconnect timeout is set to 10 minutes or less. (Automated) 93

4.6 Ensure internet access is granted and managed through your VPC (Automated) 95

4.7 Ensure Operating system updates are applied to your base image every 30 days. (Manual) 97

5 WorkLink 100

5.1 Ensure the Audit log stream is configured. (Manual) 101

5.2 Ensure device policies are configured. (Manual) 103

Appendix: Summary Table 105

Appendix: Change History 107

Overview

This document provides prescriptive guidance for configuring security options for the services within End User Computing category in AWS. This Benchmark is intended to be used in conjunction with the CIS Amazon Web Services Foundations Benchmark. For more information about this approach see the *Introduction* section of this document.
The specific AWS Services in scope for this document include:

- Amazon WorkSpaces
- Amazon WorkDocs
- Amazon AppStream 2.0
- Amazon WorkLink

To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at benchmarkinfo@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions in Amazon Web Services. A typical enterprise has use cases for each service from access desktop resources from any computer or tablet, to stream GPU intensive apps to accessing internal web-based content, from mobile devices.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide security focused best practice hardening of a technology; and
  - limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is more critical than manageability and usability
  - acts as defense in depth measure
  - may impact the utility or performance of the technology
  - may include additional licensing, cost, or addition of third party software

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Gregory Carpenter

Contributor
Mike Wicks
Darwin Sanoy

Recommendations

1 Introduction

Benchmark Approach:

The suggested approach for securing your cloud environment is to start with the CIS Amazon Web Services Foundations Benchmark found here: https://www.cisecurity.org/benchmark/amazon_web_services/. The CIS Foundations benchmark provides prescriptive guidance for configuring a subset of Amazon Web Services with an emphasis on foundational, testable, and architecture agnostic settings including:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- AWS CloudWatch
- AWS Simple Notification Service (SNS)
- AWS Simple Storage Service (S3)
- AWS VPC (Default)

The Amazon Web Services Foundation Benchmark is what you should start with when setting up your AWS environment. It is also the foundation for which all other AWS service based benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

After configuring your environment to the CIS Amazon Web Services Foundations Benchmark, we suggest implementing the necessary configurations for the services utilized as defined in the associated product and service level benchmarks. The CIS End User Compute Benchmark provides prescriptive guidance for configuring security options for the services within End User Computing in AWS. The specific AWS Services in scope for this document include:

- Amazon WorkSpaces
- Amazon WorkDocs
- Amazon AppStream 2.0
- Amazon WorkLink

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Amazon Web Services Benchmarks, please register on CIS WorkBench at https://workbench.cisecurity.org and join the CIS Amazon Web Services Benchmarks community.

2 WorkSpaces

This section contains recommendations for configuring the WorkSpaces service and any additional resources required.

2.1 Ensure Administrators of WorkSpaces is defined using IAM (Automated)

Profile Applicability:

- Level 1

Description:

To allow users to administer Amazon WorkSpaces, IAM policies must be created with the required permissions.

Rationale:

Using IAM to create and manage users for Workspaces is not supported. Workspace Administrators will manage these users within the Workspace service console.

Audit:

Perform the following to determine what policies are created:
From the Console:

1. Login in and open the IAM console at `https://console.aws.amazon.com/iam/`.
2. In the left pane click on `Groups`.
3. Click on the `group name` that should administer Workspaces.
4. Click on `Permissions` and confirm that the AmazonWorkSpacesAdmin policy is attached.
5. Click on `Users` and confirm that the list of names are the users approved to administer WorkSpaces.

From the Command Line:

1. Run the `list-attached-group-policies`.

```
aws iam list-attached-group-policies --group-name <workspace_group_name>
```

2. Confirm that the list of users in that Group is correct

```
aws iam get-group --group-name <workspace_group_name>
```

If the AWS manage policy or a custom WorkSpaces Admin policy is not attached to the group or the users in the group list is not correct refer to the remediation below.

Remediation:

If the group for WorkSpaces Administration doesn't exist.
From the Console:

1. Login to the IAM console at `https://console.aws.amazon.com/iam/`.
2. In the left pane click on `Groups`
3. Click on `Create New Group`.
    - Name the group - click `Next`
    - Attach the AmazonWorkSpacesAdmin policy - click `Next`
    - Review and click `Create`.
4. Select the `Group` from the list.
    - Click on `users`
        - Click on `Add Users to the Group`.
        - Add all the users that are designated WorkSpaces Administrators.
        - Click `Add users`.

From the Command line

1. Create the WorkSpaces Admin Group by running `aws iam create group`

```
aws iam create-group --group-name <WorkSpaces_Admin_Group>
```

2. Attach the AmazonWorkSpacesAdmin policy by running the `aws iam attach-group-policy'

```
aws iam attach-group-policy --policy-arn
arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin --group-name
<WorkSPaces_Admin_Group>
```

3. Add users to the group to administer WorkSpaces by running `aws iam add-user-to-group`

```
aws iam add-user-to-group --user-name MyUser --group-name
<WorkSpaces_Admin_Group>
```

If the group for WorkSpaces Administration exists but does not have the policy attached.
From the Console

1. Login to the IAM console at `https://console.aws.amazon.com/iam/`.
2. In the left pane click on `Groups`
3. Select the `Group`.
4. Click on the `Permissions` tab
5. Click on `Attach Policy`.
6. Select the `AmazonWorkSpacesAdmin` Policy

7. Click `Attach Policy`

From the Command Line:

1. Attach the AmazonWorkSpacesAdmin policy by running the `aws iam attach-group-policy` command

```
aws iam attach-group-policy --policy-arn
arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin --group-name
<WorkSpaces_Admin_Group>
```

2. Add users to the group to administer WorkSpaces by running the `aws iam add-user-to-group` command.

```
aws iam add-user-to-group --user-name MyUser --group-name
<WorkSpaces_Admin_Group>
```

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-access-control.html
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/manage-workspaces-users.html

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.2 Ensure MFA is enable for WorkSpaces users (Manual)

Profile Applicability:

- Level 2

Description:

Multi-Factor Authentication (MFA) adds an extra layer of authentication assurance beyond traditional username and password. With MFA enabled, when a user signs in to Amazon WorkSpaces, they will be prompted for their user name and password as well as for an authentication code from their physical or virtual MFA token. It is recommended that MFA be enabled for all accounts that utilize WorkSpaces.

Rationale:

Enabling MFA provides increased security to a user name and password as it requires the user to have a virtual or physical hardware solution that displays a time-sensitive code.

Impact:

To enable MFA for Amazon WorkSpaces you require a RADIUS server or a plugin to a RADIUS server already in use in your environment.

Multi-factor authentication is not available for Simple AD.

Audit:

Preform the following steps to check multi-factor authentication is enabled for WorkSpaces
From the Console:
For AWS Managed AD Authenticated Amazon Workspaces Environments:

1. Identify the IP address of your `RADIUS MFA server` and your `AWS Managed Microsoft AD directory`.
2. In the AWS Directory Service console navigation pane, select `Directories`.
3. Choose the directory ID link for your AWS Managed Microsoft AD directory.
4. On the Directory details page, select the `Networking & security` tab.
5. In the `Multi-factor authentication` section, confirm that it is `enabled` and that Radius Status is completed.

For Self-Managed AD (with AD Connector) Amazon Workspaces Environments:

1. Identify the IP address and port of your `RADIUS MFA server` and your `AWS Managed Microsoft AD Connector Identifier`.

2. In the AWS Workspaces console navigation pane, select `Directories`.
3. Choose the `directory ID link` for your `AWS Managed Microsoft AD connector`.
4. On the Directories page, select the `Actions > Update Details`.
5. In the `Multi-factor authentication` section, confirm that it is enabled and that Radius Status is completed, `Enable Multi-Factor Authentication` is checked and the IP Address of your `Radius MFA server` matches that of the `RADIUS server IP address(es)` field.

If it is not enabled or the Radius status is in another state refer to the remediation steps below.

Remediation:

Perform the steps below to enable multi-factor authentication for WorkSpaces
From the console:
For AWS Managed Microsoft AD based Workspaces Environments:

1. Identify the IP address of your RADIUS MFA server and your AWS Managed Microsoft AD directory.
2. In the AWS Directory Service console navigation pane, select `Directories`.
3. Choose the directory ID link for your AWS Managed Microsoft AD directory.
4. On the `Directory details` page, select the `Networking & security` tab.
5. In the Multi-factor authentication section, click `Actions`, and then click `Enable`.
6. On the `Enable multi-factor authentication (MFA)` page, provide the following values:

- Display label - Provide a label name.
- RADIUS server DNS name or IP addresses
  Note - AWS Directory Service does not support RADIUS Challenge/Response authentication.
- Port - default 1812
- Shared secret code
- Confirm shared secret code
- Protocol - MS-CHAPv2
- Server timeout (in seconds) - 20
- Max RADIUS request retries - 3

*** Multi-factor authentication is available when the RADIUS Status changes to Enabled.

7. Click `Enable`.

For AD Connector based Workspaces Environments:

1. Identify the IP address and port of your `RADIUS MFA server` and, your `AWS Managed Microsoft AD Connector Identifier`.

2. In the AWS Workspaces console navigation pane, select `Directories`.
3. Choose the `directory ID link` for your `AWS Managed Microsoft AD directory connector`.
4. On the Directories page, select the `Actions > Update Details`.
5. In the Multi-factor authentication section, click `Actions`, and then click `Enable`.
6. On the Multi-Factor Authentication section, provide the following values:

- RADIUS server DNS name (s) or IP address (s)
- Port - default 1812
- Shared secret code
- Confirm shared secret code
- Protocol - MS-CHAPv2
- Server timeout (in seconds) - 20
- Max RADIUS request retries - 3

*** Multi-factor authentication is available when the RADIUS Status changes to Enabled.

7. Click `Update and Exit`

References:

1. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_mfa.html
2. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_mfa.html
3. https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

2.3 Ensure WorkSpace volumes are encrypted. (Automated)

Profile Applicability:

- Level 1

Description:

Encrypt WorkSpaces root volume (C:drive for Windows and root for Amazon Linux) and user volume (D:drive for Windows and /home for Amazon Linux).

Rationale:

When you launch a WorkSpace, you can encrypt the root volume and the user volume. This ensures that the data stored at rest for WorkSpaces is encrypted.

Impact:

You must encrypt a WorkSpace when it is launched You cannot create a custom image from an encrypted WorkSpace You cannot disable encryption once encryption is enabled for a WorkSpace You must enable to AWS KMS CMK prior to rebuilding/rebooting an encrypted WorkSpace or it becomes unusable.

Audit:

Perform the following steps to confirm that data at rest is encrypted for WorkSpaces
From the Console:

1. Login to the WorkSpaces dashboard at `https://console.aws.amazon.com/workspaces/`.
2. In the left pane click `WorkSpaces` to access the instances listing page.
3. Check the storage volume(s) encryption status for each Amazon WorkSpaces instance available in the current AWS region

- It will be listed in the Volume Encryption column

If the value listed in the Volume Encryption column is Disabled, the selected AWS WorkSpaces instance volumes are not encrypted.

4. Change the AWS region from the navigation bar and repeat step 3 for all other regions.

From the Command line:

1. Run describe-workspaces command (OSX/Linux/UNIX) using custom query filters to list the IDs of all AWS WorkSpaces instances available within the selected region:

```
aws workspaces describe-workspaces --region us-east-1 --output table --query
'Workspaces[*].WorkspaceId'
```

2. The command output should return a table with the requested WorkSpaces IDs:

```
--------------------
|DescribeWorkspaces|
+------------------+
|   ws-aaabbbccc   |
|   ws-cccceeefff  |
+------------------+
```

3. Execute again describe-workspaces command (OSX/Linux/UNIX) using the name of the WorkSpaces instance as identifier and custom query filters to get the encryption status for both root and user storage volumes:

```
aws workspaces describe-workspaces --region us-east-1 --workspace-ids ws-
aaabbbccc --query
'Workspaces[*].[RootVolumeEncryptionEnabled,UserVolumeEncryptionEnabled]'
```

4. The command output should return the encryption status (flag) for both root and user instance volumes (true for enabled, false for disabled):

```
[
    [
        false,
        false
    ]
]
```

If the returned flag value for both root and user volumes is false (as shown in the output example above), the selected AWS WorkSpaces instance volumes are not encrypted.

5. Repeat step 3 and 4 to verify the storage volumes encryption status for other AWS WorkSpaces instances provisioned in the current region.
6. Change the AWS region by updating the --region command parameter value and repeat steps 1 - 5 to perform the audit process for other regions.

If the selected AWS WorkSpaces instance volumes are not encrypted, refer to the remediation procedure below.

Remediation:

Perform the following steps to encrypt WorkSpace volumes
From the Console:

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. Click `Launch WorkSpaces` and complete the first three steps.
3. For the WorkSpaces Configuration step, do the following:

```
   - Select the volumes to encrypt: Root Volume, User Volume, or both
volumes.

   - For Encryption Key, select an AWS KMS CMK. The CMK that you select must
be symmetric.
```

4. Click `Next Step`.
5. Click `Launch WorkSpaces`.

NOTE:
To encrypt existing AWS WorkSpaces data you must re-create the necessary WorkSpaces instances with the volumes encryption feature enabled as outlined above.
From the Command line:

1. Run the `create-workspaces` command

```
aws workspaces create-workspaces --workspaces DirectoryId=`your_directoryID`,
UserName=`user_for_workspace`, BundleId=`bundle_to_build`,
VolumeEncryptionKey=`AWS_KMS_customer_master_key_(CMK)`,
UserVolumeEncryptionEnabled=`true`, RootVolumeEncryptionEnabled='true',
WorkspaceProperties={RunningMode=`AUTO_STOP`,
RunningModeAutoStopTimeoutInMinutes=`10`, RootVolumeSizeGib=`root_GB`,
UserVolumeSizeGib=`user_GB`, ComputeTypeName=`STANDARD`}
```

2. You will receive output highlighting:

```
- FailedRequests - Will contain information about the WorkSpaces that could
not be created, and the command failed
- PendingRequests - Will contain information about the WorkSpaces that were
created and the command was successful.
```

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/encrypt-workspaces.html
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/data-protection.html

3. https://docs.aws.amazon.com/kms/latest/developerguide/viewing-keys-console.html#viewing-console-details

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest
Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

2.4 Ensure WorkSpaces are deployed in their own virtual private cloud (VPC) (Manual)

Profile Applicability:

- Level 1

Description:

Amazon WorkSpaces VPC should be created with two private subnets for your WorkSpaces and a NAT gateway in a public subnet.

Rationale:

The NAT gateway will provide WorkSpaces access to the internet for updates to the operating system and so that applications can be deployed using Amazon WorkSpaces Application Manager if that is applicable for your environment.

Impact:

Your VPC's subnets must be in different Availability Zones in the Region where you're launching WorkSpaces.

Audit:

Perform the following steps to confirm that a VPC exists for WorkSpaces and is configured correctly.

From the Console:

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Your VPC's`
3. Select the VPC for WorkSpaces
4. Confirm the IPv4 settings are using a CIDR block from the private (non-publicly routable) IP address ranges. For example, 10.0.0.0/16. For more information, see the references below.
5. Confirm the IPv6 CIDR Block, set to `No`.
6. Confirm the IPv4 CIDR block for the Public subnet (example - WorkSpaces Public Subnet)

- Availability Zone, set to `No Preference`.

7. Confirm the IPv4 CIDR block for the first private subnet (example - WorkSpaces Private Subnet 1)

```
- Availability Zone, set for Amazon WorkSpaces.

- Elastic IP Allocation ID

- Service endpoints - `Blank`

- Enable DNS hostnames, set to `Yes`.

- Hardware tenancy, Default.
```

8. Confirm the IPv4 CIDR block for the first private subnet (example - WorkSpaces Private Subnet 2)

```
- Availability Zone set for Amazon WorkSpaces.
NOTE-Make sure you select a different Availability Zone from the one you
selected for the Workspaces Private Subnet 1

- Elastic IP Allocation ID

- Service endpoints - Blank

- Enable DNS hostnames, set to `Yes`.

- Hardware tenancy, Default.
```

If this is not set as referenced above refer to the remediation procedure below.

Remediation:

Perform the following steps to create a VPC for Workspaces
From the Console:
Allocate an Elastic IP Address

1. Login in to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Elastic IPs`.
3. Click `Allocate new address`.
4. On the Allocate new address page, for iPv4 address pool, click `Amazon pool or Owned by me`
5. Click `Allocate`.
6. Make a note of the Elastic IP address, click `Close`.

Create a VPC with one public subnet and two private subnets as follows.

1. Login in to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `VPC Dashboard` in the upper-left corner.
3. Click `Launch VPC Wizard`.

4. Click `VPC with Public and Private Subnets`
5. Click `Select`.
6. Configure the VPC as follows:

```
- For IPv4 CIDR block, enter the CIDR block from the private (non-publicly
routable) IP address ranges. - example 10.0.0.0/16.
- For IPv6 CIDR Block, keep `No IPv6 CIDR Block`.
- For VPC name, enter a `name for the VPC` (example: WorkspacesVPC)
- Public subnet's IPv4 CIDR - enter a CIDR block from the private (non-
publicly routable) IP address range - ie. 10.0.0.0/24.
- For Availability Zone, keep `No Preference`.
- For Public subnet name, enter a `name for the subnet` (example: WorkSpaces
Public Subnet).
- For Private subnet's IPv4 CIDR, enter the CIDR block for the subnet.
- `Availability Zone` - Accept the default value - No Preference
- For Private subnet name, enter a `name for the subnet` (example: WorkSpaces
Private Subnet 1).
- For Elastic IP Allocation ID, enter the Elastic IP address that you
created.
- For Service endpoints, `do nothing`.
- For Enable DNS hostnames, keep `Yes`.
- For Hardware tenancy, keep `Default`.
```

7. Click Create VPC. Note that it takes several minutes to set up your VPC. After the VPC is created.
8. Click `OK`.

Create a Second Private Subnet

1. In the left pane, click `Subnets`.
2. Click `Create Subnet`.

```
- For Name tag, enter a `name for the private subnet` (example: WorkSpaces
Private Subnet 2).
- For VPC, `select the VPC` that you created.
- For Availability Zone. Make sure you select a different Availability Zone
from the one used in WorkSpaces Private Subnet 1.
- For IPv4 CIDR block, enter the CIDR block for the subnet.
```

3. Click `Create`.

Verify and Name the Route Tables for Public

1. In the left pane, click `Subnets`
2. Click the `public` subnet that you created. (example: WorkSpaces Public Subnet)
3. On the Route Table tab, choose the ID of the route table (example: rtb-12345678).
4. Click the route table.
5. Under Name, choose the edit icon, `enter a name` (example: workspaces-public-routetable)

6. Click the check mark to save the name.
7. On the Routes tab, verify that there is one route for local traffic and another route that sends all other traffic to the internet gateway for the VPC.

Verify and Name the Route Tables for Private

1. In the left pane, click `Subnets`
2. Click the `private subnet 1` that you created. (example: WorkSpaces Private Subnet 1)
3. On the Route Table tab, choose the ID of the route table (example: rtb-12345678).
4. Click the route table.
5. Under Name, choose the edit icon, `enter a name` (example: workspaces-private-routetable)
6. Click the check mark to save the name.
7. On the Routes tab, verify that there is one route for local traffic and another route that sends all other traffic to the NAT gateway.
8. Repeat steps 1-7 under `Verify and Name the Route Tables for Private' for` WorkSpaces Private Subnet 2`

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html
2. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html#vpc-sizing-ipv4
3. https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html

CIS Controls:

Version 7

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

2.5 Ensure WorkSpaces traffic is controlled and routed through a NAT Gateway. (Manual)

Profile Applicability:

- Level 1

Description:

A network address translation (NAT) gateway enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a direct connection with those instances.

Rationale:

WorkSpaces must have access to the internet so that you can install updates to the operating system and deploy applications.

Audit:

Perform the following steps to verify a NAT Gateway is configured and utilized.
From the Console:

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Route Tables`.
3. On the Route Table tab.
4. Select the public route table set for WorkSpaces.
5. Click the `Subnet Associations` Tab
6. Confirm that the Subnet ID is set to the WorkSpaces Public subnet.
7. De-select the public route table and select the WorkSpaces Private route table.
8. Click the `Subnet Associations` Tab
9. Confirm that the Subnet ID is set to the 2 WorkSpaces Private subnet.

If the Route tables aren't set for one route for local traffic and another route that sends all other traffic to the internet gateway for the VPC refer to the remediation procedure below.

Remediation:

Perform the following steps to create a NAT gateway
From the Console:

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `NAT Gateways`
3. Click `Create NAT Gateway`.

4. For NAT Gateway settings

```
- Name - although optional use something to identify it with WorkSpaces

- Specify the subnet in which to create the NAT gateway

- Select the Elastic IP Allocation ID
```

5. Click `Create a NAT Gateway`.

_The NAT gateway will display in the console and after a few moments, its status will change to Available.
If the NAT gateway goes to a status of Failed, there was an error during creation._
After you've created your NAT gateway, you must update your route tables for your private subnets to point internet traffic to the NAT gateway.
To create a route for a NAT gateway

1. Log in to the VPC console at `https://console.aws.amazon.com/vpc/`.
2. In the left pane, Click `Route Tables`.
3. Select the route table associated with your private subnet.
4. Click `Routes` tab.
5. Click `Edit routes`
6. Click `Add route`
7. For Edit routes

```
- Destination, enter 0.0.0.0/0.

- Target, select the ID of your NAT gateway.
```

8. Click `Save routes`

References:

1. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html

Additional Information:

Note In some multi-account AWS architectures organizations may choose to leverage a centralized internet egress pattern. This could be due to appliances running in the centralized pattern which are being used to enforce controls and could include DLP or category filtering on internet egress traffic. In this case the relevant audit procedure is ensuring the workspaces VPC has a route to the internet (either via proxy server configuration on the workspace instances themselves or the default route on the workspace instance VPC subnet)

CIS Controls:

Version 7

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

14.2 Enable Firewall Filtering Between VLANs
Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

2.6 Ensure Web Access to Workspaces is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

WorkSpaces access should be restricted to trusted operating systems and clients

Rationale:

WorkSpaces access is supported from a variety of clients and operating systems, including HTML5 based browsers. Disabling Web Access prevents access to the Workspace from HTML5 based browsers, ensuring access can only occur from known operating systems.

Audit:

Perform the following steps to confirm that Web Access is disabled.
From the Console:

1. Log in to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select the directory and then click `Actions`, `Update Details`.
4. Expand `Access Control Options`.
5. Confirm that `Web Access` is unchecked.

If everything is not configured as above refer to the remediation below.

Remediation:

Perform the following steps to disable Web Access.
From the Console:

1. Log in to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select the directory and then click `Actions`, `Update Details`.
4. Expand `Access Control Options`.
5. Uncheck `Web Access`.
6. Click `Update and Exit`

Default Value:

Disabled

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/web-access.html

CIS Controls:

Version 7

12.12 Manage All Devices Remotely Logging into Internal Network
Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

2.7 Ensure access is limited to trusted devices. (Manual)

Profile Applicability:

- Level 2

Description:

WorkSpaces access should be restricted to trusted devices with valid certificates.

Rationale:

WorkSpaces is accessible from any supported device that is connected to the internet. When you enable access to trusted devices, Amazon WorkSpaces uses certificate-based authentication to determine whether a device is trusted.

Impact:

For each directory, you can import up to two root certificates and Amazon WorkSpaces will present them both to the client.

Note: Certificates for trusted devices only applies to the Amazon WorkSpaces OS clients. This feature does not apply to the Amazon WorkSpaces Web Access client, or any third-party clients.

Audit:

Perform the following steps to confirm that Allow Trusted Devices is set.
From the Console:

1. Log in to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select the directory and then click `Actions`, `Update Details`.
4. Expand `Access Control Options`.
5. Confirm that the correct `Allow` settings are in place.
6. Confirm that certificates have been imported
7. Confirm that the correct device types have been enabled.

If everything is not configured as above refer to the remediation below.

Remediation:

Perform the following steps to set the restriction Allow Trusted Devices
Create the Certificates

Note - It requires root certificates generated by an internal Certificate Authority (CA) and client certificates that chain up to a root certificate.

```
Requirements
- Certificates must be Base64-encoded certificate files in CRT, CERT, or PEM
format.
- Certificates must include a Common Name.
- The maximum length of certificate chain supported is 4.
- Use a strong encryption algorithm. Minimum SHA256 with RSA, SHA256 with
ECDSA. Other options SHA381 with ECDSA, or SHA512 with ECDSA.
- Make sure "key usage: Digital signature" is present on the public key.
- For macOS, if the device certificate is in the system keychain, authorize
the WorkSpaces client application to access those certificates.
```

Deploy Client Certificates to the Trusted Devices

```
- Client certificates must be installed on the trusted devices for your
users.
Utilize a third party tool to install the certificates or have the
certificates installed locally by an administrator.
- On Windows, the WorkSpaces client application searches for client
certificates in both the user and root certificate stores.
- On macOS, the WorkSpaces client application searches for client
certificates in the entire keychain.
```

Configure the Restriction

From the Console:

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select the directory.
4. Click `Actions`, `Update Details`.
5. Expand `Access Control Options`.

```
        - [Windows] Choose Only Allow Trusted Windows Devices to Access
WorkSpaces.
        - [macOS] Choose Only Allow Trusted macOS Devices to Access
WorkSpaces.
```

5. Import up to two root certificates. For each root certificate, do the following:

```
         - Choose Import.
         - Copy the body of the certificate to the form.
         - Choose Import.
         (Optional) Specify whether other types of devices have access to
WorkSpaces.
```

6. Scroll down to the Other Platforms section.

7. Select the device types allowed to enable and clear the device types not allowed to disable.
8. To block access from all selected device types, click `Block`.
9. Click `Update and Exit`.

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/trusted-devices.html
2. https://docs.aws.amazon.com/acm/latest/userguide/gs.html
3. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_server-certs.html

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.8 Ensure the default IP access control group is disassociated. (Automated)

Profile Applicability:

- Level 1

Description:

The default IP Access Control group allows all traffic. Once you create and attach an IP Access Control Group the default is disassociated.

Rationale:

IP Access Control group acts as a virtual firewall for your WorkSpaces allowing you to add your trusted networks.

Impact:

IP access control groups do not allow the use of dynamic IP addresses when using a NAT gateway and additional configuration has to be considered.

Audit:

Perform the following steps to review your Directory
From the Console:

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select your `Directory`.
4. Click on `Actions`.
5. Click on `IP Access Control Groups`
6. Confirm that you have an IP Access Control Group Associated with this Directory.
7. Make note of the `name(s)` of the IP Access Control Group.
8. Next review the IP Access Control Group
9. In the navigation pane, click `IP Access Controls`.
10. Select the name of the `IP Access Control Group(s)` you record from the Directory.
11. For each IP Access Control Group confirm the source IP address or IP address range, and the Description.

If an IP Access Control group doesn't exist follow the remediation below.
From the Command line:
Run the `describe-ip-groups` command

```
aws workspaces describe-ip-groups
```

Review the output for the name and the IP Access controls.
If an IP Access Control group doesn't exist refer to the remediation below.

Remediation:

Perform the steps below to create an IP Access control group.
From the Console.

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, Click `IP Access Controls`.
3. Click `Create IP Group`.
4. In the `Create IP Group` dialog box, enter a name and description for the group.
5. Click `Create`.
6. Select the group
7. Click `Edit`.
8. For each IP address, click `Add Rule`.
9. For Source, enter the IP address or IP address range.
10. For Description, enter a description.

When you are done adding rules,

11. Click `Save`.

Next Associate an IP Access Control Group with a Directory

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select the directory and click `Actions`, `Update Details`.
4. Expand IP Access Control Groups and select one or more IP access control groups.
5. Click `Update and Exit`.

Note - If you associate an IP access control group that has no rules with a directory, this blocks all access to all WorkSpaces.*
From the command line:
Run the `create-ip-group` command

```
aws workspaces create-ip-group --group-name name-of-group --user-rules
ipRule=ipaddress_list
```

Associate an IP Access Control Group with a Directory
Run the 'associate-ip-groups' command

```
aws workspaces associate-ip-groups --directory-id directory_ID --group-ids
IDs_of_IP_access_ctrl_group
```

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html
2. https://docs.aws.amazon.com/cli/latest/reference/workspaces/create-ip-group.html
3. https://awscli.amazonaws.com/v2/documentation/api/latest/reference/workspaces/index.html#cli-aws-workspaces

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.9 Ensure CloudWatch is set up for WorkSpaces. (Manual)

Profile Applicability:

- Level 1

Description:

Set up and utilize Amazon CloudWatch Events for successful logins to WorkSpaces.

Rationale:

Use Cloudwatch to store/archive WorkSpaces login events for future reference, analysis, and action based on the patterns. Utilize the IP address collected to figure out where users are logged in from, and then build policies to allow access only to files or data from those WorkSpaces that meet company access criteria. With this information you can also use policy controls to block access from unauthorized IP addresses.

Audit:

Perform the following steps to review the rules for CloudWatch and WorkSpaces Events
From the Console:

1. Login to the CloudWatch console at `https://console.aws.amazon.com/cloudwatch/`
2. In the left pane click `Events`.
3. Click `Rules`.
4. Click on the Rule Name for your WorkSpaces Access Events
5. Confirm the `Event Pattern`

```
{
  "source": [
    "aws.workspaces"
  ],
  "detail-type": [
    "WorkSpaces Access"
  ]
}
```

6. Confirm Status is `Enabled`
7. Confirm at least one Target is created for `CloudWatch Log Group`

If there is no CloudWatch Event created with the rule as outlined above refer to the remediation below.

Remediation:

Perform the following steps to create a Rule for CloudWatch WorkSpaces Events
From the Console:

1. Login to the CloudWatch console at `https://console.aws.amazon.com/cloudwatch/`
2. In the left pane click `Events`.
3. Click `Create rule`.
4. For Event Source, do the following:

```
- Click `Event Pattern` and Build event pattern to match events by service
(the default).
```

5. For Service Name, click `WorkSpaces`.
6. For Event Type, click `WorkSpaces Access`.
7. For Targets, click `Add target`

```
- Click and Change the Lambda Function to `CloudWatch log group`
```

8. For Log Group, enter /aws/events/workspaces_access

Note - You can add additional targets for other services to act when a WorkSpaces Access event is detected.

9. Click `Configure details`.
10. For Rule definition, `enter a name and description`.
11. Click `Create rule'
12. Click `Create rule`.

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-monitoring.html
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/cloudwatch-events.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

2.10 Ensure that patches and updates are performed on the operating system for Workstations. (Automated)

Profile Applicability:

- Level 1

Description:

In order for Windows updates to occur auto-stop WorkSpaces must be utilized and the default for maintenance mode must be set to enabled.

Rationale:

Windows Operating systems updates can be a high security vulnerability and normal updates and patches can help eliminate these vulnerabilities.

Audit:

Perform the steps to check maintenance mode for your WorkSpaces:
From the Console:

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select your directory.
4. Click `Actions`, `Update Details`.
5. Expand `Maintenance Mode`.

If it is set to `Enabled` you are meeting this recommendation.
If it is set to `Disabled`, refer to the remediation below.
From the Command line:

1. Run the workspaces command `describe-workspace-directories`

```
aws workspaces describe-workspace-directories
```

2. Review the output under "WorkspaceCreationProperties" for "EnableMaintenanceMode" : true

```
Example output:
      "WorkspaceCreationProperties" :
      {
        "EnableInternetAccess" : false,
        "EnableWorkDocs" : true,
        "UserEnabledAsLocalAdministrator" : true
        "EnableMaintenanceMode" : true
      },
```

If it is set to `true` you are meeting this recommendation.
If it is set to `false` or is not listed in the output at all, refer to the remediation below.

Remediation:

Perform the following steps to enable maintenance mode
From the Console:

1. Login to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select your directory.
4. Choose `Actions`, `Update Details`.
5. Expand `Maintenance Mode`.
6. To enable automatic updates, choose `Enabled`.
7. Click `Update and Exit`.

Note**
If you prefer to manage updates manually or with another tool document usage of that, and choose Disabled.
From the Command line:

1. Run the WorkSpaces modify-workspace-creation-property command

```
aws workspaces modify-workspace-creation-property --resource-id
<directory_id> --workspace-creation-properties EnableMaintenanceMode=true
```

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/workspace-maintenance.html
2. https://awscli.amazonaws.com/v2/documentation/api/latest/reference/workspaces/modify-workspace-creation-properties.html

CIS Controls:

Version 7

2.2 Ensure Software is Supported by Vendor
Ensure that only software applications or operating systems currently supported by the

software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

3 Continuous Vulnerability Management

Continuous Vulnerability Management

2.11 Ensure your WorkSpaces image has the appropriate CIS Operating System Benchmark applied (Manual)

Profile Applicability:

- Level 1

Description:

Utilize the CIS Benchmark to secure the Operating system image that you are utilizing for your WorkSpaces.

Rationale:

Securing the Operating system with a CIS Benchmark ensures all systems remain in a secure, compliant and hardened state. Use the WorkSpace you applied the Benchmark to, to create an secure image for any deployments.

Audit:

Spin up a WorkSpaces instance and run a manual assessment by confirming the CIS Operating System Benchmark recommendations for the applicable operating system are applied. You can also utilize a 3rd Party Assessment tool that has been certified for the specific CIS Operating System Benchmark to automate this process.

Remediation:

Perform the steps below using the downloaded free version of the applicable CIS Operating System Benchmark and manually apply the recommendations for the WorkSpaces instance. Or Utilize a 3rd Party tool to assess and apply the CIS Operating System Benchmark.

1. Launch a WorkSpaces Bundle
2. Access that WorkSpace as an Administrator utilize SSH or RDP.
3. Apply the Benchmark:

```
- Manually

- Using Active Directory by creating a GPO that matches the Benchmark.

- Or using a Third Party tool that will apply the Benchmark recommendations.
```

4. Assess the WorkSpaces instance manually or with a 3rd Party tool.
5. Create a workspace bundle that can then be used to launch your production WorkSpaces instances.

References:

1. https://www.cisecurity.org/partners-vendor/
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/create-custom-bundle.html
3. https://docs.aws.amazon.com/workspaces/latest/adminguide/update-custom-bundle.html

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.12 Restrict WorkSpaces Bundle options to organization approved versions (Manual)

Profile Applicability:

- Level 1

Description:

Limit the existing WorkSpaces bundles that can be utilized and provisioned within your AWS account.

Rationale:

Limiting the type of AWS WorkSpaces bundle that can be utilized can address internal security and compliance requirements.

Audit:

Perform the following to ensure available workspace bundles are set.
From the Console:

1. Login to the WorkSpaces dashboard at `https://console.aws.amazon.com/workspaces/`.
2. In the left pane click `WorkSpaces` to access the instances listing page.
3. Check the bundle type value for each Amazon WorkSpaces instance available in the current AWS region, listed in Bundle column, e.g.
4. If the value listed in the `Bundle column` is the same for all listed resources, the WorkSpaces instances were launched using the approved bundle type.
5. Change the AWS region from the navigation bar and repeat step no. 4 for all other regions.

If the value listed in the `Bundle column` is not the same for all listed resources, the WorkSpaces instances were not launched using the approved bundle type, refer to the remediation procedure below.
From the Command line:

1. Run describe-workspaces command available within the selected region:

```
aws workspaces describe-workspaces
        --region us-east-1
        --output table
        --query 'Workspaces[*].WorkspaceId'
```

2 The command output should return a table with the requested WorkSpaces IDs:

```
-------------------
|DescribeWorkspaces|
+------------------+
|   ws-bbbdddeee   |
|   ws-aaabbbccc   |
|   ws-ccceeefff   |
+------------------+
```

3. Run describe-workspaces command again using the name of the WorkSpaces instance as identifier and custom query filters get the ID of the bundle used by the selected instance:

```
aws workspaces describe-workspaces
        --region us-east-1
        --workspace-ids ws-bbbdddeee
        --query 'Workspaces[*].BundleId'
```

4. The command output should return the requested WorkSpaces bundle ID:
   `[ "wsb-ccc333fff" ]`
5. Run describe-workspace-bundles command to describe the type of the bundle utilized by the selected AWS WorkSpaces instance:

```
aws workspaces describe-workspace-bundles
        --region us-east-1
        --bundle-ids wsb-ccc333fff
        --query 'Bundles[*].ComputeType.Name'
```

6. The command output should return the selected WorkSpaces bundle type:

```
[
    "PERFORMANCE"
]
```

7. Repeat steps no. 3 – 6 to verify the bundle type used by the rest of the AWS WorkSpaces instances created in the current region.
8. If the value listed for the `Bundle` is the same for all listed resources, the WorkSpaces instances were launched using the approved bundle type.
9. Repeat steps 1 – 8 to perform the entire audit process for all other AWS regions.

If the value listed in the `Bundle` output is not the same for all listed resources, the WorkSpaces instances were not launched using the approved bundle type, refer to the remediation procedure below.

Remediation:

Preform the following to limit the bundle type
Create the required AWS support case:
From the Console:

1. Login in to AWS Support Center dashboard at `https://console.aws.amazon.com/support/`.
2. Click `Create a case`.
3. For Case details:

```
- Type, choose `Account`

- Category, choose `Other Account Issues`

- Subject, "Limit AWS WorkSpaces instances launch to approved bundle types".

- Description textbox, explain that security and compliance requires the need
to limit the provisioning of WorkSpaces instances to an approved bundle type.

- Contact options, leave as default or change as needed.
```

4. Click `Submit`

References:

1. https://aws.amazon.com/workspaces/faqs/
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-bundles.html
3. https://aws.amazon.com/workspaces/features/
4. https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

CIS Controls:

Version 7

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.13 Ensure Workspaces images are not older than 90 days. (Manual)

Profile Applicability:

- Level 1

Description:

WorkSpaces images should not have a creation time stamp over 90 days.

Rationale:

WorkSpaces images require Operating system patches to be applied and updated and by confirming the creation date is not over 90 days old can help ensure that updates are being applied.

Audit:

Perform the following to determine the age of WorkSpaces images.
From the Console:

1. Login to the WorkSpaces dashboard at `https://console.aws.amazon.com/workspaces/`
2. In the left pane click Images.
3. Review the Created date and confirm that all images are newer than 90 days.

If any images are older than 90 days refer to the remediation procedure below.

Remediation:

To create a custom image
From the Console:
Note - If you are still connected to the WorkSpace, disconnect.

1. Log in to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, choose `WorkSpaces`.
3. Select the WorkSpace and choose `Actions`, `Create Image`.

```
- A message displays, prompting you to restart your WorkSpace before
continuing. Restarting your WorkSpace updates your Amazon WorkSpaces software
to the latest version.
```

Once you have restarted your WorkSpace, repeat Step 4 of this procedure.

5. Click `Next`.
6. Enter an image name and a description.
7. Click `Create Image`. While the image is being created, the status of the WorkSpace is Suspended and the WorkSpace is unavailable.

In the left pane, click Images. The image is complete when the status of the WorkSpace changes to Available.

CIS Controls:

Version 7

3 Continuous Vulnerability Management
Continuous Vulnerability Management

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.14 Ensure WorkSpaces that are not being utilized are removed. (Automated)

Profile Applicability:

- Level 1

Description:

Identify and remove any WorkSpace instances available within your AWS account that are not being utilized.

Rationale:

An AWS WorkSpaces instance is considered unused if has 0 (zero) known user connections registered within the past 30 days.

Audit:

Perform the following to ensure WorkSpaces not being utilized have been removed.
From the Console:

1. Log in to the WorkSpaces dashboard at `https://console.aws.amazon.com/workspaces/`.
2. In the left panel click `WorkSpaces`
3. Choose the WorkSpaces instance that you want to examine.
4. Click on the down arrow to `Hide or Show Details`.
5. On the selected instance configuration details panel.

```
- Verify the User Last Active attribute value is less than 30 days old
```

6. Repeat steps 4 and 5 to verify the last user login, returned by the User Last Active attribute value, for all WorkSpaces.
7. Change the AWS region and repeat the audit process for other regions.

If the User Last Active was registered more than 30 days ago (e.g. Feb 16, 2017 10:32:54 UTC), the selected WorkSpaces instance is not in use anymore and can be safely removed from your AWS account. Refer to the remediation procedure below.
From the Command line:

1. Run the describe-workspaces command to list the IDs of all WorkSpaces instances available within the selected region:

```
aws workspaces describe-workspaces
        --region us-east-1
        --output table
        --query 'Workspaces[*].WorkspaceId'
```

2. The command should return a table with the requested WorkSpaces IDs:

```
--------------------
|DescribeWorkspaces|
+------------------+
|   ws-7cgsl2k65   |
|   ws-8d6il5kr3   |
|   ws-2dtyl1g47   |
+------------------+
```

3. Run the describe-workspaces-connection-status command using the ID of the WorkSpaces instance in the table output

```
aws workspaces describe-workspaces-connection-status
        --region us-east-1
        --workspace-ids ws-7cgsl2k65
        --query
'WorkspacesConnectionStatus[*].LastKnownUserConnectionTimestamp'
```

4. The command should return the timestamp of the User last active for the selected instance:

```
[
    1489139777.721
]
```

5. Run the date command using the timestamp value returned at the previous step to convert it to a human readable date value:

```
date -d @1489139777.721
```

6. Verify the User Last Active attribute value is less than 30 days old

```
Fri Mar 10 09:56:17 UTC 2017
```

If the User last active date returned is more than 30 days ago, the selected WorkSpaces instance is not utilized anymore and can be safely removed from your AWS account. Refer to the remediation procedure below to remove the WorkSpaces.

7. Repeat steps 3 – 6 to verify the User Last active date for the other WorkSpaces instances listed in the current region.
8. Change the AWS region by updating the --region command parameter value and repeat steps no. 1 – 7 to perform the entire audit process for other regions.

Remediation:

Perform the following to remove unused WorkSpaces based on the output collected from the audit procedure
From the Console:

1. Log in to WorkSpaces dashboard at `https://console.aws.amazon.com/workspaces/`.
2. In the left panel click `WorkSpaces`
3. Select the WorkSpace ID that you have identified as not being used.
4. Click `Actions`, `Remove WorkSpaces`
5. Confirm using the Audit that this is the WorkSpaces ID you should remove.
6. Click `Remove WorkSpaces`

From the Command line:
Note that running this command does not prompt you to confirm that you are removing the correct WorkSpaces ID.

1. Run terminate-workspaces command using the ID of the WorkSpaces instance from the Audit that you want to delete:

```
aws workspaces terminate-workspaces
       --region us-east-1
       --terminate-workspace-requests ws-0cgsl1k23
```

References:

1. https://aws.amazon.com/workspaces/faqs/
2. https://awscli.amazonaws.com/v2/documentation/api/latest/reference/workspaces/index.html#cli-aws-workspaces

CIS Controls:

Version 7

1.4 Maintain Detailed Asset Inventory
Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.

13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization
Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

2.15 Ensure primary interface ports for Workspaces are not open to all inbound traffic. (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that the inbound traffic of the primary network interface for all WorkSpaces is not open to all connections 0.0.0.0\00.

Rationale:

Attached security groups to the primary elastic network interface (ENI) to manage ports and network communication should not be open to all communication. They should be restricted to what is required by WorkSpaces, the Organization and other services.

Audit:

Perform the steps below to confirm security groups are configured correctly
From the console:

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Your VPCs`
3. Note the VPC Id for WorkSpaces
4. In the left pane, click `Security Groups`
5. In the `Filter security groups` enter the name of the WorkSpaces VPC
6. Select the WorkSpaces Security Group
7. Click on Inbound rules
8. Confirm that there is no rule for All traffic, All, All, 0.0.0.0/0, -

If there is a rule for Inbound traffic that is open to all traffic and all ip addresses refer to the remediation below.

Remediation:

Perform the steps below to remove Inbound rule that allows all traffic from all IP addresses.
From the console:

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Your VPCs`
3. Note the VPC Id for WorkSpaces

4. In the left pane, click `Security Groups`
5. In the `Filter security groups` enter the name of the WorkSpaces VPC
6. Select the WorkSpaces Security Group
7. Click on `Inbound rules`
8. Click on `Edit inbound rules`
9. Click on `Delete` for the rule that shows

```
-All traffic, All, All, 0.0.0.0/0, -
```

10. Click on Save rules

Note - Make sure you have all the required ports add to Inbound rules as listed in the WorkSpaces documentation outlined in the references so that connectivity to WorkSpaces is not impacted.

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-port-requirements.html#gateway_IP
2. https://aws.amazon.com/workspaces/resources/?workspaces-whats-new.sort-by=item.additionalFields.postDateTime&workspaces-whats-new.sort-order=desc
3. https://d1.awsstatic.com/whitepapers/workspaces/Best_Practices_for_Deploying_Amazon_WorkSpaces.pdf

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports
Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.16 Ensure FIPS Endpoint encryption is enabled for WorkSpaces. (Manual)

Profile Applicability:

- Level 2

Description:

To meet a high level of security and comply with different compliance standards, you must use Federal Information Processing Standards (FIPS) endpoint encryption at the directory level with WorkSpaces.

Rationale:

You must also use an AWS Region that is authorized for the same compliance standard that you are trying to achieve.

Audit:

Perform the steps below to determine if FIPS endpoint encryption is enabled.
From the Console:

1. Log in to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Select the directory.
4. Click the arrow to expand the Directory Details
5. Endpoint Encryption should read

```
- FIPS 140-2 Validated Mode.
```

If Endpoint Encryption is not listed as FIPS 140-2 Validated Mode refer to the remediation procedure below.

Remediation:

Perform the steps below to enable FIPS endpoint encryption at the directory level
From the Console:

1. Log in to the WorkSpaces console at `https://console.aws.amazon.com/workspaces/`
2. In the left pane, click `Directories`.
3. Verify that the directory does not have any existing WorkSpaces associated with it.

4. Select the directory.
5. Click Actions, `Update Details`.
6. Click the arrow to expand `Access Control Options`
7. For Endpoint Encryption, choose `FIPS 140-2 Validated Mode`.
8. Click `Update and Exit`.

You can now create WorkSpaces from this directory that utilize FIPS endpoint encryption modules.

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/fips-encryption.html
2. https://aws.amazon.com/compliance/services-in-scope/

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest
Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

2.17 Ensure WorkSpaces API requests flow through a VPC Endpoint (Automated)

Profile Applicability:

- Level 1

Description:

For any WorkSpaces API requests setup the connection through an interface endpoint in your VPC.

Rationale:

Utilizing a VPC interface endpoint for WorkSpaces API requests keeps the communication within the AWS network.

Impact:

This feature can only be used for connecting to WorkSpaces API endpoints.

Audit:

Perform the steps to determine if WorkSpaces is using a VPC endpoint for API
From the Command line:

1. Run the WorkSpaces `describe-workspace-budles' command

```
aws workspaces describe-workspace-bundles --endpoint-url
VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com
```

2. Example output of that command:

```
--endpoint-name Endpoint_Name
--body "Endpoint_Body"
--content-type "Content_Type"
 Output_File
```

Confirm the --endpoint-name is equal to the VPC Endpoint that you have created. If the endpoint name does not match what you created or is blank, refer to the remediation below.

Remediation:

Perform the steps below if you need to create a VPC interface endpoint.
From the Console

1. Log in to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Endpoints`
3. Click `Create Endpoint`.
4. For Service category, ensure that AWS services is selected.
5. For Service Name, choose Workspaces. For Type, ensure that it indicates Interface.
6. Complete the following information.

```
- For VPC, select a VPC in which to create the endpoint.

- For Subnets, select the subnets (Availability Zones) in which to create the
endpoint network interfaces.  Not all Availability Zones may be supported for
all AWS services.

- To enable private DNS for the interface endpoint, for Enable Private DNS
Name, select the check box.

- For Security group, select the security groups to associate with the
endpoint network interfaces.
```

8. Click `Create endpoint`

From the Command line

1. Run the create-vpc-endpoint command

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type
Interface --service-name com.amazonaws.us-east-1.elasticloadbalancing --
subnet-id subnet-abababab --security-group-id sg-1a2b3c4d
```

In the output that's returned, take note of the DnsName fields. You can use these DNS names to access the AWS service.
Next perform the steps to add the Endpoint to the WorkSpace image
From the Command line

1. Run the copy-workspace-image command including the endpoint url you just created.

```
aws workspaces copy-workspace-image --endpoint-url
VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com
```

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/infrastructure-security.html
2. https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html#create-interface-endpoint

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

13.3 Monitor and Block Unauthorized Network Traffic
Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

2.18 Ensure Radius server is using the recommended security protocol (Automated)

Profile Applicability:

- Level 2

Description:

The authentication protocol between the Microsoft AD DCs and the RADIUS server supported are PAP, CHAP, MS-CHAPv1, and MS-CHAPv2.

Rationale:

MS-CHAPv2 provides the strongest security of the options supported.

Audit:

Perform the steps to check multi-factor authentication using the radius server protocol is set to MS-CHAP v2.
From the Console:
For AWS Managed AD based environments;

1. Log in to the Directory Service console at `https://console.aws.amazon.com/directoryservicev2`
2. In the left pane select `Directories`.
3. Choose the directory ID link for your AWS Managed Microsoft AD directory.
4. On the Directory details page, select the `Networking & security` tab.
5. In the Multi-factor authentication section, confirm that the Protocol is set to MS-CHAPv2.

For directory connector / self-managed AD environments

1. Log in to the AWS Workspaces console at `https://console.aws.amazon.com/workspaces`
2. In the left pane select `Directories`.
3. Select the directory ID link for your AWS Managed Microsoft AD directory.
4. On the `Directories` page, select the `Actions > Update Details`.
5. In the Multi-factor authentication section confirm that, in the `Protocol` field `MS-CHAPv2` is selected from the dropdown list.

If it is not set to `MS-CHAPv2` refer to the remediation steps below.

Remediation:

Perform the steps below to set the protocol to MS-CHAPv2 for multi-factor authentication.
From the console:
For AWS Managed AD based environments;

1. Log in to the Directory Service console at `https://console.aws.amazon.com/directoryservicev2`
2. In the left pane select `Directories`.
3. On the Directory details page, select the `Networking & security` tab.
4. In the Multi-factor authentication section, choose `Actions`, and then choose `Edit`.
5. On the Enable multi-factor authentication (MFA) page change the following value:
6. Protocol - `MS-CHAPv2`
7. Click `Save`.

For directory connector / self-managed AD environments

1. Log in to the AWS Workspaces console at `https://console.aws.amazon.com/workspaces`
2. In the left pane select `Directories`.
3. Select the directory ID link for your AWS Managed Microsoft AD directory.
4. On the Directories page, select the `Actions > Update Details`.
5. In the Multi-factor authentication section modify the protocol using the `dropdown` menu to be `MS-CHAPv2` from the currently selected option.
6. Click `Update and exit` once settings are as desired.

References:

1. https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/
2. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_mfa.html

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

3 WorkDocs

This section contains recommendations for configuring the WorkDocs service and any additional resources required.

3.1 Ensure Administrators of WorkDocs is defined using IAM (Automated)

Profile Applicability:

- Level 1

Description:

To allow users to administer Amazon WorkDocs resources, you must create an IAM policy that explicitly grants them the correct permissions. This policy should then be attached to the group or role defined for this administration.

Rationale:

WorkDocs Administrators control access and authorization for users of the WorkDocs resources.

Audit:

Perform the following to determine what policies are created:
From the Console:

1. Login in and open the IAM console at `https://console.aws.amazon.com/iam/`.
2. In the left pane click on `Groups`.
3. Click on the group name that should administer WorkDocs.
4. Click on Permissions and confirm that the AmazonWorkDocsFullAccess policy is attached.
5. Click on Users and confirm that the list of names are the users approved to administer WorkDocs.
6. To confirm that the WorkDocs policy (AmazonWorkDocsFullAccess) for admin control is attached to the correct group.

From the Command Line:

1. Run the list-attached-group-policies.

```
aws iam list-attached-group-policies --group-name <workdocs_group_name>
```

2. Confirm that the list of users in that Group is correct

```
aws iam get-group --group-name <workdocs_group_name>
```

If the AWS manage policy or a custom WorkDocs Full Access policy is not attached to the group or the users in the group list is not correct refer to the remediation below.

Remediation:

Perform the following to create an IAM group and assign the Amazon WorkDocs Full Access policy to it:
From the Console:

1. Log in to the IAM console at `https://console.aws.amazon.com/iam/`.
2. In the left pane, click `Groups` and then click `Create New Group`.
3. In the Group Name box, type the name of the group and then click `Next Step`.
4. In the list of policies, select the check box for `AmazonWorkDocsFullAccess`
5. Click `Next Step`.
6. Click `Create Group`

Perform the following to add a user to a Amazon WorkDocs Full Access group:

1. Log in to the the IAM console at `https://console.aws.amazon.com/iam/`.
2. In the left pane, click `Groups`
3. Select the group you created above
4. Click `Add Users To Group`
5. Select the users to be added to the group
6. Click `Add Users`

References:

1. https://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-access-control.html
2. https://docs.aws.amazon.com/workspaces/latest/adminguide/manage-workspaces-users.html

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts
Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

3.2 Ensure MFA is enable for WorkDoc users (Manual)

Profile Applicability:

- Level 2

Description:

Multi-Factor Authentication (MFA) adds an extra layer of authentication assurance beyond traditional username and password. With MFA enabled, when a user signs in to Amazon WorkDocs, they will be prompted for their user name and password as well as for an authentication code from their MFA token.

Rationale:

Enabling MFA provides increased security to a user name and password as it requires the user to possess a solution that displays a time-sensitive authentication code.

Impact:

To enable MFA for Amazon WorkDocs you require a RADIUS server or a plugin to a RADIUS server already implemented in your environment.

Multi-factor authentication is not available for Simple AD.

You can enable multi-factor authentication for AD Connector if you have Active Directory running on-premises or in EC2 instances.

Audit:

Perform the steps below to confirm MFA setup and configuration.
From the console:

1. Log in to the Directory Service console at `https://console.aws.amazon.com/directoryservicev2`
2. Select `Directories`.
3. Choose the directory ID link for your AWS Managed Microsoft AD directory.
4. On the Directory details page, select the `Networking & security tab`.
5. In the Multi-factor authentication section, Confirm Radius status is set to Enabled.
6. Open the WorkDocs console at `https://console.aws.amazon.com/zocalo/`
7. In the Manage Your WorkDocs Sites page, select the desired site and choose `Actions` and `Manage MFA`.
8. Confirm the values are set correctly.

Multi-factor authentication is available when the RADIUS Status reads Enabled.
From the Command line:

1. Run describe-directories command to list the identifiers of all the Active Directory (AD) Connector directories, available in the selected AWS region:

```
aws ds describe-directories
        --region us-east-1
        --output table
        --query 'DirectoryDescriptions[*].DirectoryId'
```

2. The command output should return a table with the requested resource IDs:

```
---------------------
|DescribeDirectories|
+-------------------+
|   d-12345abcde    |
|   d-abcd012345    |
|   d-aabbcc1234    |
+-------------------+
```

3. Run describe-directories command using the ID of the AD Connector directory to get the status of the RADIUS MFA server connection:

```
aws ds describe-directories
        --region us-east-1
        --directory-ids d-12345abcde
        --query 'DirectoryDescriptions[*].RadiusStatus'
```

4. The command output should return the requested status information:

```
[]
```

5. Repeat steps 3 and 4 to determine the MFA status for other AD Connector directories.
6. Change the AWS region by updating the --region command parameter value and repeat steps 1 – 5 to perform the audit process for other regions.

If describe-directories command output returns an empty array, as shown in the example above, there is no RADIUS MFA server configured for the selected AD Directory, therefore the resource does not have Multi-Factor Authentication (MFA) protection enabled. Refer to the remediation below.

Remediation:

Perform the following steps to setup MFA on the server and in WorkDocs.
From the Console:

1. Identify the IP address of your RADIUS MFA server and your AWS Managed Microsoft AD directory.
2. In the AWS Directory Service console navigation pane, select Directories.
3. Choose the directory ID link for your AWS Managed Microsoft AD directory.
4. On the Directory details page, select the Networking & security tab.
5. In the Multi-factor authentication section, choose Actions, and then choose Enable.
6. On the Enable multi-factor authentication (MFA) page, provide the following values:

```
- Display label - Provide a label name.

- RADIUS server DNS name or IP addresses

- Port - default 1812

- Shared secret code

- Confirm shared secret code
```

To enable multi-factor authentication in WorkDocs:

1. Open WorkDocs console at `https://console.aws.amazon.com/zocalo/`
2. In the Manage Your WorkDocs Sites page, select the desired site and choose `Actions` and `Manage MFA`.
3. Enter the following values:

```
- Enable Multi-Factor Authentication

- Check to enable multi-factor authentication.

- RADIUS server IP address(es) - The IP addresses of your RADIUS server
endpoints

- Port - The port that your RADIUS server is using for communications.
Default RADIUS server port (1812)

- Shared secret code - The shared secret code that was specified when your
RADIUS endpoints were created.

- Confirm shared secret code

- Protocol - MS-CHAPv2

- Server timeout - (in seconds) - 20

- Max retries - 3
```

4. Choose Enable.

Multi-factor authentication is available when the RADIUS Status changes to Enabled.
To enable RADIUS-based MFA protection for your Active Directory (AD) Connector

directories, perform the following actions:
Note: Enabling Multi-Factor authentication for AD Connector directories using the AWS Management Console is not currently supported.

From the Command line:

1. Run the enable-radius command:

```
aws ds enable-radius --region us-east-1 --directory-id <value> --radius-settings { "RadiusServers": ["radius.<your-radius-server>.com"],"RadiusPort": 1812,"RadiusTimeout": 20,"RadiusRetries": 3,"SharedSecret": "radiusmfa","AuthenticationProtocol": "MS-CHAPv2","DisplayLabel": "RADIUS Multi-Factor Authentication","UseSameUsername": true }
```

2. Repeat step 1 for other AD Connectors and the Selected regions.

References:

1. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_mfa.html
2. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_mfa.html
3. https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

3.3 Ensure Workdocs access is limited to a range of allowable IP addresses. (Manual)

Profile Applicability:

- Level 1

Description:

Access to WorkDocs can be limited to an allowed range of IP addresses.

Rationale:

Using IP address allow lists, you define and permit access to your WorkDocs site from trusted networks.

Impact:

IP Lists currently only work for IPv4 addresses and denying access through an IP list is not supported.

Audit:

Perform these steps to review the list of IP addresses allowed to access WorkDocs
From the Console:

1. Log in to the WorkDocs Console at `https://console.aws.amazon.com/zocalo/`
2. Under My Account, choose `Open admin control panel`.
3. For IP Allow List, choose `Change`.
4. Review the IP address ranges and any single IP addresses
5. Click `Cancel`.

If the IP address ranges do not match trusted networks refer to the remediation below to create or edit the IP Allow list.

Remediation:

Perform the steps below to create or edit the IP Allow list for WorkDocs
From the Console:

1. Log in to the WorkDocs Console at `https://console.aws.amazon.com/zocalo/`
2. Under My Account, choose `Open admin control panel`.
3. For IP Allow List, choose `Change`.

4. For Enter CIDR value, enter the IP address ranges to `allowlist`. To allow access from a single IP address, specify /32 as the CIDR prefix.
5. Click `Add`.
6. Click `Save Changes`.

References:

1. https://docs.aws.amazon.com/workdocs/latest/adminguide/prereqs.html
2. https://aws.amazon.com/about-aws/whats-new/2018/10/amazon-workdocs-control-ip-address-access/
3. https://docs.aws.amazon.com/workdocs/latest/adminguide/workdocs-ag.pdf

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.4 Utilize site wide activity feed for monitoring. (Manual)

Profile Applicability:

- Level 1

Description:

Admins can view and export the activity feed for an entire WorkDocs site.

Rationale:

WorkDoc admins should monitor and export activity feeds for the site as record of activity. These activity reports should be reviewed every month for any abnormalities and rotated every 90 days.

Impact:

To use this feature, you must first install the Amazon WorkDocs Companion.

Audit:

Perform the steps below to view site-wide activity feed
From the WorkDocs web application:

1. Click `Activity feed`.
2. Click Filter, then Click `Site-wide activity`.
3. Select Activity Type filters and choose `Date Modified` settings as needed, then click `Apply`.
4. When the filtered activity feed results appear, search by file, folder, or user name to narrow your results. You can also add or remove filters as needed.

Remediation:

Perform the following steps to Export site-wide activity feed
From the WorkDocs web application:

1. Click `Activity feed`.
2. Click Filter, then Click `Site-wide activity`.
3. Select Activity Type filters and choose `Date Modified` settings as needed, then click `Apply`.
4. When the filtered activity feed results appear, search by file, folder, or user name to narrow your results. You can also add or remove filters as needed.
5. Click `Export`

6. Export the activity feed as a .csv or .json file. Any filters you applied are reflected in the exported file.

References:

1. https://docs.aws.amazon.com/workdocs/latest/adminguide/site-activity.html
2. https://amazonworkdocs.com/apps.html
3. https://docs.aws.amazon.com/workdocs/latest/userguide/activity_feed.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

3.5 Ensure new users can only be invited from allowed domains. (Manual)

Profile Applicability:

- Level 1

Description:

Users that are allowed access to shared files or folders in WorkDocs should be limited to specific domains.

Rationale:

To control who should be allowed to join your WorkDocs site, users should be limited on who they can invite sharing files or folders with new people from the specified domains.

Audit:

Perform the steps to confirm WorkDocs file and sharing folders is controlled by specified domains.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator
2. Click `Security`
3. Under - `Invite settings`
4. Confirm that only

```
Users can invite new people from a few specific domains by sharing files or
folders with them
```

5. Confirm the listed `Domains` is accurate.

If the setting is not set to "Users can invite new people from a few specific domains by sharing files or folders with them" or the domains listed is not accurate refer to the remediation below.

Remediation:

Perform the steps to set WorkDocs file and sharing folders to be controlled by specified domains.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator

2. Click `Security`
3. Under - `Invite settings`
4. Select

```
Users can invite new people from a few specific domains by sharing files or
folders with them
```

5. Add in or edit the listed allowed Domains.

References:

1. https://docs.aws.amazon.com/workdocs/latest/adminguide/manage-sites.html

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

16 Account Monitoring and Control
Account Monitoring and Control

3.6 Ensure only specific users are allowed to invite external users (Manual)

Profile Applicability:

- Level 1

Description:

The organization should only allow administrators the ability to invite external users to the WorkDocs site.

Rationale:

If anyone can invite a user outside of the organization it could potentially lead to security or information leak.

Audit:

Perform the steps to confirm Only Administrators can invite new external users for WorkDocs.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator
2. Click `Security`
3. Under - `external invites`
4. Confirm that only

`Only administrators can invite new external users`
If this is not set to "Only administrators can invite new external users" refer to the remediation below.

Remediation:

Perform the steps to Set Only Administrators can invite new external users for WorkDocs.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator
2. Click `Security`
3. Under - `external invites`
4. Select

```
`Only administrators can invite new external users`
- Only administrators can invite external users to use Amazon WorkDocs.
```

References:

1. https://docs.aws.amazon.com/workdocs/latest/adminguide/manage-sites.html

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.7 Ensure publicly shareable links is not allowed in WorkDocs (Manual)

Profile Applicability:

- Level 1

Description:

The organization should not allow publicly shareable links for WorkDocs.

Rationale:

If a user can create and send a publicly shareable links allowing a file to be viewed by people outside of the organization it could potentially lead to an security or information leak.

Audit:

Perform the steps to confirm publicly shareable links for WorkDocs is not allowed.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator
2. Click `Security`
3. Under - `public share settings`
4. Confirm that - `No public sharing is selected`.

If this is not selected choice refer to the remediation below.

Remediation:

Perform the steps to set set publicly shareable links for WorkDocs to not allowed.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator
2. Click `Security`
3. Under - `public share settings`
4. Select - `No public sharing`. - Users cannot send view links to anyone outside the organization.

References:

1. https://docs.aws.amazon.com/workdocs/latest/adminguide/manage-sites.html

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.8 Ensure any user that has not accessed WorkDocs in 30 days is set to inactive. (Manual)

Profile Applicability:

- Level 1

Description:

User accounts that are not actively using the WorkDocs service should be set to inactive after a period of 30 days.

Rationale:

Inactive accounts may appear to not purpose a problem but they can provide unauthorized access to files with in WorkDocs.

Impact:

Changing a user to Inactive status does not delete their files, folders, or feedback from your Amazon WorkDocs site.

Audit:

Perform the following steps to review list of users
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator
2. Under `My Account`, choose `Open admin control panel`.
3. Under `Manage User`s, choose `Download user`.
4. For Download user, choose `All users`
5. Review the file to determine if any users have not accessed WorkDocs in the past 30 days.

If you find any users that have not accessed WorkDocs in the past 30 days refer to the remediation below.

Remediation:

Perform the steps below to disable a user's access by changing their status to Inactive.
From the WorkDocs Admin control panel

1. Log in to WorkDocs as an Administrator.
2. Under `My Account`, click `Open admin control panel`.

3. Under `Manage Users`, choose the pencil icon next to the user's name that needs to be set as inactive.
4. Choose `Inactive`, and Click Save Changes

The inactivated user no longer has access to your Amazon WorkDocs site.

References:

1. https://docs.aws.amazon.com/workdocs/latest/adminguide/inactive-user.html

CIS Controls:

Version 7

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

16.7 Establish Process for Revoking Access
Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

4 AppStream 2.0

This section contains recommendations for configuring the application streaming service and any additional resources required.

4.1 Ensure AppStream is utilizing its own virtual private cloud (VPC) (Manual)

Profile Applicability:

- Level 1

Description:

AppStream 2.0 should be configured using a VPC with Private subnets and a NAT Gateway.

Rationale:

For AppStream 2.0 the public subnet will have direct access to the internet through the NAT gateway. This setup allows the streaming instances in your private subnets to connect to the internet or other AWS services.

Audit:

Perform the following to determine if a VPC is setup for AppStream 2.0 correctly.
From Console:

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Your VPCs`
3. Select the VPC for AppStream 2.0 and take note of the name and the VPC ID
4. In the left pane, click `Subnets`
5. Confirm you have 3 subnets labeled and associated with the VPC
   `1 AppStream Public Subnet and 2 AppStream Private Subnets`
6. Confirm the `AppStream Public Subnet` is configured correctly.
   - Select AppStream Public subnet

```
Description tab - VPC matches `AppStream ID and name`
Route Table tab  - verify contains rules
`-Example` - Destination - 10.0.0.0/20, Target - local
`-Example` - Destination - 0.0.0.0/0, Target - internet_gateway_ID
```

7. Confirm the `2 AppStream Private Subnets` are configured correctly.
   - Select AppStream Private subnet 1

```
Description Tab - VPC matches `AppStream ID and name` and note Availability
zone
Route Table tab - verify contains routes
`-Example` - Destination - 10.0.0.0/20, Target - local
`-Example` - Destination - 0.0.0.0/0, Target - nat_gateway_ID
`-Example- optional` - Destination - S3bucket_enpoint_ID, Target -
storage_vpce_ID
```

```
 - Select AppStream Private subnet 2

Description Tab - VPC matches `AppStream ID and name` and Availability zone
is set to something different than Private subnet 1
Route Table tab - verify contains routes
`-Example` - Destination - 10.0.0.0/20, Target - local
`-Example` - Destination - 0.0.0.0/0, Target - nat_gateway_ID
`-Example- optional` - Destination - S3bucket_enpoint_ID, Target -
storage_vpce_ID
```

If The AppStream VPC, subnets and route tables are not configured correctly refer to the remediation procedure below.

Remediation:

Perform the steps below to create a VPC, subnets and routing table for AppStream 2.0
From the Console
Allocate an Elastic IP address

1. Login in to the Amazon VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Elastic IPs`.
3. Click `Allocate new address`.
4. Then click on `Allocate`.
5. Make a note of the Elastic IP address.
6. Click `Close`.

Create a New VPC with one public subnet and two private subnet's.

1. Login to the VPC console at `https://console.aws.amazon.com/vpc/`
2. Click `Launch VPC Wizard`.
3. Choose VPC with Public and Private Subnet's`and then click`Select`.
4. Configure the VPC as follows:

```
     - `IPv4 CIDR block` - enter a CIDR block from the private (non-publicly
routable) IP address range - example. 10.0.0.0/16.
     - `IPv6 CIDR block` - Accept the default value - No IPv6 CIDR Block
     - `VPC name` enter a name for the VPC (example, AppStream VPC).
     - `Public subnet's IPv4 CIDR` - enter a CIDR block from the private
(non-publicly routable) IP address range - ie. 10.0.0.0/24.
     - `Availability Zone` - Accept the default value - No Preference
     - `Public subnet name` - enter a name for the subnet (example, AppStream
Public Subnet)
     - `Private subnet's IPv4 CIDR` - enter the CIDR block for the subnet.
     - `Availability Zone` - Accept the default value - No Preference
     - `Private subnet name` - enter a name for the subnet (example,
AppStream Private Subnet 1).
     - `Elastic IP Allocation ID` - enter the Elastic IP address that you
created.
     - `Service Endpoints` - Accept the default value - Blank
     - `Enable DNS hostnames` - Accept the default value - Yes
     - `Hardware tenancy` - Accept the default value - Default
```

5. Click on Create VPC
   ***Note that it takes several minutes to set up your VPC. After the VPC is created, choose OK.

Create the Second Private subnet to the VPC

1. In the left pane, choose Subnets.
2. Click Create subnet.

```
    - `Name tag` - enter a name for the private subnet (example, AppStream
Private subnet 2).
    - `VPC` - select the VPC that you created for AppStream 2.0.
    - `Availability Zone` - select a different one than you are using for
AppStream2 Private subnet 1.
    - `IPv4 CIDR block` - enter the CIDR block for the subnet.
```

3. Click Create.

Verify and Name the Route Tables

1. In the left pane, choose `Subnets`
2. Select the public subnet that you created (example, AppStream Public subnet)
3. On the Route Table tab, click the ID of the route table (example, rtb-12345678).
4. Select the route table.
5. Under Name, choose the edit icon (the pencil), enter a name (for example, appstream-public-routetable), then click the check mark to save.
6. On the Routes tab, confirm one destination and target for local traffic and another destination and target that sends all other traffic to the internet gateway (example, igw-0518a307898725db2).
7. In the left pane, choose Subnets.
8. Select the first private subnet that you created (example, AppStream Private subnet 1)
9. On the Route Table tab, click the ID of the route table (example, rtb-12345678).
10. Select the route table. Under Name, choose the edit icon (the pencil), enter a name (for example, appstream-private-routetable1), then click the check mark to save.
11. On the Routes tab, confirm one destination and target for local traffic and another destination and target that sends all other traffic to the NAT gateway (example, nat-06ea352539b2fddfc).
12. In the left pane, choose Subnets.
13. Select the second private subnet that you created (example, AppStream Private subnet 2)
14. On the Route Table tab, click the ID of the route table (example, rtb-12345678).
15. Select the route table. Under Name, choose the edit icon (the pencil), enter a name (for example, appstream-private-routetable2), then click the check mark to save.

16. On the Routes tab, confirm one destination and target for local traffic and another destination and target that sends all other traffic to the NAT gateway (example, nat-06ea352539b2fddfc).

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/vpc-setup-recommendations.html
2. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html#vpc-sizing-ipv4

CIS Controls:

Version 7

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

4.2 Ensure a VPC Endpoint is set for AppStream (Manual)

Profile Applicability:

- Level 1

Description:

When you select Using a VPC endpoint, this allows users to only stream from this AppStream 2.0 stack when they have network access to the VPC.

Rationale:

Virtual Private Cloud (VPC) endpoints allow your users to stream from AppStream 2.0 through your VPC. You can create a VPC endpoint in the VPC of your choosing, then use the endpoint with AppStream 2.0 VPC to maintain the streaming traffic within the VPC.

Audit:

Perform the steps to review the interface endpoint set for AppStream 2.0
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane, click `Stacks`, then choose the stack that you want.
3. Click the `VPC Endpoints` tab
4. Confirm the Streaming Endpoint listed is the endpoint through which to stream traffic.

If there is no Streaming endpoint pointing to a specific VPC Endpoint and it is labeled as Internet refer to the remediation below.

Remediation:

Perform the following steps to create an interface endpoint
From the Console:

1. Log in to the VPC console at `https://console.aws.amazon.com/vpc/`
2. In the left pane, click `Endpoints`, `Create Endpoint`.
3. Click `Create Endpoint`.

```
- For Service category, ensure that AWS services is selected.
- For Service Name, choose com.amazonaws.<AWS Region>.appstream.streaming.
- For VPC, choose a VPC in which to create the interface endpoint.
- For Subnets, choose the subnets (Availability Zones) in which to create the
endpoint network interfaces.
```

```
- Ensure that the Enable Private DNS Name check box is selected.
- For Security group, select the security group for AppStream
```

4. Click `Create endpoint`.

To update a stack to use a new interface endpoint

1. Log in to AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane, click `Stacks`, and then choose the stack that you want.
3. Click the VPC Endpoints tab, and then choose `Edit`.
4. In the Edit VPC Endpoint dialog box, for Streaming Endpoint, choose the endpoint you just created.
5. Click `Update`.

Traffic for new streaming sessions will be routed through this endpoint. However, traffic for current streaming sessions continues to be routed through the previously specified endpoint.

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/creating-streaming-from-interface-vpc-endpoints.html

CIS Controls:

Version 7

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

4.3 Ensure maximum session duration is no longer than 10 hours. (Automated)

Profile Applicability:

- Level 1

Description:

When creating a fleet for AppStream 2.0 configure the Maximum session duration in minutes to be no greater than 600.

Rationale:

Having a session duration lasting longer than 10 hours should not be necessary and if running for any malicious reasons provides a greater time for usage than should be allowed.

Audit:

Perform the following steps to view the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. On the `Fleet details` tab confirm that Maximum session duration is set to `600` minutes or less.

If Maximum session duration is set to anything greater than 600 minutes refer to the remediation below.

Remediation:

Perform the following steps to edit the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. Click `Actions`, `Stop`
5. Click `Actions`, `Edit`

6. Change the Maximum session duration is set to `600` minutes or less.

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/set-up-stacks-fleets.html

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

4.4 Ensure session disconnect timeout is set to 5 minutes or less. (Automated)

Profile Applicability:

- Level 1

Description:

Disconnect timeout in minutes, is the amount of of time that a streaming session remains active after users disconnect.

Rationale:

If users try to reconnect to the streaming session after a disconnection or network interruption within the 5 minutes, they are connected to their previous session. Otherwise, they are connected to a new session with a new streaming instance and that instance isn't sitting out there not being used.

Audit:

Perform the following steps to view the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. On the `Fleet detail` tab confirm that Disconnect timeout is set to `5` minutes minutes or less.

If Disconnect timeout is set to anything greater than 5 minutes refer to the remediation below.

Remediation:

Perform the following steps to update the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. Click `Actions`, `Stop`

5. Click `Actions`, `Edit`
6. Change the Disconnect timeout to `5` minutes or less.

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/set-up-stacks-fleets.html

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

4.5 Ensure session Idle disconnect timeout is set to 10 minutes or less. (Automated)

Profile Applicability:

- Level 1

Description:

Idle disconnect timeout in minutes is the amount of time that users can be inactive before they are disconnected from their streaming session and the Disconnect timeout in minutes time begins.

Rationale:

Users are considered idle when they stop providing keyboard or mouse input during their streaming session. File uploads and downloads, audio in, audio out, and pixels changing do not qualify as user activity. Once disconnected from their streaming session the Disconnect timeout begins.

Audit:

Perform the following steps to view the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. On the `Fleet details` tab confirm that Idle disconnect timeout is set to `10` minutes or less.

If Idle disconnect timeout is set to anything greater than 10 minutes refer to the remediation below.

Remediation:

Perform the following steps to view the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`

4. Click `Actions`, `Stop`
5. Click `Actions`, `Edit`
6. Change the Idle disconnect timeout to 5 minutes or less.

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/set-up-stacks-fleets.html

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

4.6 Ensure internet access is granted and managed through your VPC (Automated)

Profile Applicability:

- Level 1

Description:

Default Internet Access from your fleet streaming instances should remain unchecked.

Rationale:

Default Internet Access from your fleet streaming instances should be controlled using a NAT gateway in the VPC.

Audit:

Perform the following steps to view the Fleet settings in AppStream
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. On the `Fleet details` tab confirm that Default Internet Access is set to `Disabled`.

If Default internet access is not set to disabled refer to the remediation below.

Remediation:

Perform the following steps to view the Fleet settings in AppStream
From the console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Fleets`.
3. Select the `Fleet`
4. Click `Actions`, `Stop`
5. Click `Actions`, `Edit`
6. Deselect `Default Internet Access`
7. Click `Save`

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/set-up-stacks-fleets.html

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

4.7 Ensure Operating system updates are applied to your base image every 30 days. (Manual)

Profile Applicability:

- Level 1

Description:

To ensure that your fleet instances have the latest Windows updates installed, we recommend that you install Windows updates on your image builder, create a new image, and then update your fleet with the new image once a month.

Rationale:

All fleet instances used in user streaming sessions have only the Windows and application updates that were installed on the underlying image when it was created. In addition, any updates made to Windows or to applications on the instance during the streaming session will not persist to future sessions by the same user or other users.

Audit:

Perform the following steps to review the Image date.
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. In the left pane click on `Images`
3. Select the `Image Builder` tab
4. Select `Image`
5. In the `Details` tab review the `Created at date` and the `AppStream agent version`.

If the created at date is over 30 days old refer to the remediation below.

Remediation:

Perform the steps below to create an image and update it.
From the Console

1. Log in to the AppStream 2.0 console at `https://console.aws.amazon.com/appstream2`
2. Click `Images` in the left pane, then Click the `Image Builder` tab, and Click `Launch Image Builder`.

3. Choose a base image. The latest base images released by AWS is recommended and selected by default.
4. Click `Next`.
5. Configure `Image Builder`, by doing the following:

```
- Name: Type a unique name identifier for the image builder.
-Display name (optional): Type a name to display for the image builder
(maximum of 100 characters).
- Tags (optional): Choose Add Tag, and type the key and value for the tag. To
add more tags, repeat this step.
- Instance Type: Select the instance type for the image builder.
- Network Access Points (Optional): You can create a private link, which is
an interface VPC endpoint (interface endpoint), in your virtual private cloud
(VPC). To start creating the interface endpoint, select Create PrivateLink.
- After you create the interface endpoint, you can use it to keep streaming
traffic within your VPC.
- AppStream 2.0 Agent: This section displays only if you are not using the
latest version of the agent.
- If you are not using the latest AppStream 2.0 agent always select the
option to launch your image builder with the latest agent.
- IAM role (Advanced): Use existing or create a new IAM role
```

6. Click `Next`.
7. Configure Network, do the following:

```
- Leave Default Internet Access unselected.
- For VPC and Subnet 1, choose a VPC and two subnets in different
Availability Zones.
- For Security group(s), choose up to five security groups to associate with
this image builder.
- For Active Directory Domain (Optional), expand this section to choose the
Active Directory configuration and organizational unit in which to place your
streaming instance computer objects. Ensure that the selected network access
settings enable DNS resolvability and communication with your directory.
- Choose Review and confirm the details for the image builder.
- Review the configuration details.
```

Click `Launch`.
Next Steps
Install Operating system updates and install, configure and update your applications for streaming, and then create an image by creating a snapshot of the image builder instance.

References:

1. https://docs.aws.amazon.com/appstream2/latest/developerguide/tutorial-image-builder.html#tutorial-image-builder-install
2. https://docs.aws.amazon.com/appstream2/latest/developerguide/programmatically-create-image.html
3. https://docs.aws.amazon.com/appstream2/latest/developerguide/managing-image-builders.html

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5 WorkLink

This section contains recommendations for configuring the WorkLink service and any additional resources required.

5.1 Ensure the Audit log stream is configured. (Manual)

Profile Applicability:

- Level 1

Description:

Amazon WorkLink creates activity logs that allow you to track the total number of users accessing content, the content accessed, when users accessed content and what devices users accessed content from.

Rationale:

These logs are delivered to a Kinesis data stream in your AWS account. From there you can direct that information to a data store or a 3rd Party Tool of your choice.

Audit:

Perform the steps to review your audit log delivery
From the Console

1. Log in to the WorkLink console at `https://console.aws.amazon.com/worklink/`
2. On the Fleets page, select the `fleet`, and Click `View details`.
3. Click on `Audit logs - optional`
4. Review the log details and confirm that it is going to a Kinesis data stream with the `AmazonWorkLink` prefix.

If the Audit logs is not configured or it is utilizing a data stream with a different prefix refer to the remediation below.

Remediation:

Perform the steps to configure your audit log delivery
From the Console

1. Log in to the WorkLink console at `https://console.aws.amazon.com/worklink/`
2. On the Fleets page, select the `fleet`, and Click `View details`.
3. Choose `Audit logs - optional`, `Configure audit logs`.
4. Select the Kinesis data stream. If you haven't created a Kinesis data stream with the "AmazonWorkLink-" name prefix, click `Create Kinesis Stream` to do so. After you create a Kinesis data stream, go back and select it.
5. Click `Link audit logs`.

References:

1. https://docs.aws.amazon.com/worklink/latest/ag/audit-log.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.2 Ensure device policies are configured. (Manual)

Profile Applicability:

- Level 1

Description:

Configure device policies for accessing internal content.

Rationale:

Deploying device policies provides an extra layer of security ensuring that the device that is connecting to WorkLinks is valid and approved.

Audit:

Perform the steps to review the device policy configuration
From the Console

1. Log in to the WorkLink console at `https://console.aws.amazon.com/worklink/`
2. On the Fleets page, select the `fleet`, and click `View details`.
3. Click `Device policies - optional`
4. Review the set policy and confirm that a certificate chain file has been applied, including intermediate certificates and the root certificate authority certificate.

If the device policy is not configured as outlined refer to the remediation procedure below.

Remediation:

Perform the steps to review the device policy configuration in the WorkLink console
From the Console

1. Log in to the WorkLink console at `https://console.aws.amazon.com/worklink/`
2. On the Fleets page, select the `fleet`, and choose `View details`.
3. Click `Device policies - optional` and `Configure device policies`.
4. Under `Device certificate authority`, click Choose file to select the certificate chain, including intermediate certificates and the root certificate authority certificate used to issue device certificates.
5. Click `Configure device policies`.

References:

1. https://docs.aws.amazon.com/worklink/latest/ag/configure-policy.html

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

Appendix: Summary Table

Control		**Set Correctly**	
		Yes	No
1	**Introduction**		
2	**WorkSpaces**		
2.1	Ensure Administrators of WorkSpaces is defined using IAM (Automated)	□	□
2.2	Ensure MFA is enable for WorkSpaces users (Manual)	□	□
2.3	Ensure WorkSpace volumes are encrypted. (Automated)	□	□
2.4	Ensure WorkSpaces are deployed in their own virtual private cloud (VPC) (Manual)	□	□
2.5	Ensure WorkSpaces traffic is controlled and routed through a NAT Gateway. (Manual)	□	□
2.6	Ensure Web Access to Workspaces is Disabled (Automated)	□	□
2.7	Ensure access is limited to trusted devices. (Manual)	□	□
2.8	Ensure the default IP access control group is dissassociated. (Automated)	□	□
2.9	Ensure CloudWatch is set up for WorkSpaces. (Manual)	□	□
2.10	Ensure that patches and updates are performed on the operating system for Workstations. (Automated)	□	□
2.11	Ensure your WorkSpaces image has the appropriate CIS Operating System Benchmark applied (Manual)	□	□
2.12	Restrict WorkSpaces Bundle options to organization approved versions (Manual)	□	□
2.13	Ensure Workspaces images are not older than 90 days. (Manual)	□	□
2.14	Ensure WorkSpaces that are not being utilized are removed. (Automated)	□	□
2.15	Ensure primary interface ports for Workspaces are not open to all inbound traffic. (Automated)	□	□
2.16	Ensure FIPS Endpoint encryption is enabled for WorkSpaces. (Manual)	□	□
2.17	Ensure WorkSpaces API requests flow through a VPC Endpoint (Automated)	□	□
2.18	Ensure Radius server is using the recommended security protocol (Automated)	□	□
3	**WorkDocs**		
3.1	Ensure Administrators of WorkDocs is defined using IAM (Automated)	□	□
3.2	Ensure MFA is enable for WorkDoc users (Manual)	□	□

3.3	Ensure Workdocs access is limited to a range of allowable IP addresses. (Manual)	□	□
3.4	Utilize site wide activity feed for monitoring. (Manual)	□	□
3.5	Ensure new users can only be invited from allowed domains. (Manual)	□	□
3.6	Ensure only specific users are allowed to invite external users (Manual)	□	□
3.7	Ensure publicly shareable links is not allowed in WorkDocs (Manual)	□	□
3.8	Ensure any user that has not accessed WorkDocs in 30 days is set to inactive. (Manual)	□	□
4	**AppStream 2.0**		
4.1	Ensure AppStream is utilizing its own virtual private cloud (VPC) (Manual)	□	□
4.2	Ensure a VPC Endpoint is set for AppStream (Manual)	□	□
4.3	Ensure maximum session duration is no longer than 10 hours. (Automated)	□	□
4.4	Ensure session disconnect timeout is set to 5 minutes or less. (Automated)	□	□
4.5	Ensure session Idle disconnect timeout is set to 10 minutes or less. (Automated)	□	□
4.6	Ensure internet access is granted and managed through your VPC (Automated)	□	□
4.7	Ensure Operating system updates are applied to your base image every 30 days. (Manual)	□	□
5	**WorkLink**		
5.1	Ensure the Audit log stream is configured. (Manual)	□	□
5.2	Ensure device policies are configured. (Manual)	□	□

Appendix: Change History

Date	Version	Changes for this version
Nov 13, 2020	1.0.0	Document Created