CIS Arista MLS EOS 4.X L2S STIG Benchmark

v1.0.0 - 08-27-2025

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/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Arista MLS EOS 4.X L2S Secure Technical Implementation Guide (STIG)

Version: 2 Release: 3 Benchmark

Date: 02 Jul 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Arista MLS EOS 4.X L2S and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

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

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Arista MLS EOS 4.X L2S.

Recommendations

1 STIG RULES

Arista Cloud EOS

Arista MLS EOS 4.X L2S Secure Technical Implementation Guide (STIG)

Version: 2 Release: 3 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

1.1 ARST-L2-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista MLS layer 2 switch must uniquely identify all network-connected endpoint devices before establishing any connection.

```
GROUP ID: V-255968
RULE ID: SV-255968r882246
```

Rationale:

Controlling LAN access via 802.1x authentication can assist in preventing a malicious user from connecting an unauthorized PC to a switch port to inject or receive data from the network without detection.

Satisfies: SRG-NET-000148-L2S-000015, SRG-NET-000343-L2S-000016

Audit:

Verify the Arista MLS switch configuration has 802.1x authentication implemented for all access switch ports connecting to LAN outlets (i.e., RJ-45 wall plates) or devices not located in the telecom room, wiring closets, or equipment rooms. MAC Authentication Bypass (MAB) must be configured on switch ports connected to devices that do not provide an 802.1x supplicant.

Verify the Arista MLS switch configuration for 802.1x is configured globally and, on the required host-based access ports or MAB, is configured on ports that require RADIUS and MAC-based supplicants.

```
switch# show run | section dot1x
logging level DOT1X informational
aaa authentication dot1x default group radius
dot1x system-auth-control
!
interface Ethernet6
   description 802.1X Access Network
   switchport access vlan 100
   dot1x pae authenticator
   dot1x reauthentication
   dot1x port-control auto
   dot1x host-mode single-host
   dot1x timeout quiet-period 10
!
interface Ethernet7
   description STIG MAC-Based Authentication
   speed 100full
   dot1x pae authenticator
   dot1x port-control auto
   dot1x mac based authentication
!
```

If 802.1x authentication or MAB is not configured on all access switch ports connecting to LAN outlets or devices not located in the telecom room, wiring closets, or equipment rooms, this is a finding.

Remediation:

Configure Arista MLS switch for 802.1X globally with the following mandatory parameters, and then configure non-data center access ports and all applicable interfaces.

Step 1: Configure the Arista MLS switch for 802.1X globally using the following commands:

```
!
logging level DOT1X informational
aaa authentication dot1x default group radius
dot1x system-auth-control
!
```

Step 2: Configure the Arista switch for all non-data center access ports with 802.1X VLAN to an access/trunk port and set the 802.1X port access entity (PAE) to authenticator with the following commands:

```
interface Ethernet4
description 802.1X Host-Mode Access Port
   switchport access vlan 100
   dot1x pae authenticator
   dot1x reauthentication
   dot1x port-control auto
   dot1x host-mode single-host
   dot1x timeout quiet-period 10
!
```

Step 3: The Arista switch can be also configured for MAC-based authentication. Configuring MAB requires that every supplicant trying to gain access to the switch authenticator port is individually authenticated by MAC address as opposed to authenticating just one supplicant on a given VLAN or port with 802.1X, and then using the MAC address of these devices as username and password in the RADIUS request packets.

```
!
interface Ethernet7
 description MAC-Based Authentication
   speed 100full
   dot1x pae authenticator
   dot1x port-control auto
   dot1x mac based authentication
!
```

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.2 ARST-L2-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must be configured for Storm Control to limit the effects of packet flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-255969
RULE ID: SV-255969r991773
```

Rationale:

Denial of service is a condition when a resource is not available for legitimate users. Packet flooding distributed DoS (DDoS) attacks are referred to as volumetric attacks and have the objective of overloading a network or circuit to deny or seriously degrade performance, which denies access to the services that normally traverse the network or circuit. Volumetric attacks have become relatively easy to launch by using readily available tools such as Low Orbit Ion Cannon or by using botnets.

Measures to mitigate the effects of a successful volumetric attack must be taken to ensure that sufficient capacity is available for mission-critical traffic. Managing capacity may include, for example, establishing selected network usage priorities or quotas and enforcing them using rate limiting, Quality of Service (QoS), or other resource reservation control methods. These measures may also mitigate the effects of sudden decreases in network capacity that are the result of accidental or intentional physical damage to telecommunications facilities (such as cable cuts or weather-related outages).

Satisfies: SRG-NET-000193-L2S-000020, SRG-NET-000362-L2S-000024, SRG-NET-000512-L2S-000001

Audit:

Verify the Arista MLS switch is configured for storm-control on applicable Ethernet interfaces.

```
switch#show storm-control
Port          Type  Level Rate(Mbps)   Status      Drops Reason
Et10/2         all     75       7500   active          0
Et4   multicast     55       5500   active          0
Et4   broadcast     50       5000   active
switch#
```

If the Arista MLS switch is not configured to implement a storm-control policy, this is a finding.

Remediation:

The Arista MLS switch must be configured to implement a storm-control policy for traffic prioritization and bandwidth reservation.

Storm-control on switch Ethernet interfaces can be configured to limit the packets based on broadcast, multicast, and unknown-unicast traffic:

```
switch#configure
switch(config)#internet et[X]
interface Ethernet[X]
switchport
   storm-control broadcast level pps 5000
   storm-control multicast level pps 5000
   storm-control unknown-unicast level pps 5000
```

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

CCI-004866 Employ organization-defined controls by type of denial-of-service to achieve the denial-of-service objective.

- NIST SP 800-53 Revision 5::SC-5 b

1.3 ARST-L2-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Arista MLS switch must have Root Guard enabled on all switch ports connecting to access layer switches and hosts.

```
GROUP ID: V-255970
RULE ID: SV-255970r882252
```

Rationale:

Spanning Tree Protocol (STP) does not provide any means for the network administrator to securely enforce the topology of the switched network. Any switch can be the root bridge in a network. However, a more optimal forwarding topology places the root bridge at a specific predetermined location. With the standard STP, any bridge in the network with a lower bridge ID takes the role of the root bridge. The administrator cannot enforce the position of the root bridge but can set the root bridge priority to 0 in an effort to secure the root bridge position.

Audit:

Review the Arista MLS switch topology as well as the configuration to verify that root guard is enabled on switch ports facing switches that are downstream from the root bridge.

Example:

```
switch#sh run | sec guard root
interface Ethernet37
   spanning-tree guard root
```

If the Arista MLS switch has not enabled guard root on all ports connecting to the access layer where the root bridge must not appear, this is a finding.

Remediation:

The Arista MLS switch must be configured for spanning-tree guard root mode on all ports connecting to the access layer interface.

Configure Arista MLS switch Ethernet interface with the following commands:

```
switch#config
switch(config)interface Ethernet[X]
switch(config-if-Et[X])#spanning-tree guard root
switch(config-if-Et[X])#exit
!
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.4 ARST-L2-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have BPDU Guard enabled on all switch ports connecting to access layer switches and hosts.

```
GROUP ID: V-255971
RULE ID: SV-255971r882255
```

Rationale:

If a rogue switch is introduced into the topology and transmits a Bridge Protocol Data Unit (BPDU) with a lower bridge priority than the existing root bridge, it will become the new root bridge and cause a topology change, rendering the network in a suboptimal state. The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into a disabled state and sends a log message.

Audit:

Review the Arista MLS to verify that BPDU Guard is enabled on all user-facing or untrusted access switch ports.

```
switch#show run | section bpdu
interface Ethernet37
   spanning-tree bpduguard enable
```

If the Arista MLS switch has not enabled BPDU Guard, this is a finding.

Remediation:

The Arista MLS switch provides the capability to configure "spanning-tree bpduguard". Configure the Ethernet interface commands:

```
config
interface Ethernet[X]
switch(config)#interface ethernet [X]
switch(config-if-Et[X])#spanning-tree bpduguard enabled
switch(config-if-Et[X])
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.5 ARST-L2-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS switch must have STP Loop Guard enabled on all nondesignated STP switch ports.

```
GROUP ID: V-255972
RULE ID: SV-255972r1107168
```

Rationale:

The Spanning Tree Protocol (STP) loop guard feature provides additional protection against STP loops. An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. In its operation, STP relies on continuous reception and transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the nondesignated port receives BPDUs. When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes a designated port and moves to a forwarding state. This situation creates a loop. The loop guard feature makes additional checks. If BPDUs are not received on a nondesignated port and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state. In topologies where fiber optic interconnections are used, physical misconnections can occur that allow a link to appear to be up when there is a mismatched set of transmit/receive pairs. When such a physical misconfiguration occurs, protocols such as STP can cause network instability.

Audit:

Review the Arista MLS switch configuration to verify that STP Loop Guard is enabled. It can be enabled globally or applied to an interface.

Note: Arista uses STP Loop guard to protect against one-way connections.

```
switch# sh run | sec spanning-tree
spanning-tree guard loop default
```

Or,

```
interface Ethernet6
    spanning-tree guard loop
```

If STP Loop Guard is not configured globally or on nondesignated STP ports, this is a finding.

Remediation:

Configure the Arista MLS switch for STP Loop Guard globally with the following command:

```
switch(config)#spanning-tree guard loop default
switch(config)#
```

Alternatively, configure Loop Guard on each interface:

```
switch(config-if-Eth6)# spanning-tree guard loop
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.6 ARST-L2-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have DHCP snooping for all user VLANs to validate DHCP messages from untrusted sources.

```
GROUP ID: V-255973
RULE ID: SV-255973r882261
```

Rationale:

In an enterprise network, devices under administrative control are trusted sources. These devices include the switches, routers, and servers in the network. Host ports and unknown DHCP servers are considered untrusted sources. An unknown DHCP server on the network on an untrusted port is called a spurious DHCP server, any device (PC, Wireless Access Point) that is loaded with DHCP server enabled. The DHCP snooping feature determines whether traffic sources are trusted or untrusted. The potential exists for a spurious DHCP server to respond to DHCPDISCOVER messages before the real server has time to respond. DHCP snooping allows switches on the network to trust the port a DHCP server is connected to and not trust the other ports.

The DHCP snooping feature validates DHCP messages received from untrusted sources and filters out invalid messages as well as rate-limits DHCP traffic from trusted and untrusted sources. DHCP snooping feature builds and maintains a binding database, which contains information about untrusted hosts with leased IP addresses, and it utilizes the database to validate subsequent requests from untrusted hosts. Other security features, such as IP Source Guard and Dynamic Address Resolution Protocol (ARP) Inspection (DAI), also use information stored in the DHCP snooping binding database. Hence, it is imperative that the DHCP snooping feature is enabled on all user VLANs.

Audit:

Review the Arista MLS switch configuration and verify that DHCP snooping is enabled on all user VLANs.

Verify the Arista MLS has the DHCP Snooping feature enabled globally by executing "show ip dhcp snooping".

```
switch(config)# show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping is operational
DHCP Snooping is configured on following VLANs:
 650
DHCP Snooping is operational on following VLANs:
 650
```

If the Arista MLS switch does not have DHCP snooping enabled for all user VLANs to validate DHCP messages from untrusted sources, this is a finding.

Remediation:

Configure the Arista MLS switch to have DHCP snooping enabled globally and for all user VLANs to validate DHCP messages from untrusted sources.

Step 1: Configure DHCP Snooping globally by using the following command:

```
switch(config)# ip dhcp snooping
```

Step 2: Configure DHCP Snooping to enable the insertion of option-82 in DHCP request packets. By default, option-82 is not enabled and without this, DHCP Snooping is not operational.

```
switch(config)#ip dhcp snooping information option
```

Step 3: Configure the Arista MLS switch to enable IP DHCP Snooping on the corresponding VLANs. By default, DHCP Snooping will not be enabled on any VLAN.

```
switch(config)#ip dhcp snooping vlan <vlan-id>
```

Step 4: Configure the following command to set the circuit-id information that will be sent in option-82. By default, Interface name and VLAN ID are sent. Remote circuit-id will always be the MAC address of the relay agent.

```
switch# ip dhcp snooping information option circuit-id type 2 format
  Hostname and interface name
  Interface name and VLAN ID
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.7 ARST-L2-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Arista MLS layer 2 switch must have IGMP or MLD Snooping configured on all VLANs.

```
GROUP ID: V-255976
RULE ID: SV-255976r882270
```

Rationale:

IGMP and MLD snooping provides a way to constrain multicast traffic at Layer 2. By monitoring the IGMP or MLD membership reports sent by hosts within a VLAN, the snooping application can set up Layer 2 multicast forwarding tables to deliver specific multicast traffic only to interfaces connected to hosts interested in receiving the traffic, thereby significantly reducing the volume of multicast traffic that would otherwise flood the VLAN.

Audit:

Review the Arista MLS switch configuration to verify that IGMP or MLD snooping has been configured.

Determine which snooping feature is used.

For IGMP:

Verify the PIM that also enables IGMP on an Arista MLS switch VLAN interface by using the "sh run interface vlan8" command:

```
switch(config)#sh run int vlan8
interface VLAN8
   ip igmp
   pim ipv4 sparse-mode
switch(config)#exit
```

For MLD:

Verify the Arista MLS switch is configured for MLD snooping on an interface for version 1 and 2. Version 2 is the default MLD version.

switch#sh run | section mld

mld snooping

vlan 200

If the Arista switch is not configured to implement IGMP or MLD snooping for each VLAN, this is a finding.

Remediation:

Configure the Arista MLS switch for IGMP snooping for IPv4 and IPv6 multicast traffic for each VLAN.

Configure the Arista MLS switch for IP PIM, which also enables IGMP on an Arista MLS switch VLAN or interface, by using the following command:

```
switch(config)#int vlan8
   ip igmp
   pim ipv4 sparse-mode
   pim ipv6 sparse-mode
switch(config)#exit
!
```

Arista MLS switch alternative configuration for MLD snooping on an interface for version 1 and 2. Version 2 is the default MLD version.

```
switch(config)# mld snooping
switch(config-mld-snooping)# vlan 200
!
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.8 ARST-L2-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have Dynamic Address Resolution Protocol (ARP) Inspection (DAI) enabled on all user VLANs.

```
GROUP ID: V-255975
RULE ID: SV-255975r882267
```

Rationale:

DAI intercepts Address Resolution Protocol (ARP) requests and verifies that each of these packets has a valid IP-to-MAC address binding before updating the local ARP cache and before forwarding the packet to the appropriate destination. Invalid ARP packets are dropped and logged. DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in the DHCP snooping binding database. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

Audit:

Review the Arista MLS switch configuration to verify that Dynamic Address Resolution Protocol (ARP) Inspection (DAI) feature is enabled on all user VLANs.

Verify ARP inspection for user VLANs by the following command:

```
sh ip arp inspection vlan

VLAN 2200
------------
Configuration: Enabled
Operation State: Active
```

If static ARP inspection is not enabled on all user VLANs, this is a finding.

Remediation:

Configure the Arista MLS switch to have static Address Resolution Protocol (ARP) Inspection to be enabled on all user VLANs.

By default, Arista MLS switch static ARP Inspection is disabled on all VLANs. Static ARP inspection can be enabled on all specific user VLANs by using the following command:

```
switch(config)#ip arp inspection vlan <vlan-list>
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.9 ARST-L2-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have IP Source Guard enabled on all user-facing or untrusted access switch ports.

```
GROUP ID: V-255974
RULE ID: SV-255974r882264
```

Rationale:

IP Source Guard (IPSG) provides source IP address filtering on a layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

Audit:

Review the Arista MLS switch configuration to verify that IPSG is enabled on all user-facing or untrusted access switch ports.

Step 1: The Arista MLS switch command verifies the IPSG configuration and operational states.

```
switch(config)#show ip verify source

Interface       Operational State
--------------- ------------------------
Ethernet1       IP source guard enabled
Ethernet2       IP source guard disabled
```

Step 2: The following command displays all VLANs configured in no IP verify source VLAN:

```
switch(config)#show ip verify source vlan

IPSG disabled on VLANS: 1-2
VLAN            Operational State
--------------- ------------------------
1               IP source guard disabled
2               Error: vlan classification failed
```

If the Arista MLS switch does not have IP Source Guard enabled on all untrusted access switch ports, this is a finding.

Remediation:

Configure the Arista MLS switch to have IPSG enabled on all user-facing or untrusted access switch ports.

Step 1: The Arista MLS IPSG feature must be configured by applying filters to inbound IP packets based on their source MAC and IP addresses. The following example commands exclude VLAN IDs 1 through 3 from IPSG filtering. When enabled on a trunk port, IPSG filters the inbound IP packets on all allowed VLANs. IP packets received on VLANs 4 through 10 on Ethernet 36 will be filtered by IPSG, while those received on VLANs 1 through 3 are permitted.

```
switch(config)#no ip verify source vlan 1-3
switch(config)#interface ethernet 36
switch(config-if-Et36)#switchport mode trunk
switch(config-if-Et36)#switchport trunk allowed vlan 1-10
switch(config-if-Et36)#ip verify source
switch(config-if-Et36)#
```

Step 2: By using the Arista MLS switch command, the switch binds the source IP-MAC binding entries to IP address 10.1.1.1, MAC address 0000.aaaa.1111, VLAN ID 4094, and Ethernet interface 36.

```
switch(config)#ip source binding 10.1.1.1 0000.aaaa.1111 vlan 4094 interface
ethernet 36
```

switch(config)#

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.10 ARST-L2-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 Arista MLS switch must implement Rapid STP where VLANs span multiple switches with redundant links.

```
GROUP ID: V-255977
RULE ID: SV-255977r882273
```

Rationale:

Spanning Tree Protocol (STP) is implemented on bridges and switches to prevent layer 2 loops when a broadcast domain spans multiple bridges and switches and when redundant links are provisioned to provide high availability in case of link failures. Convergence time can be significantly reduced using Multiple Spanning-Tree (802.1s) instead of Rapid STP (802.1w) instead of STP (802.1d), resulting in improved availability. Multiple Spanning-Tree Protocol (MSTP) should be deployed by implementing either Rapid Per-VLAN-Spanning-Tree (Rapid-PVST) or Multiple Spanning-Tree MST, the latter scales topologies much better when there are many VLANs.

Audit:

In cases where VLANs do not span multiple switches, it is a best practice to not implement STP. Avoiding the use of STP will provide the most deterministic and highly available network topology. If STP is required, review the Arista MLS switch configuration to verify that Rapid STP has been implemented.

```
switch(config)#sh run | sec spanning-tree
spanning-tree mode rstp
!
```

Note: MSTP can be configured as an alternate mode. MSTP uses RSTP for rapid convergence and enables multiple VLANs to be grouped into and mapped to the same spanning-tree instance, thereby reducing the number of spanning-tree instances needed to support a large number of VLANs.

If MSTP or Rapid STP has not been implemented where STP is required, this is a finding.

Remediation:

Configure the Arista MLS switch for Multiple Spanning-tree (MST) or Rapid STP to be implemented at the access and distribution layers where VLANs span multiple switches.

```
switch(config)#spanning-tree mode mstp
```

The Arista MLS switch can alternatively be configured for spanning-tree mode RSTP to support a spanning-tree instance for each VLAN:

```
switch(config)#
spanning-tree mode rstp
!
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.11 ARST-L2-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have all trunk links enabled statically.

```
GROUP ID: V-255979
RULE ID: SV-255979r882279
```

Rationale:

When trunk negotiation is enabled via Dynamic Trunk Protocol (DTP), considerable time can be spent negotiating trunk settings (802.1q or ISL) when a node or interface is restored. While this negotiation is happening, traffic is dropped because the link is up from a layer 2 perspective. Packet loss can be eliminated by setting the interface statically to trunk mode, thereby avoiding dynamic trunk protocol negotiation and significantly reducing any outage when restoring a failed link or switch.

Audit:

Review the Arista MLS switch configuration to verify that all Ethernet interfaces designated as trunk links are statically configured to specify only member tagged VLAN traffic is allowed and all nonmember VLAN traffic will be dropped unless untagged traffic is associated with the interface's native VLAN.

```
switch#show run | section trunk
!
interface Ethernet6
   description STIG Static Trunk
   speed forced 10000full
   switchport trunk native vlan 2102
   switchport trunk allowed vlan 2100-2102
   switchport mode trunk
!
```

If trunk negotiation is enabled on any interface, this is a finding.

Remediation:

Configure static Ethernet interfaces for switchport trunk mode. Ensure required VLAN member tagged traffic is allowed and all other VLAN traffic will be dropped unless an associated untagged native VLAN for the Ethernet interface is allowed.

```
switch#configure
switch(config)#interface Ethernet6
   description STIG Static Trunk
   speed forced 10000full
   switchport trunk native vlan 2102
   switchport trunk allowed vlan 2100-2102
   switchport mode trunk
!
switch(config)#interface Ethernet7
   description STIG Static Trunk
   speed forced 10000full
   switchport trunk native vlan 3102
   switchport trunk allowed vlan 3100-3102
   switchport mode trunk
!
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.12 ARST-L2-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have all disabled switch ports assigned to an unused VLAN.

```
GROUP ID: V-255980
RULE ID: SV-255980r991774
```

Rationale:

It is possible that a disabled port that is assigned to a user or management VLAN becomes enabled by accident or by an attacker and as a result gains access to that VLAN as a member.

Audit:

Step 1: Review the switch configuration and examine all access switch ports. Verify the unused port is configured to be intentionally shut down and assigned to an inactive VLAN.

```
switch(config)#sh run int eth8
interface Ethernet8
   description PORT IS INTENTIONALLY SHUTDOWN
   switchport access vlan 999
   shutdown
switch(config)#
```

Step 2: Verify traffic from the inactive VLAN is not allowed on any trunk links as shown in the example below:

```
switch(config)#sh run int eth9
interface Ethernet9
   switchport trunk native vlan 1000
   switchport trunk allowed vlan 2-998, 1001-4094
   switchport mode trunk
switch(config)#
```

If any access switch ports are not in use and not in an inactive shutdown, this is a finding.

Note: Switch ports configured for 802.1x are exempt from this requirement.

Remediation:

Configure all Arista MLS switch ports not in use to be shut down and assigned to an unused VLAN.

Step 1: Configure all unused ports to be shut down and assigned to an unused VLAN.

```
switch(config)#interface ethernet 9
switch(config-eth9)#shutdown
switch(config-eth9)# description this port is intentionally shutdown
switch(config-eth9)# switchport access vlan 999
```

Step 2: Configure any trunk links to exclude the unused VLAN.

```
switch(config)# interface ethernet 10
switch(config-eth10)# switchport trunk native vlan 1000
switch(config-eth9)# switchport trunk allowed vlan 2-998, 1001-4094
switch(config-eth9)# switchport mode trunk
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.13 ARST-L2-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must not have the default VLAN assigned to any host-facing switch ports.

```
GROUP ID: V-255981
RULE ID: SV-255981r991775
```

Rationale:

In a VLAN-based network, switches use the default VLAN (i.e., VLAN 1) for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, the default VLAN may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Audit:

Review the Arista MLS switch configurations and verify no access switch ports have been assigned membership to the default VLAN (i.e., VLAN 1).

```
switch(config)#sh vlan
VLAN  Name                             Status    Ports
----- -------------------------------- --------- -------------------------------
---
1     default
8     VLAN0008                           active    Cpu
25    VLAN0025                          active    Cpu
100   VLAN0100                         active    Cpu
1000  VLAN1000                        active    Eth1, Eth2
```

If access switch ports are assigned to the default VLAN, this is a finding.

Remediation:

Configure the Arista MLS switch to remove the assignment of the default VLAN from all access switch ports.

Step 1: Configure the Default VLAN 1 to shut down by using the following command:

```
switch:(config#)interface vlan 1
switch(config-int-vlan1)#shutdown
```

Step 2: Configure all access switch ports to be placed in a VLAN other than the default (1):

```
switch(config)#interface ethernet 8
switch(config-eth8)#switchport access vlan 1000
switch(config-eth8)#exit
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.14 ARST-L2-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have the default VLAN pruned from all trunk ports that do not require it.

```
GROUP ID: V-255982
RULE ID: SV-255982r991776
```

Rationale:

The default VLAN (i.e., VLAN 1) is a special VLAN used for control plane traffic such as Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP). VLAN 1 is enabled on all trunks and ports by default. With larger campus networks, care needs to be taken about the diameter of the STP domain for the default VLAN. Instability in one part of the network could affect the default VLAN, thereby influencing control-plane stability and therefore STP stability for all other VLANs.

Audit:

Review the Arista MLS switch configuration and verify the default VLAN is pruned from trunk links that do not require it.

Step 1: Review the Arista MLS switch configuration by using the following commands to ensure the default VLAN 1 state is suspended:

```
switch(config)#vlan 1
switch(config-vlan-1)#sh act
vlan
   !! STIG suspend vlan 1 #state suspend vlan 1
switch(config-vlan-1)#exit
```

Step 2: Review the configuration to ensure default VLAN 1 is pruned from any trunk active links by using the command "show vlan brief":

```
switch(config-vlan-4090)#
switch(config-vlan-4090)#sh vlan brie
VLAN  Name                             Status    Ports
----- -------------------------------- --------- -------------------------------
---
1     default
8     VLAN0008                          active    Cpu
25    VLAN0025                         active    Cpu
100   VLAN0100                        active    Cpu
1000  VLAN1000                       active
4090  VLAN4090                       active
```

If the default VLAN state is not suspended and pruned from trunk links that should not be transporting frames for the VLAN, this is a finding.

Remediation:

Best practice for VLAN-based networks is to configure Arista MLS switch to prune unnecessary trunk links from gaining access to the default VLAN and ensure frames belonging to the default VLAN do not traverse trunks not requiring frames from the VLAN.

Step 1: Configure the Arista MLS switch to ensure VLAN1 is pruned from all trunk and access ports that do not require it by using the following commands:

```
switch(config)#vlan 1
switch(config-vlan-1)#show active
switch(config-vlan-1)#sh act
vlan
   !! STIG suspend vlan 1 #state suspend vlan 1
switch(config-vlan-1)#exit
```

Step 2: Configure the Arista MLS switch to allow VLAN trunking except default VLAN 1 and configure Ethernet port 1 to change the native VLAN to 1000.

```
switch(config)#interface e10
switch(config-eth1o)#switchport trunk native vlan 1000
switch(config-eth1)#switchport trunk allowed vlan except 1
```

Step 3: Alternatively, the Arista MLS switch can use trunk groups to determine which trunks service which VLANs:

```
switch(config)#vlan 1
switch(config-vlan-1)#trunk group DO_NOT_USE
switch(config-vlan-1)#sh act
vlan
   !! STIG suspend vlan 1 #state suspend vlan 1
   trunk group DO_NOT_USE
hss474.10:51:12(config-vlan-1)#
```

Step 4: On Arista MLS switch, ensure any unnecessary trunk links have not gained access to default VLAN 1; this can be verified with the command "show vlan brief":

```
switch(config)#sh vlan brief
VLAN Name                              Status    Ports
----- -------------------------------- --------- -------------------------------
---
1     default
8     VLAN0008                           active    Cpu
25    VLAN0025                          active    Cpu
100   VLAN0100                         active    Cpu
1000  VLAN1000                        active    Eth1, Eth15, Eth16, Eth17
4090  VLAN4090                        active    Eth2, Eth20, Eth32
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.15 ARST-L2-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must not use the default VLAN for management traffic.

```
GROUP ID: V-255983
RULE ID: SV-255983r991777
```

Rationale:

Switches use the default VLAN (i.e., VLAN 1) for in-band management and to communicate with directly connected switches using Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, the default VLAN may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Audit:

Verify the Arista MLS configuration for a Management_Network VRF instance globally on the switch with the following example:

```
switch(config)#sh run | sec vrf
ip name-server vrf default 192.168.10.20
!
vrf instance Management_Network
!
interface Ethernet12
   description MANAGEMENT NETWORK PORT
   no switchport
   vrf Management_Network
   ip address 10.10.40.254/30
!
ip routing vrf Management_Network
```

If the VRF is not configured to prevent the default VLAN from being used to access the switch, this is a finding.

Remediation:

Step 1: Configure the Arista MLS switch for a VRF instance for Management Network access by using the following commands:

```
switch(config)#vrf instance Management_Network
switch(config-vrf-Management_Network)#exit
```

Step 2: Configure the Ethernet port for VRF Management_Network and IP address for the management network traffic:

```
switch(config-if-Et12)#vrf Management_Network
switch(config-if-Et12)#ip address 10.10.40.254/30
switch(config-if-Et12)#exit
```

Additional Information:

CCI-004931 Establish organization-defined alternate communications paths for system operations organizational command and control.

- NIST SP 800-53 Revision 5::SC-47

1.16 ARST-L2-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have all user-facing or untrusted ports configured as access switch ports.

```
GROUP ID: V-255984
RULE ID: SV-255984r991778
```

Rationale:

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

Audit:

Review the Arista MLS switch configurations and examine all user-facing or untrusted switch ports configured as access switch ports.

```
switch(config)# show run interface ethernet 13 - 15
interface Ethernet13
   switchport access vlan 100
interface Ethernet14
   switchport access vlan 100
interface Ethernet14
   switchport access vlan 100
```

If any of the user-facing switch ports are configured as a trunk, this is a finding.

Remediation:

Configure the Arista MLS switch to disable trunking on all user-facing or untrusted switch ports.

```
switch(config)#interface ethernet 13 - 15
switch(config-if-Et13-15)#description disable trunking untrusted ports
switch(config-if-Et13-15)#switchport mode access
switch(config-if-Et13-15)#exit
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.17 ARST-L2-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista MLS layer 2 switch must have the native VLAN assigned to an ID other than the default VLAN for all 802.1q trunk links.

```
GROUP ID: V-255985
RULE ID: SV-255985r991779
```

Rationale:

VLAN hopping can be initiated by an attacker who has access to a switch port belonging to the same VLAN as the native VLAN of the trunk link connecting to another switch that the victim is connected to. If the attacker knows the victim's MAC address, it can forge a frame with two 802.1q tags and a layer 2 header with the destination address of the victim. Since the frame will ingress the switch from a port belonging to its native VLAN, the trunk port connecting to the victim's switch will simply remove the outer tag because native VLAN traffic is to be untagged. The switch will forward the frame on to the trunk link unaware of the inner tag with a VLAN ID of which the victim's switch port is a member.

Audit:

Review the Arista MLS switch configuration for all trunk ports to have a unique native VLAN ID that is not the default VLAN 1 by using the following example:

```
switch(config)#sh run | sec native vlan
interface Ethernet4
   description STIG Disable_VLAN 1 and native vlan to 1000
   switchport trunk native vlan 1000
   switchport trunk allowed vlan 2-4094
```

If the native VLAN has the same VLAN ID as the default VLAN, this is a finding.

Remediation:

Configure the interface trunk ports for the unique Native VLAN ID and configure the VLAN allowed by using the following commands:

```
switch(config)#interface Ethernet10
switch(config-eth10)#description #STIG VLAN 1 Pruning
switch(config-eth10)# switchport trunk native vlan 1000
switch(config-eth10)#switchport trunk allowed vlan 2-4094
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.18 ARST-L2-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Arista MLS layer 2 switch must not have any switch ports assigned to the native VLAN.

```
GROUP ID: V-255986
RULE ID: SV-255986r991780
```

Rationale:

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

Audit:

Review the configuration for all trunking ports to determine the native VLAN by using the following example (for vlan 1000):

```
switch(config-if-Et4)#sh run int eth4
interface Ethernet4
   description STIG Disable_VLAN 1 and native vlan to 1000
   switchport trunk native vlan 1000
   switchport trunk allowed vlan 2-999,1001-4094
switch(config-if-Et4)#
```

Review the configuration to ensure no access switch ports are configured in the native VLAN by using the following example (for vlan 1000):

```
swtich#sh vlan brief
VLAN  Name                             Status    Ports
----- -------------------------------- --------- -------------------------------
---
1     default
8     VLAN0008                         active    Cpu
25    VLAN0025                        active    Cpu
100   VLAN0100                       active    Cpu
1000  VLAN1000                      active
4090  VLAN4090                      active
```

If any access switch ports have been assigned to the same VLAN ID as the native VLAN, this is a finding.

Remediation:

Configure the Arista MLS switch to ensure all access switch ports use a VLAN other than the native VLAN.

Configure all access switch ports to a VLAN other than the designated native VLAN by using the following example:

```
switch(config)#interface Ethernet 21
switch(config-Eth21)# switchport access vlan xxxx
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	ARST-L2-000020 (Manual)	☐	☐
1.2	ARST-L2-000030 (Manual)	☐	☐
1.3	ARST-L2-000050 (Manual)	☐	☐
1.4	ARST-L2-000060 (Manual)	☐	☐
1.5	ARST-L2-000070 (Manual)	☐	☐
1.6	ARST-L2-000090 (Manual)	☐	☐
1.7	ARST-L2-000130 (Manual)	☐	☐
1.8	ARST-L2-000110 (Manual)	☐	☐
1.9	ARST-L2-000100 (Manual)	☐	☐
1.10	ARST-L2-000140 (Manual)	☐	☐
1.11	ARST-L2-000160 (Manual)	☐	☐
1.12	ARST-L2-000170 (Manual)	☐	☐
1.13	ARST-L2-000180 (Manual)	☐	☐
1.14	ARST-L2-000190 (Manual)	☐	☐
1.15	ARST-L2-000200 (Manual)	☐	☐
1.16	ARST-L2-000210 (Manual)	☐	☐
1.17	ARST-L2-000220 (Manual)	☐	☐
1.18	ARST-L2-000230 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 27, 2025	1.0.0	Initial CIS Release