Create a Remote Log Source - Cisco ISR.mobile.phone

Create a Remote Log Source (Cisco ISR)

Topics Discussed

To obtain Log Relay and to configure your account for remote log collection, you must have the following AMP permissions added to your account:

- Write Virtual Machine
- Delete Log Management
- Read Log Endpoints
- Read Log Relays
- Write Log Relays
- Delete Log Relays

You can use this document to send Cisco Integrated Services Router (ISR) logs to Armor's Security Information & Event Management (SIEM).

This document only applies to:

- Cisco Integrated Services Router (ISR) (IOS)

Pre-Deployment Considerations

To create a remote Log Relay, you must already have:

- Added Log Relay to your account
  - To learn how to add Log Relay to your account, see Obtain Log Relay for Remote Log Collection.
- Configured the system clock

Update Your Cisco ISR Device

1. Log into your Cisco ISR device.
2. Access the privileged EXEC mode:

```
hostname> enable
```

3. Access the global configuration mode:

```
hostname# configure terminal
```

4. Enable logging:

```
hostname(config)# logging on
```

5. Configure the global logging settings:

```
hostname(config)# no logging console
hostname(config)# logging trap warning
hostname(config)# logging origin-id hostname
```

6. Configure the logs to be sent to a designated Armor Log Relay device:

```
hostname(config)# logging source-interface <interface>
hostname(config)# logging host <ipaddress> transport <protocol> port <port>
```


- In **<interface>**, enter the name of the Cisco ISR interface, such as GigabitEthernet 1.
- In **<ipaddress>**, enter the IP address of the designated Armor Log Relay device.
  - To locate your IP address in AMP, in the left-side navigation, click **Infrastructure**, click **Virtual Machines**, and then review the **Primary IP** column for the corresponding virtual machine.
- For <**protocol**> and <**port**>,
  - For UDP, enter **transport udp port 10117**.
    - Armor recommends that you use UDP.
  - For TCP, enter **transport tcp port 10117**.

7. Exit the configuration:

```
hostname(config)# exit
```

8. Save the changes:

```
hostname# write memory
```

9. Review the logging configuration:

```
hostname# show run all logging
logging enable
logging timestamp
logging hide username
logging buffer-size 4096
logging asdm-buffer-size 100
logging buffered warnings
logging trap warnings
logging asdm warnings
logging device-id hostname
logging host inside 100.64.0.10 17/5140
logging flash-minimum-free 3076
logging flash-maximum-allocation 1024
```


If present, **logging standby** enables logging on a standby unit with failover enabled. As a result, this option causes increases traffic on the syslog server.

Troubleshooting

Verify that logs are formatted correctly, similar to the following example:

```
May 22 2019 16:11:55 asav-984 : %ASA-4-411004: Interface Management0/0, changed state to
administratively down
```

Was this helpful?

Your Rating:

Results:

1 rates