AQUILA - Cisco Meraki Integration

Cisco Meraki provides a centralized cloud management platform for devices like MX Security Appliances, MR Access Points, and more. Its cloud-based architecture enables secure, scalable networks manageable from anywhere via the Meraki Dashboard or Mobile App. Each Meraki network generates events that can be collected and analyzed.

Integration Overview

This integration supports event collection through:

- **Syslog** messages from Meraki devices

Events can be searched, observed, and visualized.

Compatibility

- Supports event collection from **MX Security Appliances** and **MR Access Points** via syslog.
- **MS Switch** events are **not supported** and will not be recognized.

Syslog Setup:

1. I**dentify Syslog-ng IP Address**

Access the log collector virtual machine and open a terminal. Run the following command to determine the IP address of the syslog-ng server:

```
ifconfig -a
```

> Please take note of the IP address, as this will be referenced during the configuration.

2. **Install Syslog-ng**

Install syslog-ng along with its required dependencies using the following command:

```
sudo apt-get install syslog-ng
```

3. **Configure Syslog-ng**

Edit the syslog-ng configuration file:

```
sudo nano /etc/syslog-ng/syslog-ng.conf
```

> Locate the following line:

```
log { source(s_src); filter(f_crit); destination(d_console); };
```

> Add the configuration below it, ensuring that Server_IP_Address and <MERAKI_IP_ADDRESS> are replaced with the appropriate values:

```
# Define syslog source
source s_net { udp(ip(Server_IP_Address) port(5140)); };

# Create filter to match traffic (this filter will catch all syslog messages from the MX)
filter f_meraki { host("<MERAKI_IP_ADDRESS>"); };

# Define a destination for syslog messages
destination df_meraki { file("/var/log/cisco_meraki.log"); };

# Bundle the source, filter, and destination rules together
log { source(s_net); filter(f_meraki); destination(df_meraki); };
```

4. **Restart Syslog-ng**
After saving the configuration, restart the syslog-ng service to apply the changes:

```
sudo /etc/init.d/syslog-ng restart
```

Configuring the Cisco Meraki Integration

Once the syslog-ng server is configured, please proceed with the following steps in the Cisco Meraki dashboard:

1. **Log in to the Cisco Meraki dashboard.**

2. **Navigate to Network-wide > Configure > General.**

3. **Click Add a syslog server.**

4. **Populate the required fields as follows:**

- Server Address: Syslog server IP address
- Port: 10514
- Protocol: UDP

5. Under Roles, enable**:**

- Switch Event Log
- Wireless Air Marshal Events
- Wireless Flow

> Optional: Configuration Verification

To verify successful log ingestion, access the syslog server and run:

```
cd /var/log/
ls
```

> If the file **cisco_meraki.log** is present, the configuration has been successfully applied and logs are being received.

Log Rotation Configuration

To manage log growth and prevent disk space issues, please configure log rotation as follows:
Create a logrotate configuration file:

```
sudo nano /etc/logrotate.d/meraki
```

Add the following content:

```
/var/log/cisco_meraki.log {
    daily
    missingok
    rotate 1
    compress
    delaycompress
    notifempty
    create 0640 root root
    postrotate
        # Optional commands, such as reloading syslog services
```

```
        # /etc/init.d/syslog-ng reload
    endscript
}
```

Log Events

Enable this option to collect Cisco Meraki log events across all applications configured for the selected log stream.

Logs Dataset

- The `cisco_meraki.log` dataset contains events collected from the configured syslog server.
- All Cisco Meraki specific syslog fields are available under the `cisco_meraki.log` field group for detailed analysis.

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #6
Created 2 July 2025 12:13:47 by Richmond Abella
Updated 19 June 2026 12:10:21 by Benjie Janlay Jr.