Network Automation with Event-Driven Architecture

in Agentic Era

Kareem Iskander
Principal Engineer, Learn with Cisco
@kareem_isk

Session ID: CISCOU-1607

Agenda

01 Introduction

02 Event-Driven Architectures

03 NetBox Events

04 Splunk HEC

05 Meraki Alerts

06 Automation with AI

07 Live Demo

08 Conclusion

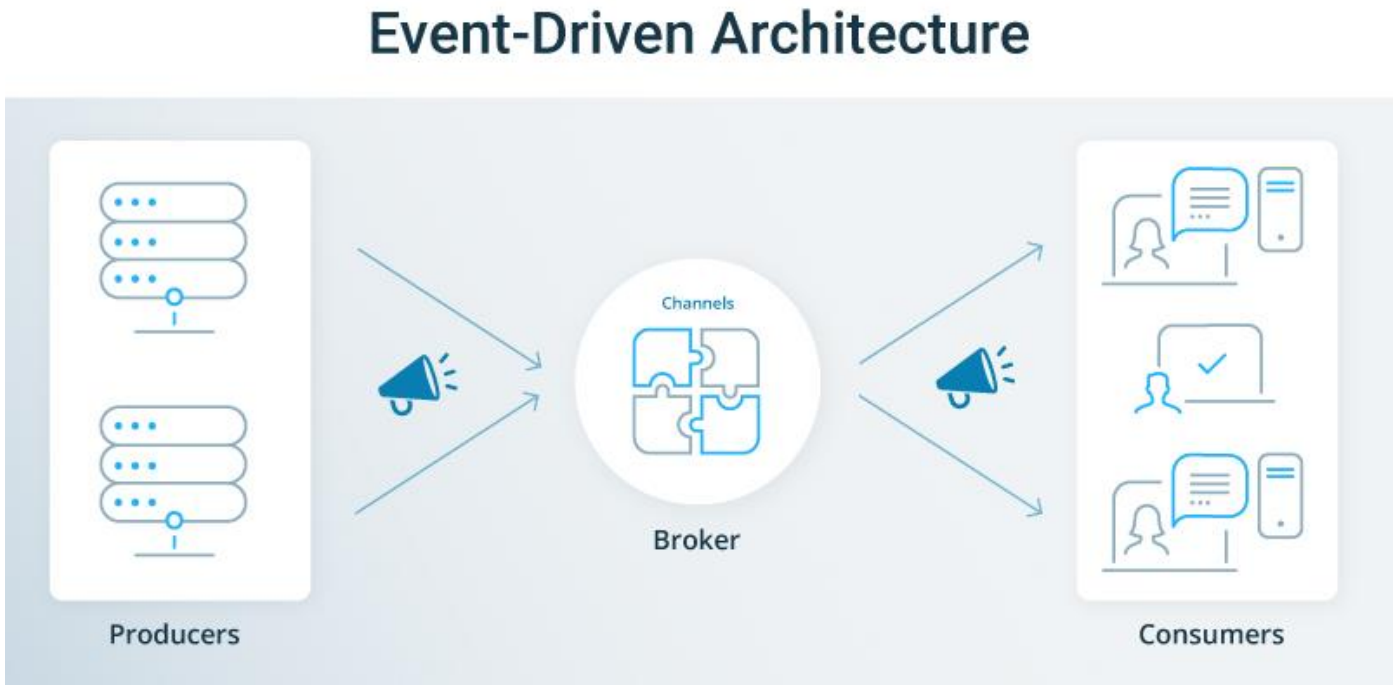
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Introduction

What is Event-Driven Architecture?

Event-Driven Architecture (EDA) is a software design pattern where decoupled components communicate through events.



© 2025 Cisco and/or its affiliates. All rights reserved.

Event-Driven Architectures

Event-Driven Architecture (EDA)

Core Components

- **Event Producers:** Generate events when actions occur.
- **Event Brokers:** Transport events from Producers to Consumers.
- **Event Consumers:** Listen for and process events.

Producers

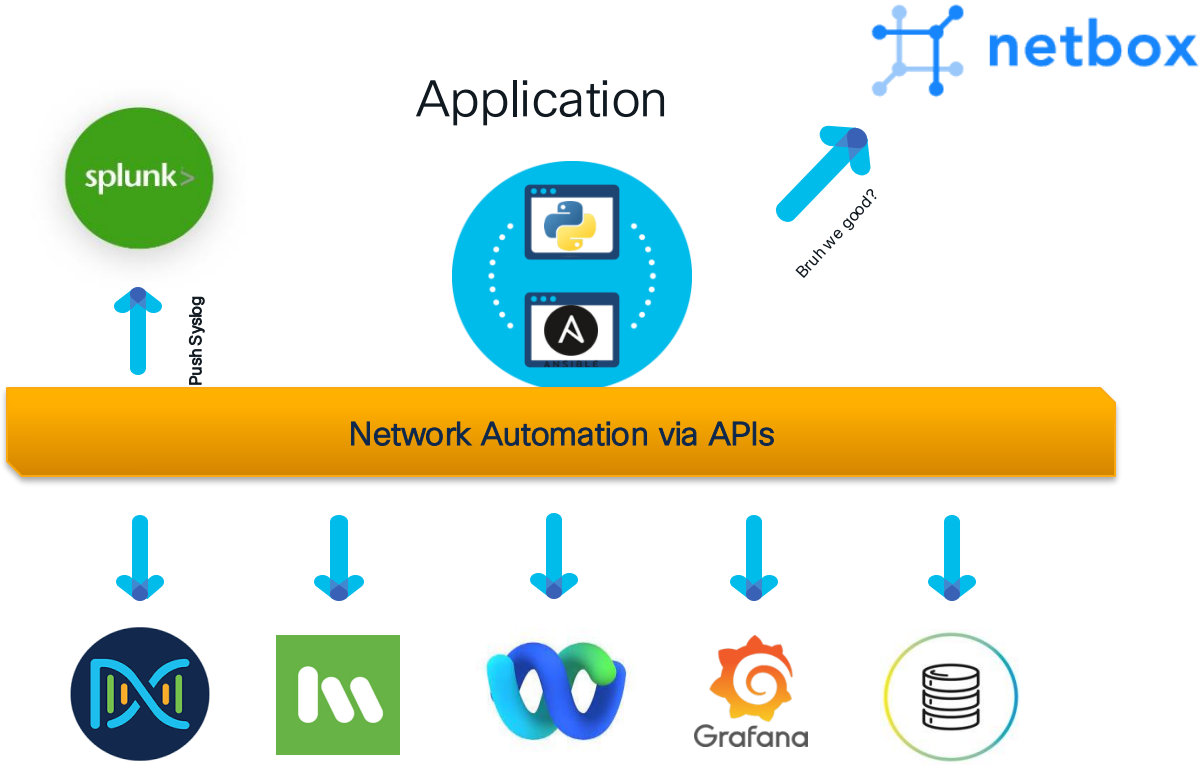
Brokers

Consumers

© 2025 Cisco and/or its affiliates. All rights reserved.

Network Automation – As we know it

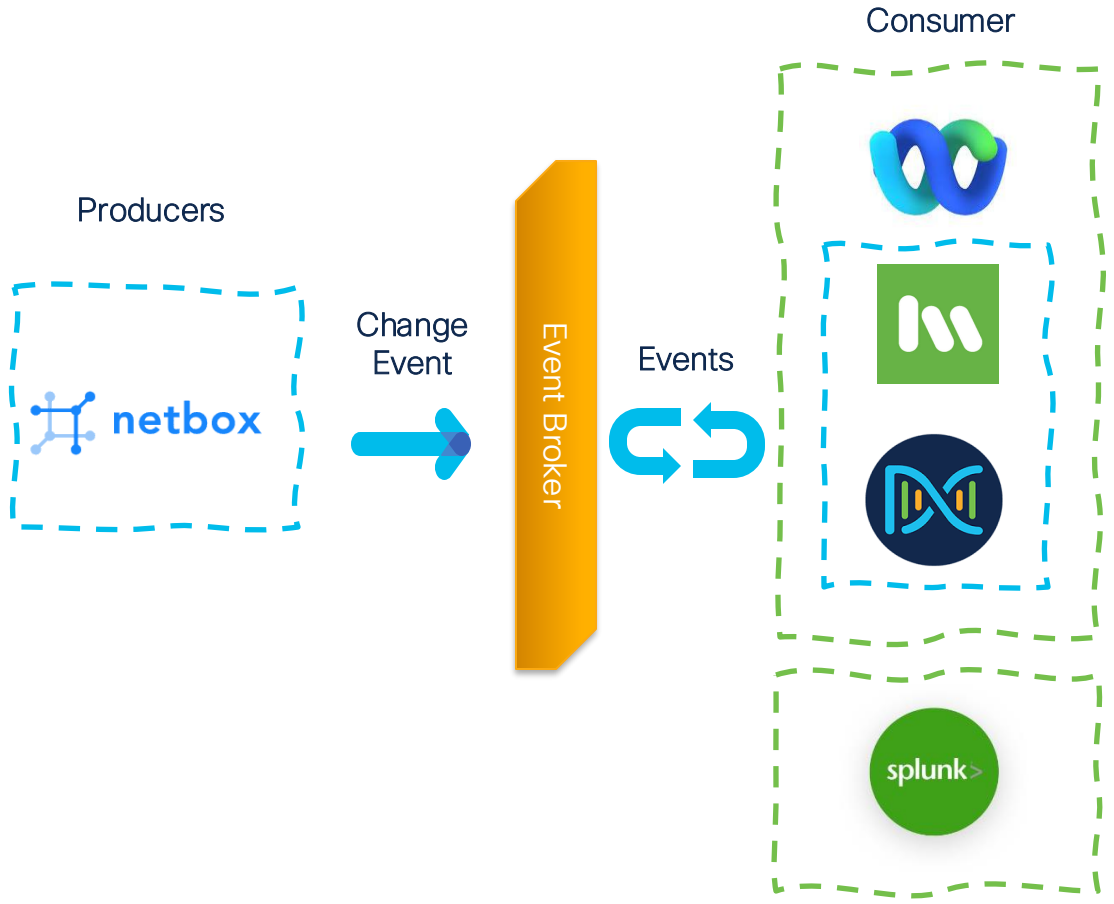
- Automation Script
- Read from Source of Truth
- Check Network Devices
- Compare Changes or Make Changes
- Store Audit Log



© 2025 Cisco and/or its affiliates. All rights reserved.

Network Automation – Event Driven

- Change Events fired
- Broker receives events
- Directs messages to the recipient
- Consumer updates
- Some consumers are also producers



© 2025 Cisco and/or its affiliates. All rights reserved.

Use Case

Use Case

- Carl – Network Automation Engineer.
- Maintain **a single source of truth** for your network configuration.
- Automate config changes and prevent config drift.
- Security – audit log of changes in a single source

© 2025 Cisco and/or its affiliates. All rights reserved.

Use Case - Components

Source of Truth

Network Controller

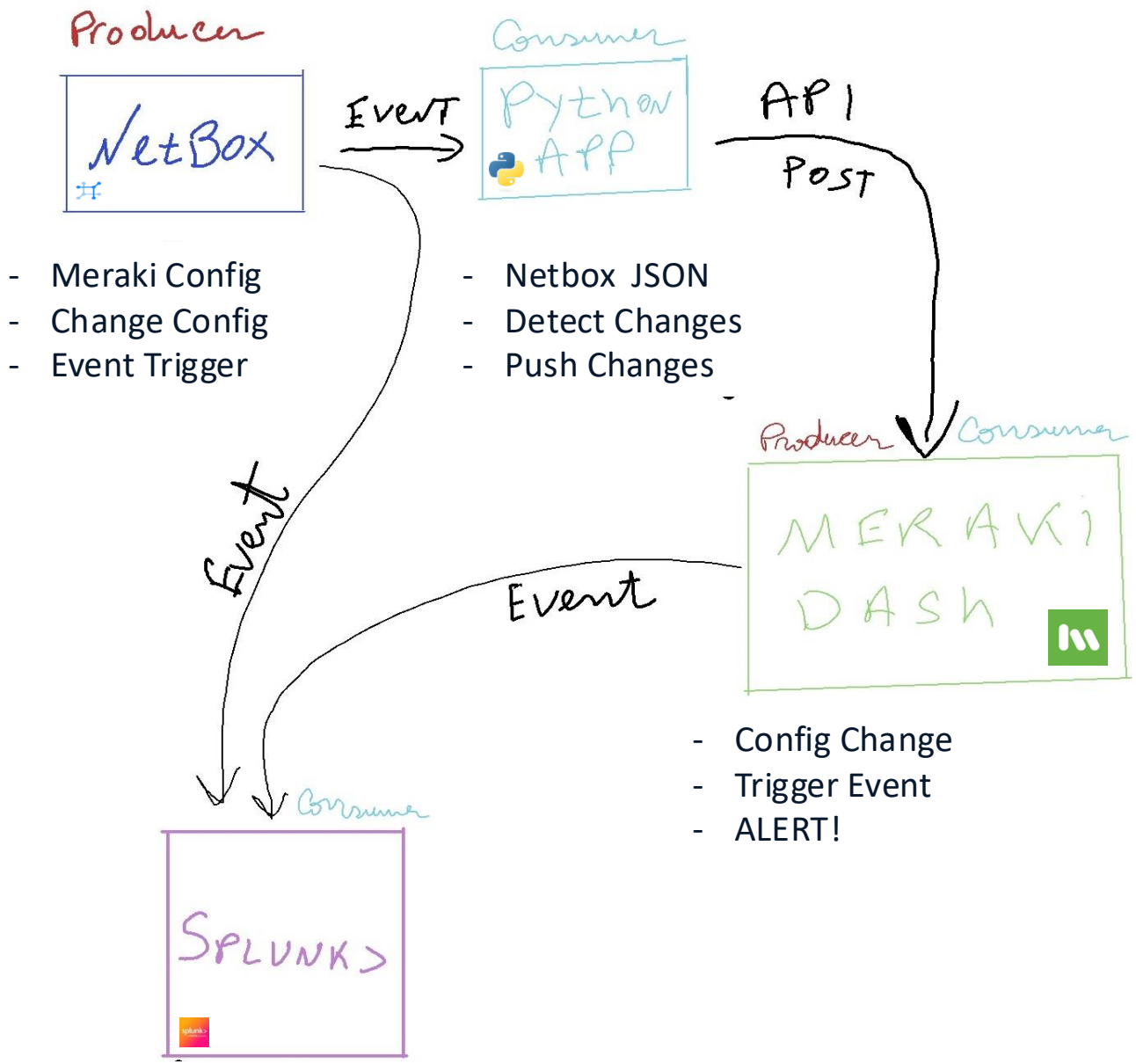
Middleware

Observability

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Architecture Design



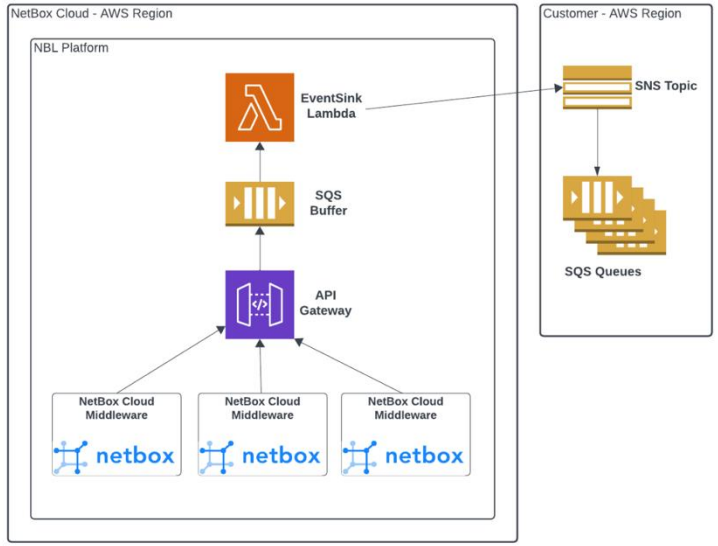
© 2025 Cisco and/or its affiliates. All rights reserved.

NetBox Events

NetBox Events

Event Streams

- Available for NetBox Cloud
- Continuously broadcast all NetBox changes in real time
- Requires a backend setup

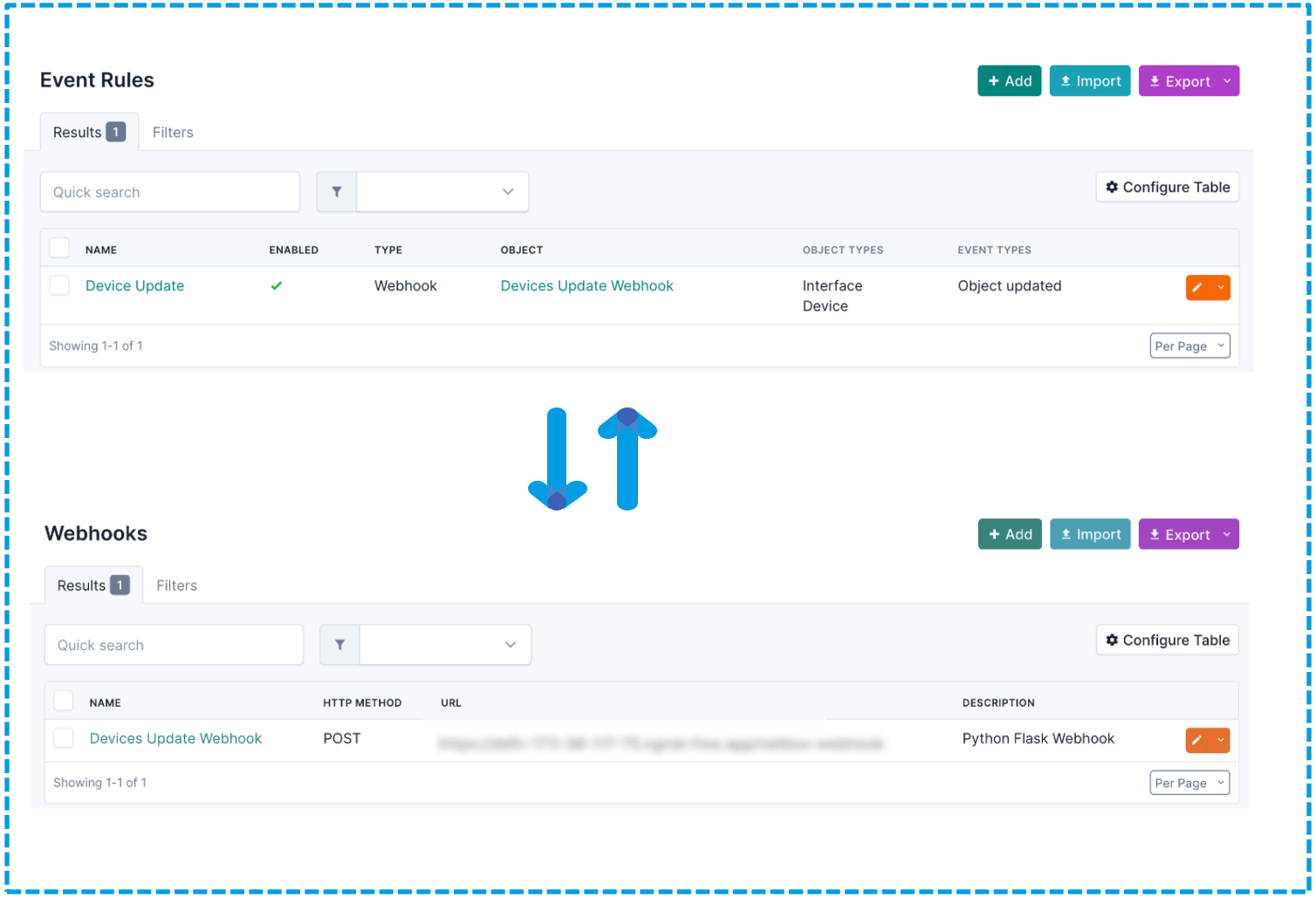


Webhooks

- Available on all NetBox platforms
- Trigger HTTP POST requests for specific NetBox changes
- Can be setup through the UI

© 2025 Cisco and/or its affiliates. All rights reserved.

NetBox Webhooks + Event Rules



JSON Payload

```
{
    "event": "updated",
    "model": "device",
    "timestamp": "2025-01-28T12:34:56Z",
    "data": {
        "name": "SW-1",
        "serial": "QBSB-XYZ-1234",
        "primary_ip4": {
            "address": "192.168.X.X/24"
        },
        "custom_fields": {
            "gateway_ip": "192.168.X.1"
        }
    }
}
```

```
$ python app.py
```

AWS Lambda

CISCO Meraki

© 2025 Cisco and/or its affiliates. All rights reserved.

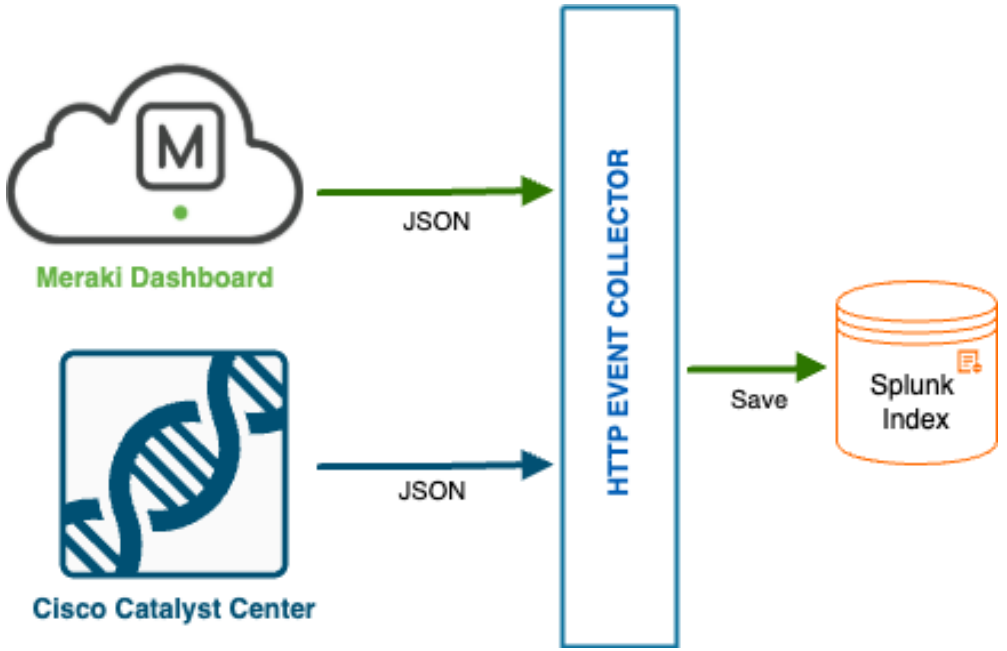
cisco

Splunk Events

Webhooks | Understanding Splunk HEC

HTTP Event Collector (HEC)

- Splunk Service that allows clients to send event data to Splunk via HTTP(S)
- Useful for Devices where forwarders can't be installed (Cloud Managed Devices)
- Token-based authentication ensures that only authorized clients send data
- Works with JSON-formatted event data
- Link to a Splunk Index
- Data is available in the Search Head



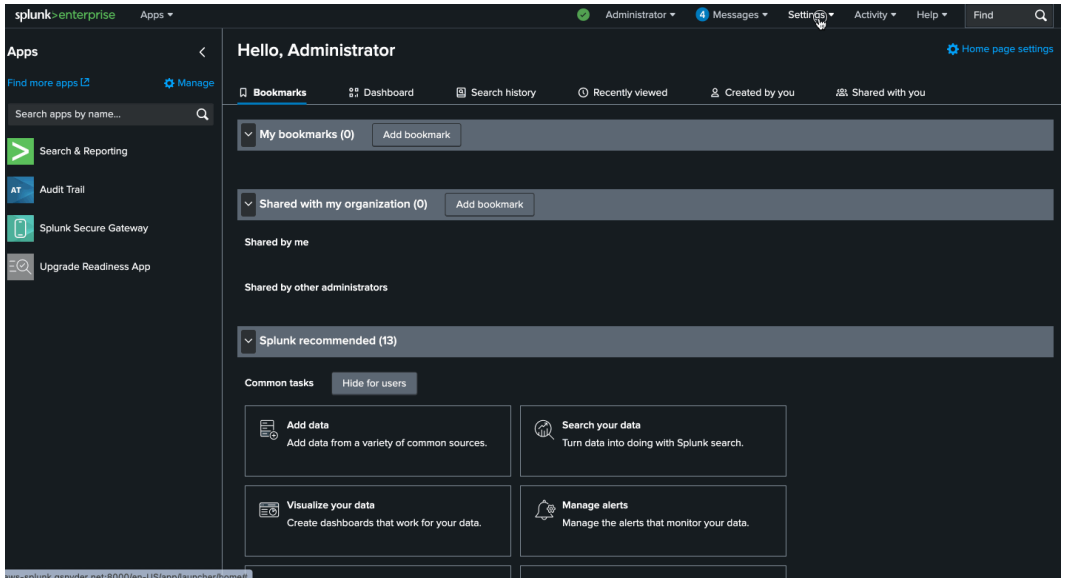
© 2025 Cisco and/or its affiliates. All rights reserved.

Configuring the HEC out of Splunk

It's Easy as 1 , 2 , 3

1. Create New Token to Authenticate Webhook
2. Configure and Connect to an Indexer
3. Generate and Capture HEC URL

   https://<splunk server>:8088/services/collector/event



© 2025 Cisco and/or its affiliates. All rights reserved.

HEC | The Good, The Bad & The Ugly

1. Security Risks Without Proper Configuration

If **SSL encryption** is not used, data is sent in plaintext.

2. Reliance on Custom Clients

Developers must implement logic to format data in **JSON**, handle **HTTP headers**,

3. Limited Retry Logic Without Acknowledgment

Without **Indexer Acknowledgment** enabled, there's **no guarantee** that data was successfully indexed.

4. Port and Firewall Dependencies

HEC typically uses **port 8088**

© 2025 Cisco and/or its affiliates. All rights reserved.

Meraki Events

Meraki + Splunk

Syslog Protocol

- Send Log Data from various devices on the Network (e.g., switches, access points)
- Ideal to use Universal Forwarder to Splunk

Webhooks

- Filter on specific Alerts
- Flexibility with Templating (Liquid Template)
- Push Alerts to Splunk
- Ideal to use Heavy Forwarders to Splunk
- Use HEC

© 2025 Cisco and/or its affiliates. All rights reserved.

Configure Meraki Events

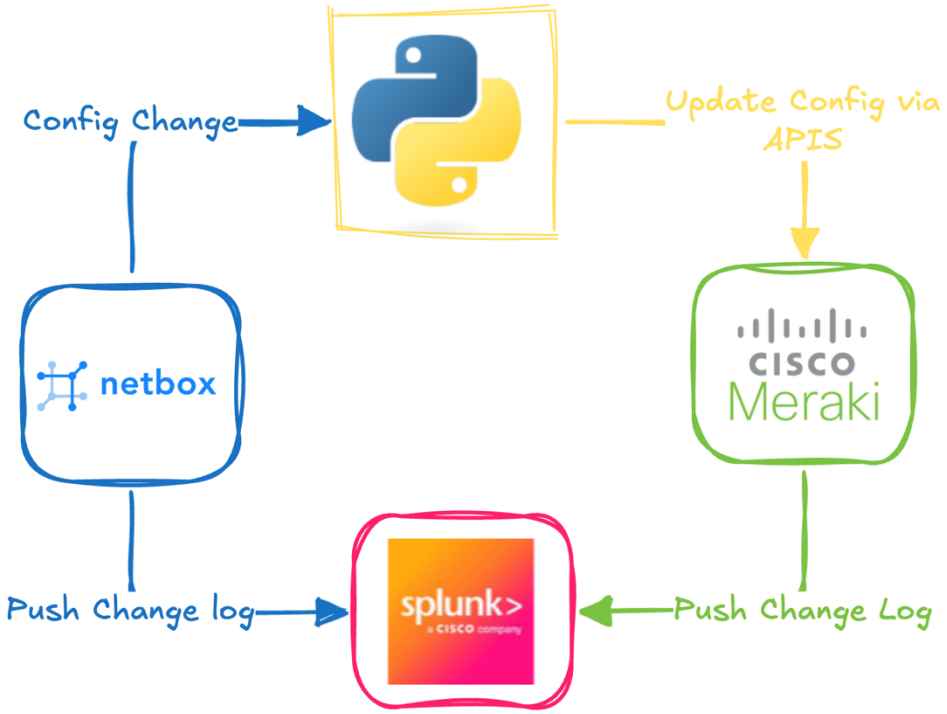
1. Build a Webhook template in Meraki Dashboard, using Liquid Templates to format the data.
2. Configure a Receiver, in this case, Splunk HEC, to send the data.
   - URL: https://<splunk-server>:8088/services/collector/event/raw make sure you use /raw at the end of the URL
   - Shared Secret: HEC Token
3. Select the Alerts that we want to send to Splunk.

© 2025 Cisco and/or its affiliates. All rights reserved.

Putting It All Together

In a perfect world ...

- All config changes start in NetBox
- NetBox fires off a Webhook
- Middleware updates config
- Meraki pushes change log
- Splunk stores logs

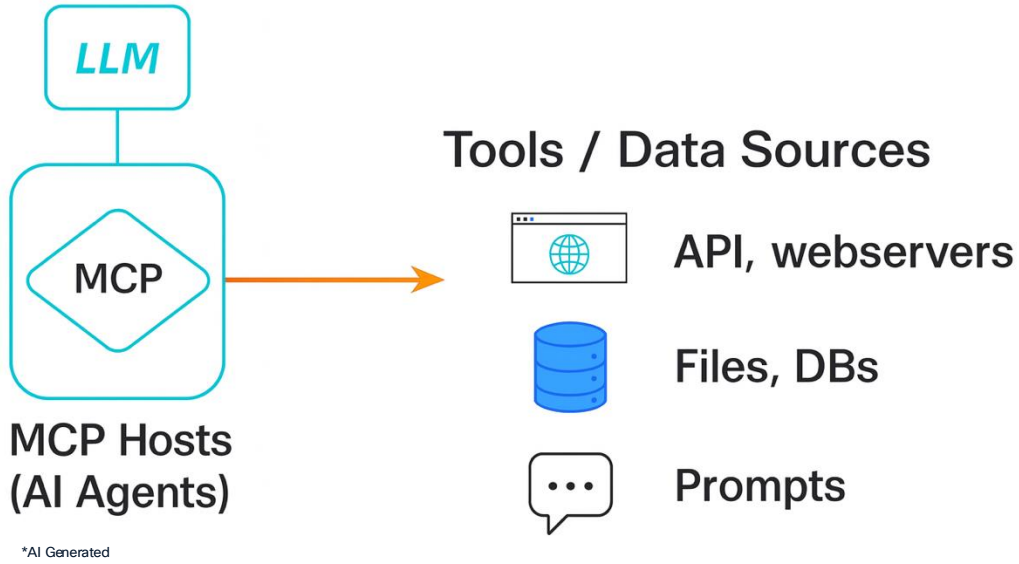


© 2025 Cisco and/or its affiliates. All rights reserved.

Network Automation with MCP

MCP – The USB-C for AI Agents

- **Model Context Protocol (MCP):**
  - Open standard developed by Anthropic
  - Connects AI Agents with external data & tools
  - Defines a simple **Host-Protocol-Server architecture**
  - Exposes **primitives**: Tools (actions), Resources (data), Prompts (templates)



© 2025 Cisco and/or its affiliates. All rights reserved.

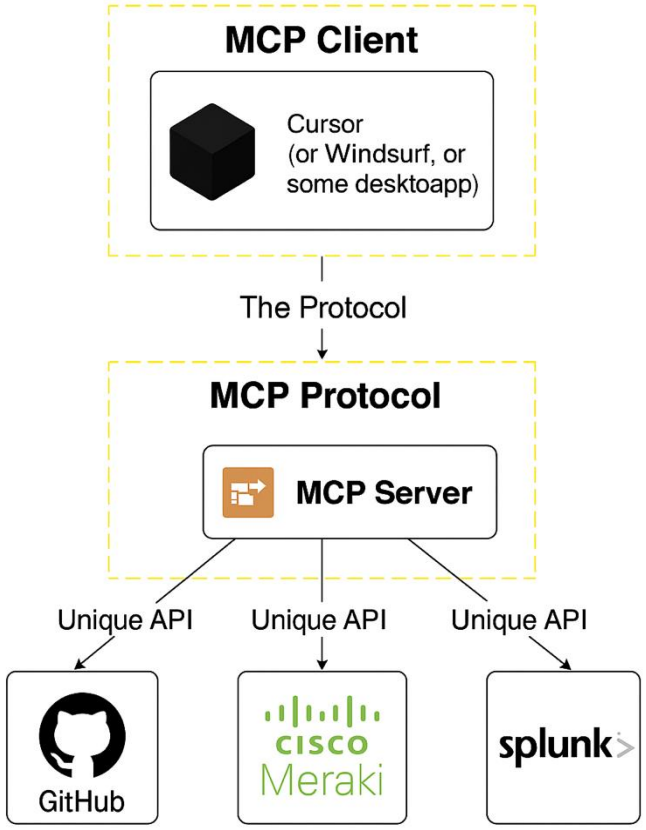
Quick Introduction to MCP

MCP – Model Context Protocol

- **Model Context Protocol (MCP)** is an **open standard** that standardizes how applications provide context to large language models (LLMs).

Three Key Components:

- **MCP Hosts**: Applications like Claude Desktop or IDEs that initiate connections to MCP Servers.
- **MCP Clients**: Components within the host application that maintain connections with MCP Servers.
- **MCP Servers**: Programs that provide context, tools, and prompts to clients
  - **Resources** – Provides access to data (files, code, messages, etc.)
  - ***Tools*** – *Offers callable functions (e.g., search, API calls)*
  - **Prompts** – Supplies context-specific instructions or templates



*AI Generated

© 2025 Cisco and/or its affiliates. All rights reserved.

Demo Time!

Thank you

CISCO