
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Health Monitoring in Next Generation Firewall

Jayesh Chhapekar, Principal Engineer
@j_chhapekar

BRKSEC-1022

About me

Jayesh Chhapekar

Principal Engineer, Security Business Group working on Next Generation Firewall.

- MS, computer Science with 25+ years of experience designing networking products
- Lead Architect for Device Health Monitoring platform
- Passionate about, simplifying product & user experience
- Co-ordinates:
  - jchhapek@cisco.com
  - https://www.linkedin.com/in/jayeshchhapekar/
  - https://twitter.com/j_chhapekar

Agenda

- Introduction
- Walkthrough of the FMC UI for health monitoring
- Common use-cases walkthrough
- Monitoring devices on Azure Application Insight*
- Conclusion

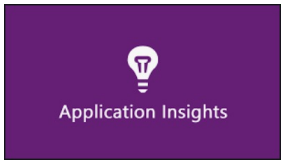
Introduction

What is Health Monitoring Platform

Provides comprehensive visibility and analysis into health & performance

Collect
USE Metrics

Stream



Trend Charts

Event Overlays

Custom Dashboard

FMC

Amazon CloudWatch

Render

Why invent new health monitoring

- Device visibility has been limited

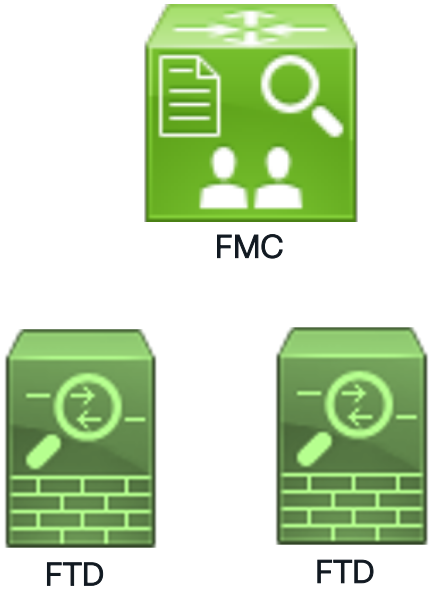


Table of Metrics

SysLogs

CLI

SNMP

Hard to Operationalize

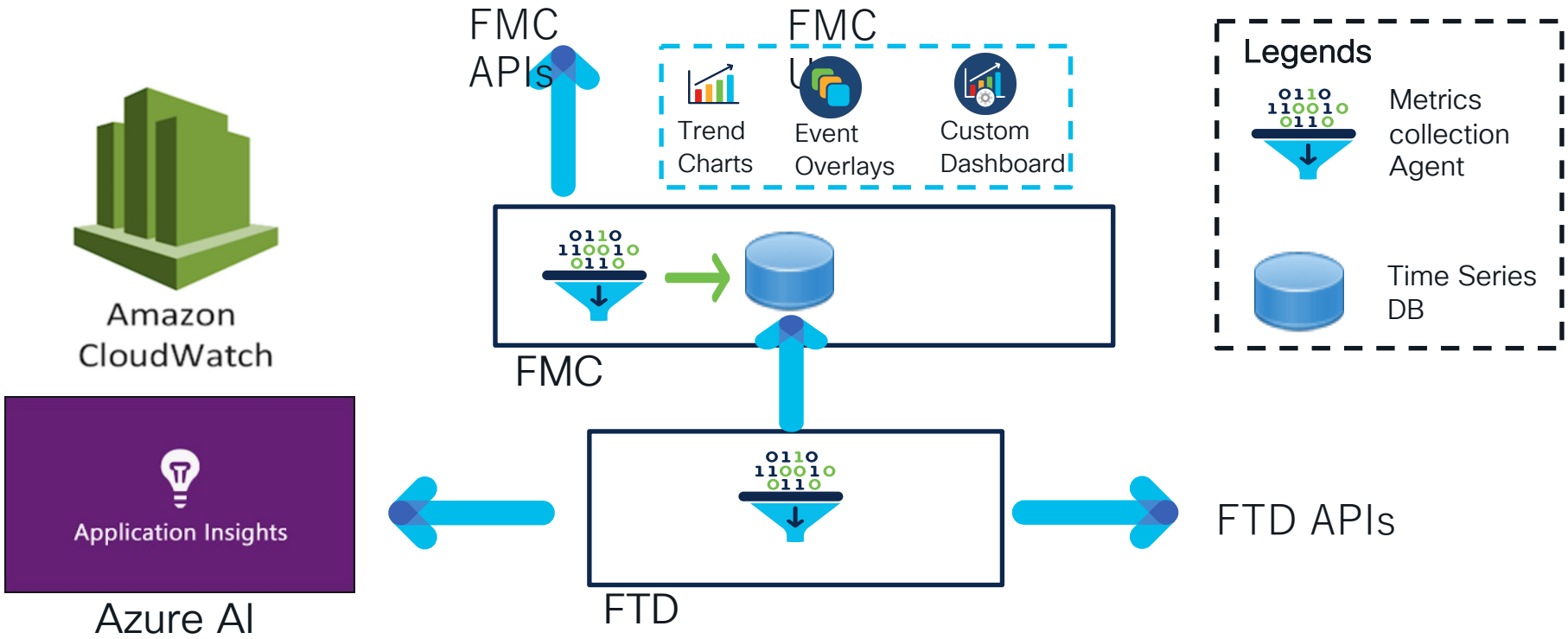
Hard to correlate

Hard to do causal analysis

Device-Specific

Slow

Functional description



FMC UI walkthrough

FMC UI walkthrough

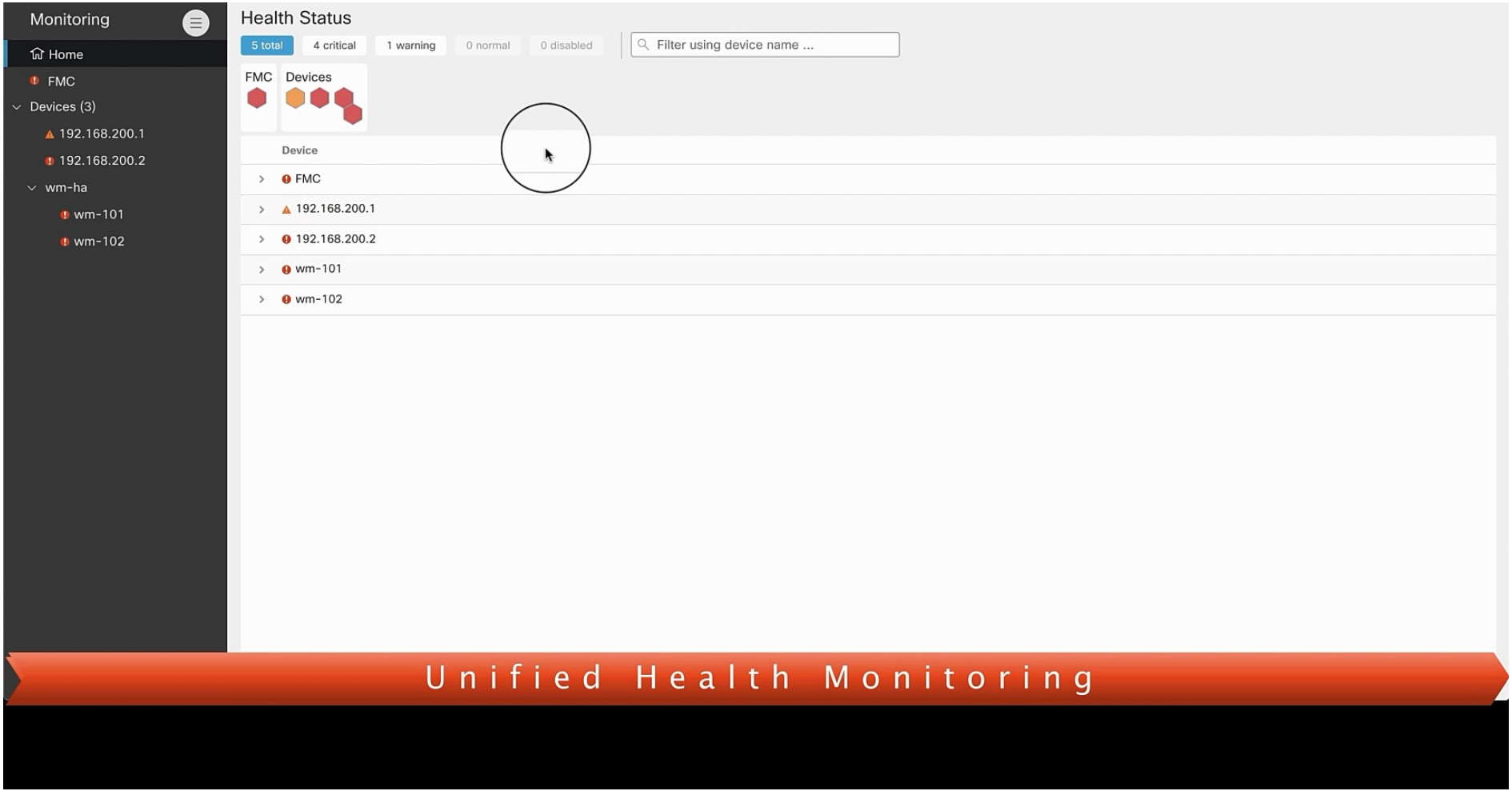
- FMC UI provides rich features
  - Trend Charts, event overlays and custom dashboards
- The coming demo would provide deep dive into FMC UI
  - to understand bells & whistles
  - The key features

FMC UI demo

Common usecases walkthrough

- Visibility into network traffic and device health
- Debugging with health monitoring dashboard

Common usecases demo



FTD HA split brain detection

Introduction – FTD HA Split Brain Detection (new)

- Split brain – both FTD devices in HA pair: Active – Active
- Can be caused by:
  - Communication failure between the two FTDs
  - Delay in sending or processing state updates
- It causes:
  - Network disruption
  - Blackholing
- Monitoring split brain
  - FMC monitors status of both devices and report when both are Active

FTD HA Split Brain Detection (new)

- The feature will be generally available in second half of year 2021.
- FTD V7 – Customer Beta opened since 7 Feb 2021

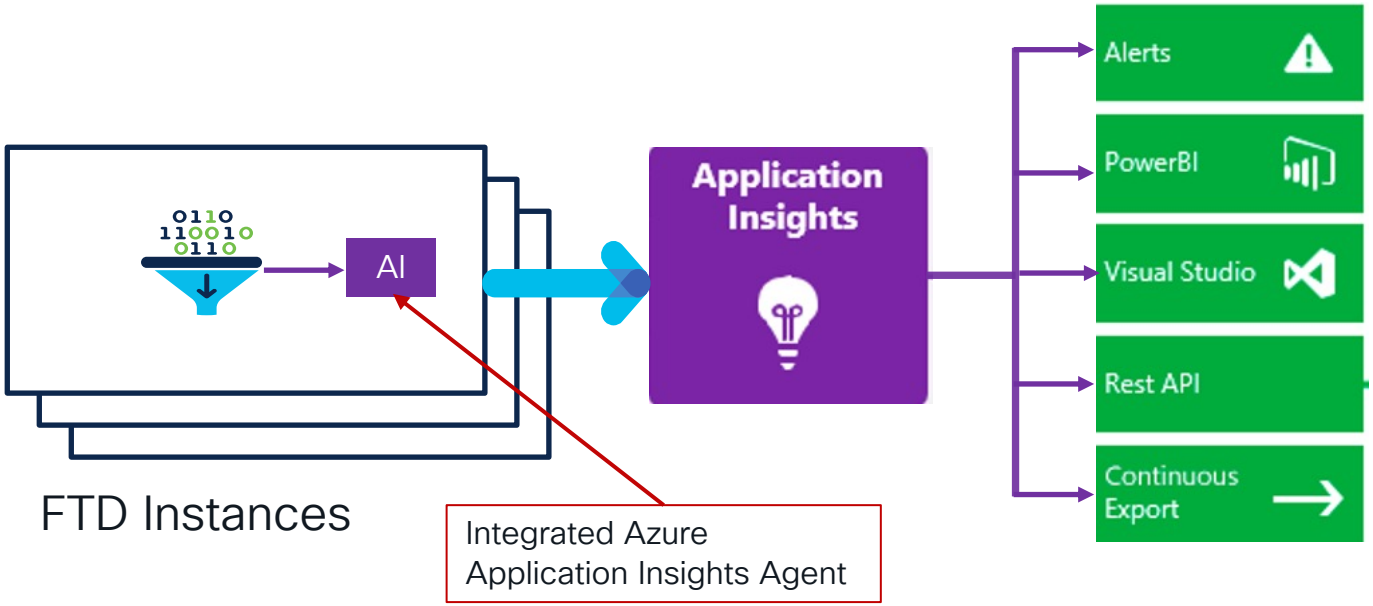
- The demo will cover:
  - Detecting split brain and taking corrective action

FTD HA split brain detection demo

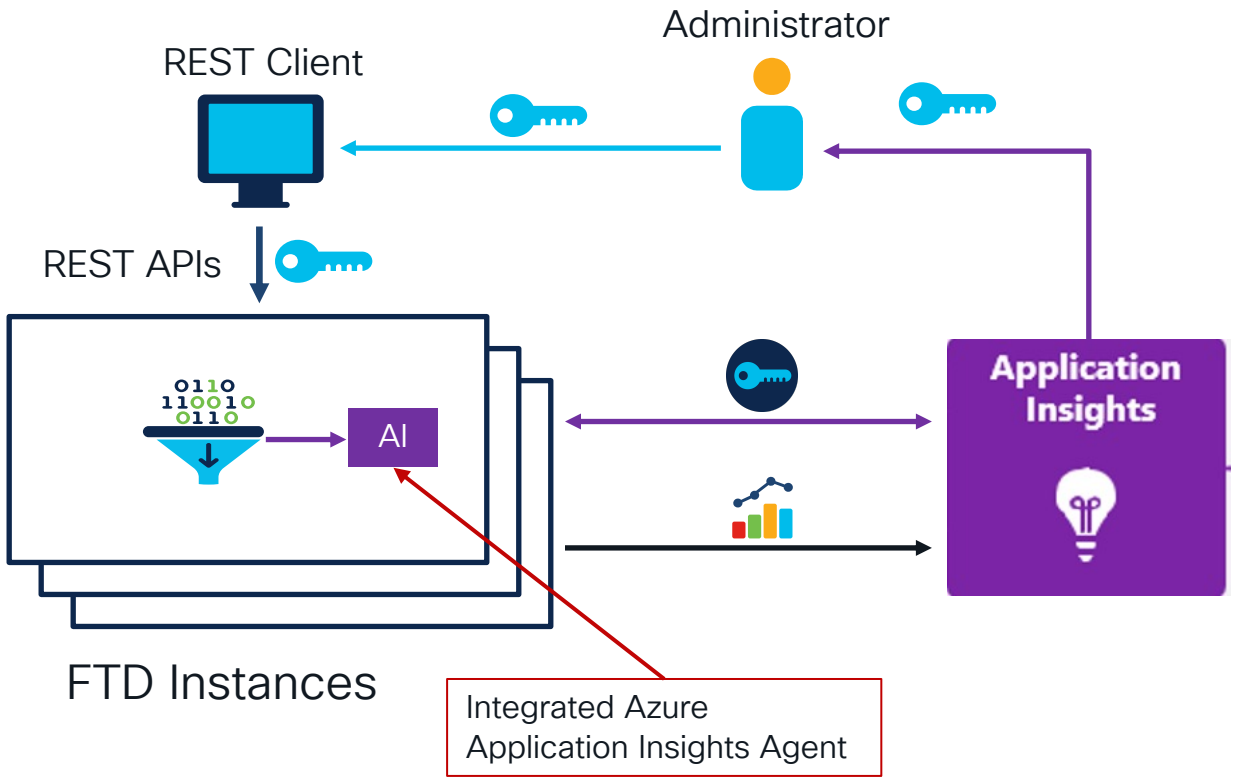
Monitoring FTDs @ Azure Application Insights

cisco Live!

Azure Application Insights monitoring architecture

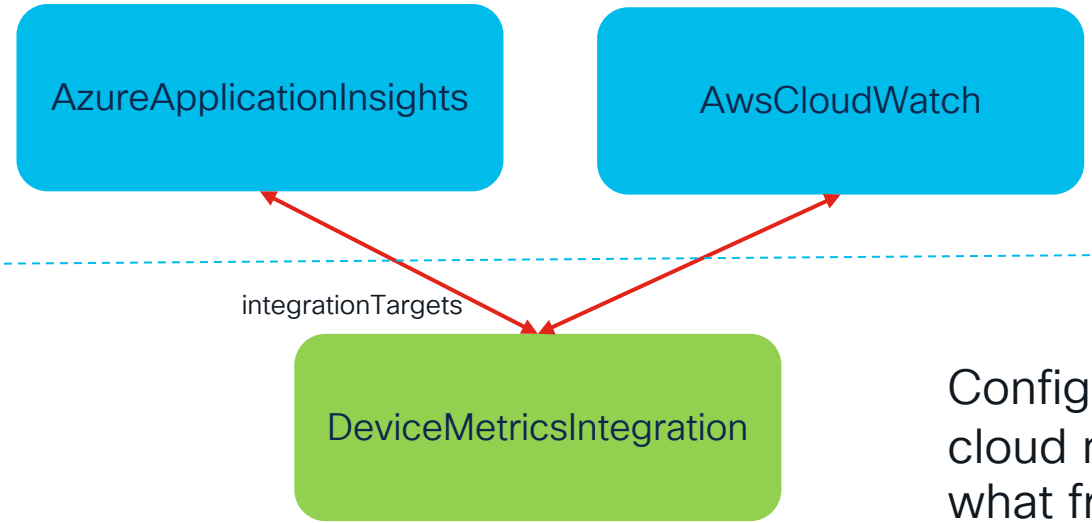


Configuration & Monitoring Flow



REST APIs configuration

Need to configure two objects:



Configure the Cloud Credentials in FTD

Configure Metrics to be sent to cloud monitoring system and at what frequency

Demo – configuration and monitoring on Azure Application Insights

The demo will cover...

- Creating Azure Application Insights (AI) Instance on the Azure portal
- Configuring FTD device to send metrics to Azure AI
- Viewing the metrics on Azure Application Insights
- Configuring Grafana application to pull metrics from Azure Application Insights
- Downloading Grafana dashboard and configuring it to start monitoring

FTD monitoring on Azure Application Insights

- The feature will be generally available in May 2021.
- FTD V7 – Customer Beta opened since 7 Feb 2021

- This concludes all of the demos and presentation…

Conclusion

- The session demonstrated:
  - Monitoring via FMC User Interface
  - Monitoring via Azure Application Insights dashboard
  - Visibility into device's health and traffic
  - Troubleshooting of configuration error with event overlays
- These are just examples
  - Many possible ways by which the feature can be used
- Please provide feedback and suggestion on how to make this feature more useful and relevant

More information, next steps, call for action

- Link to detailed documentation: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/health_monitoring.html
- New feature introduction – health monitoring in release 6.7: https://www.youtube.com/watch?v=ualSK2e3cMg
- Please register for Beta Program
- Details of more related videos in Cisco Live 2021.. On next page

Related Sessions on network security in CL 2021

- BRKSEC-2016 *Firepower Virtual Routing and Forwarding (VRF)*
- BRKSEC-2014 *Deploy Network Security as Code Using DevOps*
- **BRKSEC-2106** ***TLS Server Identity Discovery on Cisco Secure Firewall (Threat Defense)***
- BRKSEC-2029 *Security in an Encrypted World: Enhancing Firewalls, IPS, and Proxies*
- BRKSEC-2417 *Keeping Up on Network Security with Cisco Secure Firewall*
- BRKSEC-2411 *Zero Trust: Securing Applications and Workloads Using a Cloud Native Approach*
- BRKSEC-2412 *Leveraging Endpoint Security in Our Encrypted World!*
- BRKSEC-2415 *The Future of Network Security is in the Cloud with Cisco SASE!*
- BRKSEC-3008 *Demystify Public Cloud Security Using Secure Firewall and Tetration*

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive