Cisco live!
January 29 - February 2, 2018 · Barcelona
Tetration Hands-on Lab from Deployment to Operations Support

Furong Gisiger, Solutions Architect
Lawrence Zhu, Sr. Solutions Architect
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#LTRACI-2184
Agenda

- Tetration Introduction
- Sensor Installation and Monitoring
- Inventory | Annotation | Scope | RBAC
- Flow Search | Application Workspaces
- Service Status | Cluster Status | VM Information
- Monitoring – Charts | Cluster | Alerts
- Maintenance – Explore | Snapshots
- Lab Setup
## Recommended Tetration Sessions

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Session Title</th>
<th>Session Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSOACI-4591</td>
<td>Tetration Overview</td>
<td>Product or Strategy Overview</td>
</tr>
<tr>
<td>TECDCI-1757</td>
<td>Technical seminar for Tetration analytics</td>
<td>Technical Seminars</td>
</tr>
<tr>
<td>BRKACI-2040</td>
<td>Tetration Analytics – Network Analytics &amp; Machine Learning Enhancing Data Center Security and Operations</td>
<td>Breakout Session</td>
</tr>
<tr>
<td>BRKACI-2060</td>
<td>Cisco Tetration: Data Center Analytics Deployment and Use Cases</td>
<td>Breakout Session</td>
</tr>
<tr>
<td>BRKACI-2509</td>
<td>Customer Data Center Insights using Tetration</td>
<td>Breakout Session</td>
</tr>
<tr>
<td>BRKCOC-2006</td>
<td>Inside Cisco IT: ACI &amp; Tetration Analytics</td>
<td>Breakout Session</td>
</tr>
<tr>
<td>LABACI-1366</td>
<td>Tetration Analytics Open API 101</td>
<td>Walk-in Self-Paced Lab</td>
</tr>
<tr>
<td>LABACI-2020</td>
<td>Whitelist policy and security enforcement through Tetration Analytics</td>
<td>Walk-in Self-Paced Lab</td>
</tr>
<tr>
<td>LABDCN-1206</td>
<td>An Introduction to Tetration and Policy Deployment</td>
<td>Walk-in Self-Paced Lab</td>
</tr>
</tbody>
</table>
Tetration Introduction
Cisco Tetration
Architecture Overview

Access mechanism
- Web GUI
- REST API
- Event notification
- Cisco Tetration apps

Analytics engine
- Cisco Tetration™
  - Third-party sources (configuration data)
  - Bring your own data (streaming telemetry)

Data collection layer
- Software sensor and enforcement
- Embedded network sensors (telemetry only)
- ERSPAN sensors (telemetry only)
Use Cases

- Operations
  - Network and TCP performance
  - Application insight
  - Process inventory
  - Neighborhood graphs

- Security
  - Compliance
  - Application segmentation
  - Policy simulation
  - Policy

- Visibility and forensics

Cisco Tetration™ platform
Cisco Tetration Analytics: Deployment Options

On-premises options

Cisco Tetration™ platform (large form factor)
• Suitable for deployments of more than 5000 workloads
• Built-in redundancy
• Scales to up to 25,000 workloads

Includes:
• 36 Cisco UCS® C220 servers
• 3 Cisco Nexus® 9300 platform switches

Cisco Tetration-M (small form factor)
• Suitable for deployments of less than 5000 workloads

Includes:
• 6 Cisco UCS C220 servers
• 2 Cisco Nexus 9300 platform switches

Public cloud

Cisco Tetration Cloud
• Software deployed in public cloud
• Suitable for deployments of less than 1000 workloads
• Public cloud instance owned by customer

Amazon Web Services
Microsoft Azure
Sensor Installation & Monitoring
Cisco Tetration Analytics Data Sources

Main features
- Low CPU overhead (SLA enforced)
- Low network overhead

New Enforcement point (software agents)
- Highly secure (code signed and authenticated)
- Every flow (no sampling) and no payload

Software sensors
- Available today
  - Linux servers (virtual machine and bare metal)
  - Windows servers (virtual machines and bare metal)
  - Windows Desktop VM (virtual desktop infrastructure only)
  - Universal* (basic sensor for other OS)

Network sensors
- Next-generation Cisco Nexus® Series Switches
  - Cisco Nexus 9300 EX
  - Cisco Nexus 9300 FX

Third-party sources
- Third-party data sources
  - Asset tagging
  - Load balancers
  - IP address management
  - CMDB
  - ...

*Note: No per-packet telemetry; not an enforcement point
Sensor Type

- Starting with version 2.1.x, Tetration supports 6 different agent types.

<table>
<thead>
<tr>
<th>Sensor Agent type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Visibility Agent</td>
<td>Provides highest fidelity in terms of time series flow data, processes running on a host. Most Linux and Windows platforms are supported.</td>
</tr>
<tr>
<td>Enforcement Agent</td>
<td>Provides all capabilities available in Deep Visibility Agents. In addition, Enforcement agents have capability to set firewall rules on the installed host.</td>
</tr>
<tr>
<td>Universal Visibility Agent</td>
<td>Provides flexibility to be installed on almost any compute platform. Hosts that have a Universal Visibility Agent installed allows conversation analysis via ADM.</td>
</tr>
<tr>
<td>Hardware Switch Agent</td>
<td>Provides the highest throughput flow analysis without requiring any per-host agent installation. Requires to be installed on Cisco N9K switch operating system.</td>
</tr>
<tr>
<td>Netflow Agent</td>
<td>Provides the flow data from NetFlow v9 and IPFIX flows. NetFlow agents consume netflow records sourced by any NetFlow compatible switch and forwards the records to the cluster</td>
</tr>
<tr>
<td>SPAN Agent</td>
<td>Provides the flow analysis without requiring any per-host agent installation. It runs in the Tetration SPAN VM appliance. It consumes ERSPAN packets sourced by any Cisco switch.</td>
</tr>
</tbody>
</table>
Monitoring – Agents

- You can monitor agents health, agent distribution, CPU/Bandwidth utilization and etc.
Inventory | Annotation | Scope | RBAC
Inventory and Annotation - User-Uploaded Asset Tags

- Discovered inventory through sensors
- Inventory tracked in real time, along with historical trends
- Uploaded inventory and metadata (32 arbitrary tags)
Tetration Native Management – RBAC

• Roles are used to implement a role-based access control (RBAC) model so features and data can be restricted to sets of users.
  • Scopes: Used to group together assets and/or endpoints
  • Roles: Define access to scopes; set of capabilities
  • Users: Assigned to roles

Actions: Read, Modify, ADM, Enforce, etc.
Flow Search | Application Workspaces
Flow Search

- Map applications to network flow
- Pinpoint most active hosts
- Trace complex network paths

- Map applications to network flow
- Debug application vs network performance
- Visualize long-lived flows
Application Dependency and Cluster Grouping

Cisco Tetration Analytics™ platform

Unsupervised machine learning
Behavior analysis

Cisco Nexus® 9000 Series

Bare metal, VM, and switch telemetry

Bare-metal and VM telemetry

VM telemetry (AMI …)

Network-only sensors, host-only sensors, or both (preferred)

Bare metal and VM

On-premises and cloud workloads (AWS)

Brownfield

BM VM VM VM BM

BM VM VM BM

BM VM BM

BM VM BM

VM BM VM BM

VM BM BM

VM BM BM

BM VM VM BM

BM VM VM BM
Application Dependency Mapping

InfoSec Horizontal Policy

Policy Graph

InfoSec Horizontal Policy

Priority | Action | Consumer | Provider | Services
---|---|---|---|---
100 | DENY | Production | NonProduction | Any / 3:65536 / 65536
100 | DENY | NonProduction | Production | Any / 3:65536 / 65536

Priority | Action | Consumer | Provider | Services
---|---|---|---|---
100 | ALLOW | HAProxy | DefaultLab | TCP : 443...
100 | ALLOW | HAProxy | Wordpress | TCP : 80...
100 | ALLOW | Redis | DefaultLab | UDP : 123...
100 | ALLOW | DefaultLab | OpenCart | TCP : 22...
100 | ALLOW | DefaultLab | Wordpress | TCP : 80...
100 | ALLOW | Wordpress | DefaultLab | UDP : 53...
100 | ALLOW | DefaultLab | OpenCart | TCP : 80...
100 | ALLOW | Default | OpenCart | TCP : 6379

App View
Service Status

- The **Service Status** page displays all services that are used in Cisco Tetration Analytics cluster with their dependencies and health status.

- Gears Menu -> Maintenance -> Service Status
  - Table view
  - Graph view
<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>Count</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hadoop</td>
<td>Down</td>
<td>1 / 1</td>
<td>Please check dependencies!</td>
</tr>
<tr>
<td>HDFS</td>
<td>Down</td>
<td>1 / 2</td>
<td>Dependencies Failed, Dependencies Failed, No field name=Hadoop:service=fluNameNode,name=NameNodeInfo is present in response from url:<a href="http://namenode.namenode.service.consul:50070/jmx?qry=Hadoop">http://namenode.namenode.service.consul:50070/jmx?qry=Hadoop</a>:* Please check dependencies!</td>
</tr>
<tr>
<td>DataNode</td>
<td>Healthy</td>
<td>24 / 24</td>
<td></td>
</tr>
<tr>
<td>NameNode</td>
<td>Down</td>
<td>0 / 1</td>
<td>Dependencies Failed, No field name=Hadoop:service=fluNameNode,name=NameNodeInfo is present in response from url:<a href="http://namenode.namenode.service.consul:50070/jmx?qry=Hadoop">http://namenode.namenode.service.consul:50070/jmx?qry=Hadoop</a>:*</td>
</tr>
</tbody>
</table>

**Service Status - Critical Example**

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cluster Status

- The **Cluster Status** page shows the status of all the physical servers in Cisco Tetration Analytics rack.

- Gears Menu-> Maintenance -> Cluster Status

## Cluster Status

### Active
The node is powered on.

### Inactive
The node is not powered on / connected.

Switch ports refer to the uplink vPC ports connected to the two leaf switches.

<table>
<thead>
<tr>
<th>State</th>
<th>Status</th>
<th>Switch Port</th>
<th>Serial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commissioned</td>
<td>Active</td>
<td>Ethernet 1/1</td>
<td>FCH2002V1RZ</td>
</tr>
</tbody>
</table>

**Serial:** FCH2002V1RZ

- **Private IP:** 1.1.0.36
- **CIMC IP:** 10.201.147.11
- **Status:** Active
- **State:** Commissioned
- **SW Version:** 2.0.2.20
- **Hardware:** 20 cores, 541G memory, 8 disks, 13.60T space, HDD
- **Firmware:** View Firmware Upgrade Logs

**General info (Serial#, CIMC IP, SW and etc)**

- **Instances**
  - appServer-2
  - datanode-16
  - orchestrator-1

**VM Instances running on this node**
## VM Information

**Model:** 39RU-GEN1

### Virtual Machine Information

Displaying 100 virtual machines

<table>
<thead>
<tr>
<th>Serial</th>
<th>Private IP</th>
<th>Instance Name</th>
<th>Public IP</th>
<th>Deploy Status</th>
<th>Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCH2002V1A9</td>
<td>1.1.0.117</td>
<td>adhoc-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V17L</td>
<td>1.1.0.118</td>
<td>adhoc-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V01W</td>
<td>1.1.0.131</td>
<td>appServer-1</td>
<td>10.201.147.86</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V1KZ</td>
<td>1.1.0.132</td>
<td>appServer-2</td>
<td>10.201.147.87</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V01W</td>
<td>1.1.0.91</td>
<td>collectorDatamover-1</td>
<td>10.201.147.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2003V1D9</td>
<td>1.1.0.96</td>
<td>collectorDatamover-6</td>
<td>10.201.147.75</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V0NP</td>
<td>1.1.0.97</td>
<td>collectorDatamover-7</td>
<td>10.201.147.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V0NR</td>
<td>1.1.0.94</td>
<td>collectorDatamover-4</td>
<td>10.201.147.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCH2002V0rX</td>
<td>1.1.0.95</td>
<td>collectorDatamover-5</td>
<td>10.201.147.74</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
External Management Access

- CIMC and Leaf switch passwords are randomized at the installation of software
- External Management Access allows end-users access to limited/read-only activity on CIMC and Leaf switches
- Changing the read-only password is controlled in Cluster Status.
  - The read-only username is ta_guest for all servers and both leaf switches.
  - Default password is C1sco@123
Hawkeye / Chart / Grafana

- Dashboard to provide graphical view of the status and data of the cluster
- Time interval can be adjust and default is “Last 6 hours”
Consul / Cluster

- Consul is a tool for discovering and configuring services in your infrastructure
Bosun

- Simple alert management that includes acknowledging rules, history for a rule/alert, incident management

<table>
<thead>
<tr>
<th>Needs Acknowledgement</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄 error - batchmover.inputLatencyIsHigh</td>
<td>1 alerts</td>
</tr>
<tr>
<td>🔄 error - collector.checkMissingMetric</td>
<td>1 alerts</td>
</tr>
</tbody>
</table>
Maintenance
Explore | Snapshots
Explore

• Check service status and logs, start/stop/restart services
• Actions GET, POST, PUT, DELETE
Snapshots

• A Tetration snapshot is the equivalent of a 'tech support'
  • Up to 100MB of logs compressed in tar.gz format

• A snapshot is recommended to be collected:
  • Any time a TAC case is opened
  • Before / After an upgrade
  • Before / After a node is RMA'd

• User can specify what to collect
  • Logs, YARN, alerts, TSDB

Snapshots

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Progress</th>
<th>Comments</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-07-19_162319</td>
<td>Ready</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017-07-16_153230</td>
<td>Ready</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lab Setup Overview
Lab Setup Overview

• A single 8-RU Tetration cluster in a DMZ environment
• Cluster UI is reachable only from the remote desktop over RDP session
• Each user has one VM allocated for sensor installation practice
• Lab guide can be launched from local laptop in the room or remote desktop
• Verify and follow the lab guide for your pod as it has information specific to you
• Lab guide navigation
• Screenshots are samples, follow information in the text
Lab Sessions

• Part 1: Understanding the lab environment
  • Cluster platform info (platform, setup info and etc)
  • User, roles, scope

• Part 2: Deployment
  • Sensor installation
  • Sensor monitoring
  • Flow Search
  • Application Dependency Mapping

• Part 3: Monitoring and Management
  • Monitoring features
  • Maintenance features
Keyboard in RDP

<table>
<thead>
<tr>
<th>~</th>
<th>!</th>
<th>@</th>
<th>#</th>
<th>$</th>
<th>%</th>
<th>^</th>
<th>&amp;</th>
<th>*</th>
<th>(</th>
<th>)</th>
<th>-</th>
<th>+</th>
<th>Backspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>=</td>
<td>=</td>
<td>=</td>
<td></td>
</tr>
</tbody>
</table>

Tab ➪ Q W E R T Y U I O P { [ ] } |

Caps Lock ➪ A S D F G H J K L ; : " Enter|

Shift ➪ Z X C V B N M , . / Shift|

Ctrl | Win Key | Alt | Alt | Win Key | Menu | Ctrl |
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#LTRACI-2184
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you