SCOPED CERTIFIED APPLICATION DESIGN

Cisco Tetration Application (1.0.0)

Template effective date: August 2017
Table of Contents

1 Overview .................................................................................................................................................. 3
1.1 References............................................................................................................................................ 3
2 Application overview and intended use .................................................................................................. 3
2.1 Third-party dependencies .................................................................................................................. 4
3 Software architecture overview ........................................................................................................... 4
4 Software design description .................................................................................................................. 4
5 Performance considerations and concerns ........................................................................................... 7
6 Security considerations and concerns ................................................................................................... 7
7 Application components ....................................................................................................................... 7
7.1 Components created by the application: ......................................................................................... 7
7.2 Integration components created by the application: ....................................................................... 8
8 Future plans ........................................................................................................................................... 9
9 Service Level Agreement Definition .................................................................................................... 9
10 Debugging and troubleshooting ........................................................................................................... 9
10.1 Debugging tips:................................................................................................................................... 9
10.2 Failure modes:.................................................................................................................................... 10
1 Overview

Cisco Tetration Analytics uses rich traffic flow telemetry to address critical data centre operational use cases. It uses both hardware and software agents as telemetry sources and performs advanced analytics on the data collected. Cisco Tetration Analytics system uses Role based access control and visibility of data depend on the role assigned to the user. Roles contain sets of Capabilities and are assigned to users on the Users page. A user can have any number of roles. Roles can have any number of capabilities.

This rich information in the cluster is discovered through RESTful interfaces supported by Cisco Tetration Analytics to populate ServiceNow CMDB.

1.1 References

<table>
<thead>
<tr>
<th>#</th>
<th>Document Identifier</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Table 1

2 Application overview and intended use

The application is intended to do the following:

- Import Tetration Analytics discovered devices into ServiceNow CMDB (utilizing Cisco Tetration Analytics cluster as a source of truth)
- Annotate required devices with the class, instance and discovery source information on Tetration Analytics from ServiceNow

The Inventory discovered by this application are:

Tetration Analytics -

These are the minimal information that are extracted:

- List of all VRFs from Tetration
- List of all end points with Sensor agents installed
- List of all End Points discovered by Tetration Analytics with following information -
  - IP Address
  - MAC Address
  - Address Type
  - IFace Name
  - Host Name
  - Operating System and its version
  - Scope to which the End point belongs

This application helps customers maintain a single repository of the endpoints and post annotations based on requirement.
2.1 Third-party dependencies
This application uses HTTPS REST APIs to retrieve information from Cisco Tetration Analytics Cluster as defined in [1]. This application is compatible with Cisco Tetration Analytics release 2.0 or higher releases.

3 Software architecture overview
The application contains the following components:

- Staging tables that extends Import Set Row
- CI table that extends the base CI (cmdb_ci) for endpoint elements.
- Transform map to move data from staging tables to CI tables
- Script Includes – define REST messages and retrieve the response. The Responses are parsed and staging tables populated using the SNOW REST API.
- Scheduled Jobs - to execute discovery on demand.

<table>
<thead>
<tr>
<th>Cisco Tetration Application CI Tables</th>
<th>Extends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Tetration VRFs</td>
<td>Configuration Items (cmdb_ci)</td>
</tr>
<tr>
<td>Cisco Tetration Sensors</td>
<td>Configuration Items (cmdb_ci)</td>
</tr>
<tr>
<td>Cisco Tetration End Points</td>
<td>Configuration Items (cmdb_ci)</td>
</tr>
<tr>
<td>Cisco Tetration ServiceNow Discovered Endpoints</td>
<td>Configuration Items (cmdb_ci)</td>
</tr>
<tr>
<td>Cisco Tetration IP Sets</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 2

4 Software design description
At the heart of Cisco Tetration Analytics platform is a big data platform, designed to deal with large volumes of streaming rich telemetry, map thousands of applications spanning across tens of thousands of workloads, enforcement millions of policy rules for applications. Using Unsupervised Machine Learning, algorithmic approaches and automated enforcement, customers get a turnkey solution with this platform.

Data is collected and fed into Tetration a few different ways -

1) Is by using a Software agent on a host.
2) Is by using hardware sensors located in our 9K switching platform ASIC. It is recommended that you use both sensors together to get the best coverage, but you can implement Tetration with only the Software or Hardware sensor.
3) In addition to the collection sensors, we can add 3rd party data. Like SLB configs, ACE, F5 information, HA-Proxy, Route-Tags, etc. to Tetration to increase its full understanding of your environment.

Tetration Platform is designed to be open. Its Open Access method provide REST API for users to query the information from a northbound system, Publish notifications to northbound systems using Kafka message bus, for example trigger a notification when an application communication deviates from the policy. Custom Apps enables developers to write their own application on the
platform using python or Scala. It provides access to the deep store within the platform and developers [Figure 1].

Cisco Tetration Analytics architecture:

Data Collection
- Software Sensor and Enforcement
- Embedded Network Sensors (Telemetry Only)
- Third Party Sources (Configuration Data)

Analytics Engine
- Cisco Tetration Analytics Cluster

Open Access
- Web GUI
- REST API
- Event Notification
- Tetration Apps

Figure 1

Cisco Tetration Analytics Annotations:
Users define tags/annotations for inventories:
- Easy to find inventories or search flows
- Easy for enforcement
- Easy to apply policies on sensors

Figure 2

Cisco Tetration Application:
Cisco Tetration Application initiates a discovery of Cisco Tetration Analytics Cluster using scheduled jobs and scripts detailed in later sections. The application uses Cisco Tetration REST APIs to import the information and map to different CMDB tables detailed in later sections [Figure 3].

Currently the application initiates the import of data on-demand by user.
Cisco Tetration Application uses MID server interfaces to communicate with Cisco Tetration Analytics Cluster. The user using scheduled jobs initiates discovery. This schedule job imports information from Tetration Analytics Cluster and maps them to ServiceNow CMDB tables [Figure 4].
5 Performance considerations and concerns

- Data import time depends on the volume of data in each customer environment.
- The inbound web services are used to extract data from Tetration Cluster. Average number of records extracted per transaction is 150.

6 Security considerations and concerns

- Tetration API Keys
  1. User updates the table “Cisco Tetration IP Sets” with the API Key and Secret Key generated from Tetration’s web interface with other information. These keys will be used to make REST requests to the cluster.
    - NOTE – Please ensure the keys are generated with proper roles. Please refer User Guides on Tetration Web Interface for more information.

7 Application components

Below are the newly created artifacts and modifications to base ServiceNow artifacts:

7.1 Components created by the application:

- List of script includes:
  - CiscoTetrationVRFs
  - CiscoTetrationSensors
  - CiscoTetrationInventory
  - CiscoTetrationAnnotations
  - CiscoAnnotationEndPoints

- List of All UI Actions:
  - Cisco Tetration Discovery
  - Cisco Tetration Annotations

- List all newly defined tables:
  - Cisco Tetration VRFs
  - Cisco Tetration Sensors
  - Cisco Tetration End Points
  - Cisco Tetration ServiceNow Discovered Endpoints
  - User Input forms tables
  - Cisco Tetration IP sets

- List all gauges
  - Cisco Tetration Application
• List all pages
  ▪ Cisco Tetration Dashboard
  ▪ Cisco Tetration Support Contacts

• The scope(s) used: x_caci_cisco_tetr

• The application menu(s) used: Cisco Tetration Application

7.2 Integration components created by the application:

• List all import set tables:
  ▪ Cisco Tetration VRF Stages
  ▪ Cisco Tetration Sensor Stages
  ▪ Cisco Tetration End Points Stages
  ▪ Cisco Tetration Annotations Stages

• List all transformation maps:
  ▪ Cisco Tetration VRF TM
  ▪ Cisco Tetration Sensors TM
  ▪ Cisco Tetration End Points TM
  ▪ Cisco Tetration Annotations TM

• List of All REST Messages:
  ▪ CiscoTetrationVRFs
  ▪ CiscoTetrationSensors
  ▪ CiscoTetrationInventory
  ▪ CiscoTetrationAnnotations

• List of All Scripted REST APIs:
  ▪ CiscoTetrationAPI
    ▪ Inventories
    ▪ Sensors
    ▪ VRFs

• List any scheduled jobs for data exports:
  ▪ Cisco Tetration Discovery
  ▪ Cisco Tetration Application Cleanup
  ▪ Cisco Tetration Annotations
8 Future plans
Cisco Tetration Application currently supports discovery of the End Points, Sensors and VRFs in the infrastructure to visualize the inventory components and post annotations into the cluster. In the latter phase, this application will develop features to support:

- Incident Management
- ADM Mapping using ServiceNow ‘s ServiceWatch

9 Service Level Agreement Definition
In this section, you define the Service Level Agreement (SLA) for your customers.

Customers will be instructed to contact the integration provider (your organization) for technical support. If a customer first contacts ServiceNow Customer Support, then ServiceNow Customer Support will isolate the problem and instruct the customer to resolve the issue with your organization.

- Support Hours of Operation: 8am – 5pm EST
- Support Days of Operation: Monday – Friday Excluding holidays
- Promised Call Response Time: 4 Hours
- Promised Call Resolution Time: 5 Business Days
- Contact Method: Email
- Contact Details: insbu-servicenow@cisco.com

10 Debugging and troubleshooting

10.1 Debugging:

- ServiceNow Logs:
  The scripts uses gs.error () and gs.info () methods to print errors and information messages respectively.
  The “application logs” under “system logs” will contain all the logs for the application. Critical error messages are listed as Error and debug statements are listed as Information.

- Mid Server Logs
  The error logs are populated in the file Agent0.log on the MidServer.
  Path = “/servicenow/<mid server name>/agent_folder/logs/agent0.log”

  These logs are also available from the instance. Go to, ‘Mid Server -> Server -> [Specific Record] Mid Server’. Click on ‘Grab Mid Logs’ under the Related Links [Figure 5].
Figure 5

- **API Server Logs**
  
  API Server logs are available in the same directory the API Server is installed on and has complete information about API calls being made to the Tetration Cluster and their responses.

  Path = “/<API Server Path>/Tetration_API/TET_API_Server.log”

### 10.2 Failure modes:

For proper functioning of the application, ensure:

- MID server must be accessible from ServiceNow instance
- The Mid Server needs to be able to communicate with the ServiceNow instance directly
- Ensure the proxies are set properly
- Tetration_API Server from Cisco Tetration Application should be installed on Mid Server
- Cisco Tetration Analytics must be accessible from MID server
- Cisco Tetration Analytics APIs must be allowed from MID server

Application will timeout waiting for responses if any of the above are not configured correctly.

END OF DOCUMENT