Oracle® Unified Operations

Trouble to Resolve Reference Solution Guide

Release 8.0
G49379-01
December 2025

Oracle Unified Operations Trouble to Resolve Reference Solution Guide, Release 8.0

G49379-01

Contents

About this Content

This document explains concepts and information regarding the Unified Operations Trouble to Resolve Reference Solution. It also describes the reference solution deliverables and the functional use cases.

Audience

This document is intended for readers who require an understanding of the Unified Operations Trouble to Resolve Reference Solution.

- Reference Solution Architects
- Business Analyst
- Network Operations personnel
- System Integrators

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

About Trouble to Resolve Reference Solution

This chapter provides an overview of the Trouble to Resolve Reference Solution.

For information about implementing the reference solution, see the *Trouble to Resolve Reference Solution Getting Started Guide*.

Reference Solution Architecture

The Trouble to Resolve Reference Solution comprises the Unified Inventory Management (UIM) and Unified Assurance applications. The following diagram illustrates the reference solution architecture. Both Unified Assurance and UIM are deployed within a Kubernetes cluster.

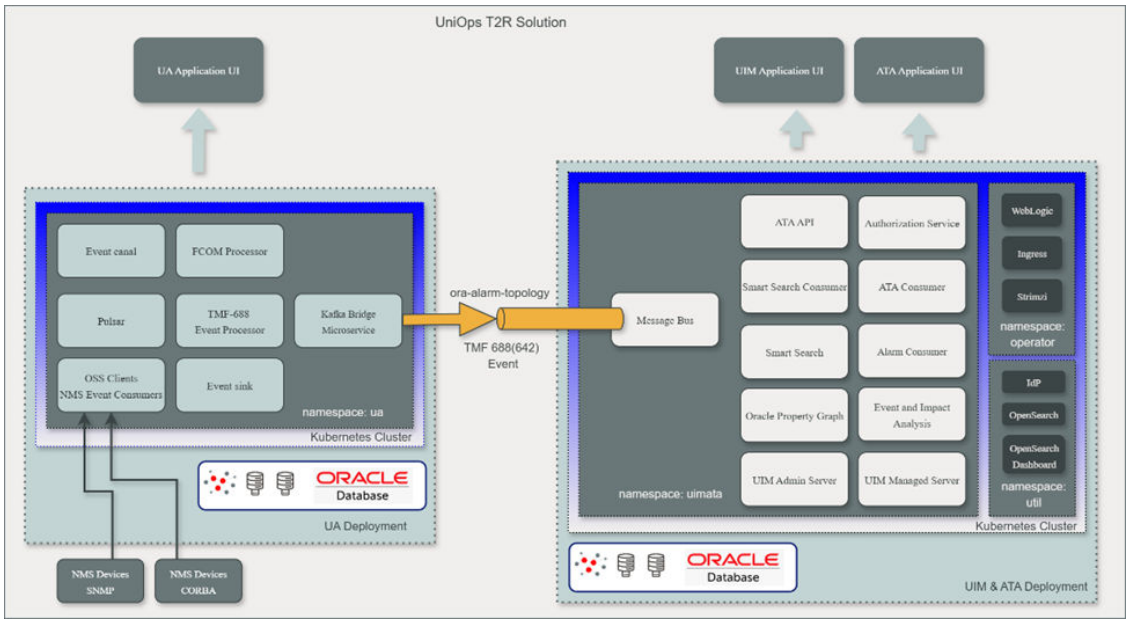
Within this setup, UIM's Messaging Bus uses a specific Kafka topic where Unified Assurance publishes TMF42 notification events wrapped inside TMF688 notification events. Each TMF688 alarm notification event carries alarm resource details for a particular network element.

UIM components process and store the alarm information for subsequent reference solution activities. Users (for example, network administrators) can then visualize alarms within the service topology, perform impact analysis to identify affected entities, and qualify or disqualify the alarms accordingly.

Reference Solution Deployment Diagram

The following diagram illustrates the deployment of the reference solution:

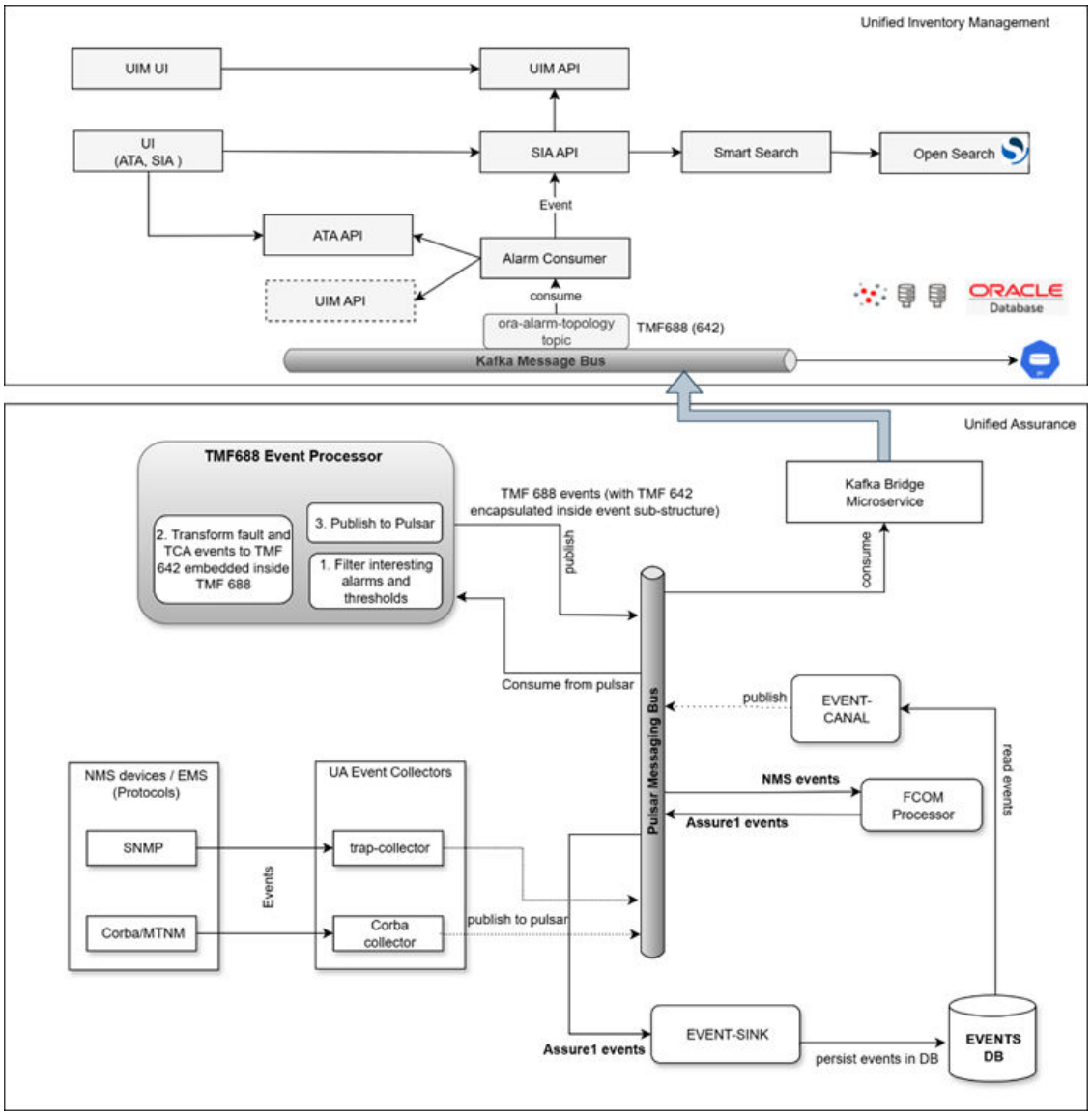
Figure 1-1 Reference Solution Deployment



Reference Solution Functional Architecture

The following diagram illustrates the functional architecture of the Trouble to Resolve Reference Solution:

Figure 1-2 Trouble to Resolve Reference Solution Functional Architecture



For more information on the UIM and United Assurance application architectures, see *UIM Unified Inventory and Topology Deployment Guide* and “What is Unified Assurance?” in *Unified Assurance Concepts*.

2

About the Trouble to Resolve Reference Solution Archive Package

This chapter describes the contents of the Trouble to Resolve Reference Solution archive, which includes the reference solution package's details, the fault management use cases. It also outlines the event types, notifications, and device protocols for which the reference solution is tested.

The reference solution download archive includes the following components:

- Reference solution documentation
- Smoke Test artifacts
  - Design time cartridges
  - Runtime seed data
- Reference solution (DWDM, OTN, SNMP) artifacts
  - Design time cartridges
  - Runtime seed data
  - Extensions

The reference solution archive package contains the required deliverables to be used after reference solution applications deployment. The details of this package are provided in the following table. After the reference solution deployment is complete, the package items must be loaded according to the corresponding guidelines. After loading these packages, the reference solution will be ready to process alarm events.

Table 2-1 Reference Solution Package details

Package	Format	Location	Sub Directories	Reference Solution Component	Details
uniops-t2r-artifacts_.<tag>.<build_ number>.tar.gz	Compressed	uniops-t2r-artifacts\uim\cartridges	common smoketest solution	UIM	Accelerates the process of defining a new Service domain by creating a domain package containing a single CFS-RFS-Resource structure that you can re-factor, expand, and link to, as needed.
uniops-t2r-artifacts_.<tag>.<build_ number>.tar.gz	Compressed	uniops-t2r-artifacts\uim\seeddata	smoketest solution	UIM	Streamlines the expansion of a Technology domain definition by creating a default RFS-Resource structure.

Table 2-1 (Cont.) Reference Solution Package details

Package	Format	Location	Sub Directories	Reference Solution Component	Details
uniops-t2r-artifacts_.<tag>.<build_number>.tar.gz	Compressed	uniops-t2r-artifacts\ua\packages	common smoketest solution	Unified Assurance	Accelerates the process of expanding a Technology domain definition by creating a default Resource structure.

About Fault Management Use Cases

The Trouble to Resolve Reference Solution is tested for the following event types, notifications, and device protocols:

Table 2-2 Fault Management Use Cases

Category	Supported
Alarm type	• Fault Alarm • Threshold Crossing Alarm **Note**: TCA is applicable only for CORBA Events.
Event Notification	• AlarmCreateEvent • AlarmAttributeValueChangeEvent • ClearAlarmCreateEvent • AlarmDeleteEvent
Protocol	• SNMP • CORBA (MTNM/TMF 814 compliant)

About Supported Domains and Traps

The Trouble to Resolve Reference Solution is tested for the following domains and traps:

Table 2-3 Domains and Traps

Category	Supported
Business Domains	Fault Management
Technology Domains	SDH, Ethernet, DWDM, OTN
Devices	CORBA Devices for SDH Technology
CORBA Events	Below event types are supported based on MTNM / TMF 814 standard: • NT_ALARM • NT_TCA

Table 2-3 (Cont.) Domains and Traps

Category	Supported
SNMP Traps	Example traps: • Device down • • Link down • LOS • Interface disabled

3

Configuring Trouble to Resolve Reference Solution

This chapter describes the steps needed to configure the Trouble to Resolve Reference Solution using the reference solution package. It is assumed that the following points are taken into consideration before performing the subsequent steps:

- UIM and Unified Assurance applications have already been set up successfully by referring to the *Trouble to Resolve Reference Solution Installation Guide*.
- UIM and Unified Assurance have been deployed with SSL enabled as described in their respective installation guides to ensure security for all external APIs and URLs.
- UIM Message has been enabled with SSL based configuration, external system will need to use SSL certificate to send message to Message Bus.

Configuring UIM

This section describes the process of configuring UIM.

Installing Design-Time Environment

A design-time environment is required for the reference solution developer to deploy and configure UIM-related design-time components (cartridges).

Installing Design Studio

Service Catalog and Design - Design Studio is an IDE used for cartridge design and deployment. It supports both reference solution-specific cartridges and UIM-base cartridges.

This section provides sample guidelines for setting up Design Studio. For complete instructions, refer to *the Design Studio Installation Guide.*

To set up Design Studio:

1. Get the following files:
   - OEPE bundle
   - Design Studio installer zip
2. Extract the above files to a folder of your choice.
3. Open the OEPE or Eclipse application.
4. Follow the steps in *Design Studio Installation Guide* to install the Design Studio plug-ins and any required Eclipse plug-ins.

Setting Up Workspace

To set up a workspace:

1. Launch Eclipse using a fresh workspace.

2. Turn off the **Project** under the **Build Automatically** option.
3. Import the Inventory cartridges listed below:
   a. Required UIM and Base cartridges:
      - ora_uim_basetags
      - ora_uim_baseextpts
      - ora_uim_basemeasurements
      - ora_uim_baserulesets
      - ora_uim_basetechnologies
      - ora_uim_basespecifications
      - ora_uim_mds
      - ora_uim_model
      - ora_uim_basewdm
      - ora_uim_common
      - ora_uim_workorder
   b. UIM Tech-pack cartridges:
      - ora_uim_party_customer
      - OracleComms_UIM_CarrierEthernet
      - OracleComms_UIM_Packet
   c. Reference solution cartridges:
      - ora_uim_bulkloader
      - OracleComms_UIM_Sample_DWDM_OTN_Device
      - OracleComms_UIM_Sample_SDH_Device
      - OracleComms_UIM_Sample_Ethernet_Device
      - OracleComms_UIM_Sample_DWDM_OTN_SDH_Ethernet_Service
      - OracleComms_UIM_Sample_DWDM_OTN_SDH_Ethernet_Ports_Interfaces
4. Double-click on each cartridge name (one-by-one) to open its description into the editor and make the following changes:
   a. Unseal the cartridge if it is not already unsealed.
   b. Change the minor version from **7** to **8**, where the major version is **7**. This means that cartridge version will be changed from **7.7** to **7.8**.

      > **Note**
      >
      > If major version of any cartridge is **1**, then leave the minor version as **0**.

   c. Change the target versions of all those cartridges to **7.8.0**.
5. Add JRE 8 in Eclipse:
   a. Click on Windows menu and choose **Preferences**.
   b. In the **Preferences** window, expand Java in the left side panel and then click **Installed JREs**.

c. Click **Add**.

> **Note**
>
> JDK-21 must be shown in already installed JREs and as **Default JRE**.

d. Select **JRE Type** as **Standard VM** and click **Next**.

e. Select **JRE Home**.

f. Click **Finish**.

6. Configure Java Compiler compliance level for your Eclipse workspace:
   a. Click on the Windows menu and choose **Preferences**.
   b. In the **Preferences** window, expand Java in the left side panel and select **Compiler**.
   c. On the Compiler page, check **Configure workspace settings**.
   d. Set the Compiler compliance level to **1.8** from the dropdown menu.
   e. Click **Apply and Close** to save the changes.
7. Add **UIM_LIB** and **OTHER_LIB** in Java Build Path of any of the failed cartridge project:
   a. Download **UIM_LIB** and **OTHER_LIB** from reference solution package.
   b. Right-click on any (failed) cartridge name in the **Studio Projects** pane.
   c. Open **Properties**, select **Java Build Path**, and the **Libraries**. Click **Add Variable**, then **Configure Variables**, and finally click **New**.
   d. Add the variables with **UIM_LIB** and **OTHER_LIB**.
   e. Click **Apply and Close**.
   f. You will be prompted to re-compile. You must compile and build the whole workspace.
8. Fixing Groovy error: if you see following error, **OracleComms_UIM_FibreBroadband - Groovy: compiler mismatch: project level is 2.5, workspace level is 5.0**, then do the following:
   a. Right-click on (failed) cartridge **OracleComms_UIM_FibreBroadband** in the **Studio Projects** pane.
   b. Open **Properties** and then the **Groovy** compiler.
   c. Change the dropdown value of Groovy compiler level for this project: **5.0**.
   d. Click **Apply and Close**.
9. Compile and build the workspace. There should be no errors now.
10. Deploy UIM base cartridges, tech-pack cartridges, and custom cartridges. Then deploy the reference solution cartridges in the given order in UIM.

Loading Domain-Specific Seed Data

The reference solution package includes domain-specific (protocol) seed data for runtime, corresponding to the design-time specifications. This seed data must be installed in the UIM runtime application.

Configuring the UIM Application for Seed Data Import

The bulk import of the Trouble to Resolve Reference Solution seed data is tested with the following chunk size for live context import. Update the corresponding properties in the **custom-config.properties** file as follows:

```
custom-confg.properties file:
ExecuteBulkLoadInLive=true
InsertCardTaskChunkSizeInThread=100
PortMappingTaskChunkSizeInThread=100
ConnectivityPipeEnablementChunkSizeInThread=100
NetworkTaskChunkSizeInThread=200
PortMappingTaskChunkSizeInThread=200
```

Use the following configuration in the **managedServers** section of the **shape.yaml** file where the **ParallelGCThreads**, under the **dev.yaml** file, must be updated to **8** for managed servers to upload seed data without any performance issues.

```
dev.yaml file
managedServers:

# USER_MEM_ARGS variable to be set on all managed servers
  shape:
    user_mem_args: "-XX:+UseContainerSupport -Xms5g -Xmx5g -Xmn2g -
XX:+HeapDumpOnOutOfMemoryError  -XX:HeapDumpPath=/logMount/$(DOMAIN_UID)/
servers/$(SERVER_NAME)"

    gc_mem_args:
      options: "-XX:+UseG1GC -XX:ParallelGCThreads=8"
```

After the above configuration is updated, perform an upgrade or restart of the UIM application.

Loading the Seed Data

Seed data is provided for DWDM, OTN, SDH, and Ethernet, corresponding to the specifications deployed during the design-time setup. Create this sample seed data in UIM using the UIM Bulk Loader utility tool.

Seed data with locations, devices, and networks are created after uploading excel sheets using the bulk loader utility. You must manually create protection path for service connectivities and assign those service connectivities to the services from UIM by following steps 4 and 5 mentioned below.

To create the seed data and load the Unified Operations Trouble to Resolve Reference Solution datasets into UIM and ATA:

1. Extract the data sheets from the reference solution package. You will find multiple folders and each folder may have multiple excel sheets. You must upload each excel sheet from all the folders in the following order to create Trouble to Resolve sample data in UIM:
    a. DWDM Texas
    b. Ethernet Texas
    c. OTN Dallas

d. OTN Fort Worth
e. OTN Houston
f. OTN San Antonio
g. SDH Dallas
h. SDH Fort Worth
i. SDH Houston
j. SDH San Antonio
k. SDH Subnet Dallas
l. SDH Subnet1 Houston
m. SDH Subnet2 Houston
n. Texas Common

2. You must update the **NativeEMSName** value in each seed data excel sheet against only those devices where you want to simulate an SNMP alarm according to the following guidelines:

Table 3-1 Guidelines for Simulating an SNMP Alarm

Entity Sheet	Column Name	For Alarm Simulator Type	Value Format
Physical Devices	NativeEMSName	SNMP Alarm using MIMIC simulator	IP Address of the Mimic Device. **Example**: [ipaddress]
Physical Devices	NativeEMSName	SNMP Alarm using netsnmp script	Fully Qualified DNSName of VM from which netsnmp commands are sent. **Example**: abc.xyz.com
Equipments	NativeEMSName	SNMP Alarm using MIMIC simulator	IP Address of the Mimic Device followed by ::index. **Example**: [ipaddress]::1 **Note:** index should always be unique for identifying sub nodes like card, port, device interface.
Equipments	NativeEMSName	SNMP Alarm using netsnmp script	Fully Qualified DNSName of VM followed by ::index from which netsnmp commands are sent. **Example**: abc.xyz.com::2
		SNMP Alarm using MIMIC simulator	IP Address of the Mimic Device followed by ::index. **Example**: [ipaddress]::2
InsertCards	CardNativeEMSName	SNMP Alarm using netsnmp script	Fully Qualified DNSName of VM followed by ::index from which netsnmp commands are sent. **Example**: abc.xyz.com::2

Table 3-1 (Cont.) Guidelines for Simulating an SNMP Alarm

Entity Sheet	Column Name	For Alarm Simulator Type	Value Format
PortMappings	PortNativeEMSName	SNMP Alarm using MIMIC simulator	IP Address of the Mimic Device followed by ::index. **Example**: [ipaddress]::3
PortMappings	PortNativeEMSName	SNMP Alarm using netsnmp script	Fully Qualified DNSName of VM followed by ::index from which netsnmp commands are sent. **Example**: abc.xyz.com::2
PortMappings	InterfaceNativeEMSName	SNMP Alarm using MIMIC simulator	IP Address of the Mimic Device followed by ::index. **Example**: [ipaddress]::4
PortMappings	InterfaceNativeEMSName	SNMP Alarm using netsnmp script	Fully Qualified DNSName of VM followed by ::index from which netsnmp commands are sent. **Example**: abc.xyz.com::4

3. For each of the data sheets, perform the following the steps:
   a. Log in to UIM and click on **Engineering Work Orders**.
   b. Click **Create** and select **Workflow Template** as **DataLoader**.
   c. Click **Save and Continue**.
   d. Navigate to the **Activity Details** tab and select **Load Data** (avoid clicking on the name link).
   e. Click **Assign** and select **User** as **Logged-in UIM Use**, and then click **Assign User**.
   f. Click **Start**.
   The **Activity1** status will change from **Ready** to **In Progress**.
   g. Click the **Load Data name** link and go to the **Activity Summary** page. Expand the **Automated Bulk Import** menu.
   h. Click **Browse** and select the Excel file (from the folder mentioned in step 5) to be uploaded.
   i. Click **Process**.
   j. Perform steps **g** and **h** for all excel files in the folder to be uploaded and processed, one file at a time.
   k. Click **Complete** on top of the **Activity Summary** page.
   This will change the **Load Data** status as **Completed**.
   l. Click on the name link next to **Engineering Work Order** and click **Actions**, then click **Approve Configurations**.
   m. Click **Issue Configurations** and click **Complete**.
   n. Repeat all steps for each excel file in all folders, in the given order.
4. After successfully completing the above, proceed with the following steps to create the protection path for service connectivity:
   a. Identify the service connectivities from **Texas Common**, in the **Texas_ServiceTrail_Connectivities_3.xlsx** and click **Connectivities**.

b. Navigate to each of the desired service connectivity in UIM, click **Connectivity**.

c. Click **Identification** and then click **Provide Name of Service Connectivity**.

d. Click **Search**. Select and edit the connectivities displayed under **Search Results**.

e. To create a new connectivity design version, open the **Connectivity Design** tab and click **Design Versions**. From the dropdown menu, select **Create New Version**.

f. Click on the "**+**" icon in **Path 1** located below **Jump To Path**.

g. To perform a path analysis under **Path 2**, click **Select Pipe**.

h. The **Source** and **Target** values will be auto populated. You can select the desired **Algorithm**, **Custom Tuning**, and click **Analyse**. This returns the results of the path analysis.

i. Select the desired path from the results by selecting the radio button next to Path and click **Assign**.

j. Once the path is successfully assigned, complete the connectivity design version.

5. Create the services manually from UIM as follows:

a. Log in to UIM, click on **Services** and then click **Create**.

b. Select the **Specification** as **Digital Twin Subscriber Service**. Enter the name and click **Save and Continue**.

c. Under the **Configurations** tab, click **Create** to create a service configuration. Click **Save And Close** to create **Service Configuration1**.

d. Go to **Configuration Items** and right-click on S**ervice:<Service name> - 1 - 1 - Se_1_1**.

e. Click **Add Configuration Item**. Update **Quantity of Service Trail** to **1** and click **Save And Close**.

f. Go to **Configuration Items**, right-click on S**ervice Trail**, then click **Add Config Item**.

g. Update the value of **Quantity of Service Connectivity** to **1** and click **Save And Close**.

h. Go to **Configuration Items**, click **Configurations** and then **Service Connectivity**.

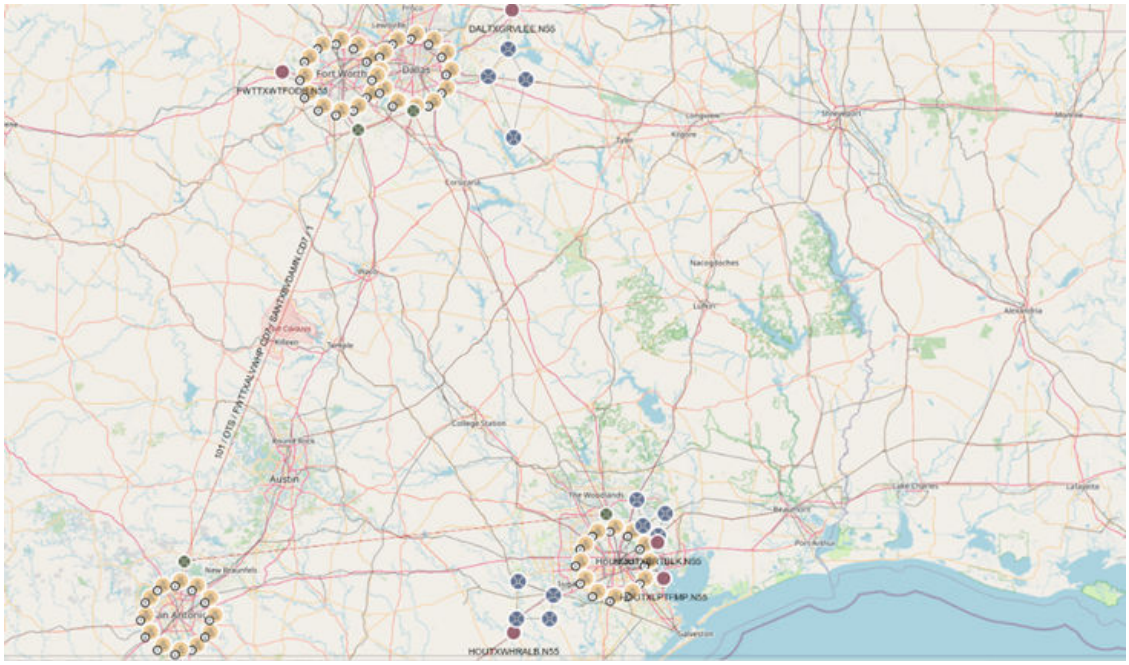
i. Click **Reference**. Then click **Search** under the **Connectivity Search** page to find and click **OK** to assign the desired Service Connectivity to Service Configuration.

j. After a Service Connectivity is assigned under a Service Configuration, click **Actions** dropdown menu on the top-right side and then click **Approve Issue and Complete** to complete the service configuration version.

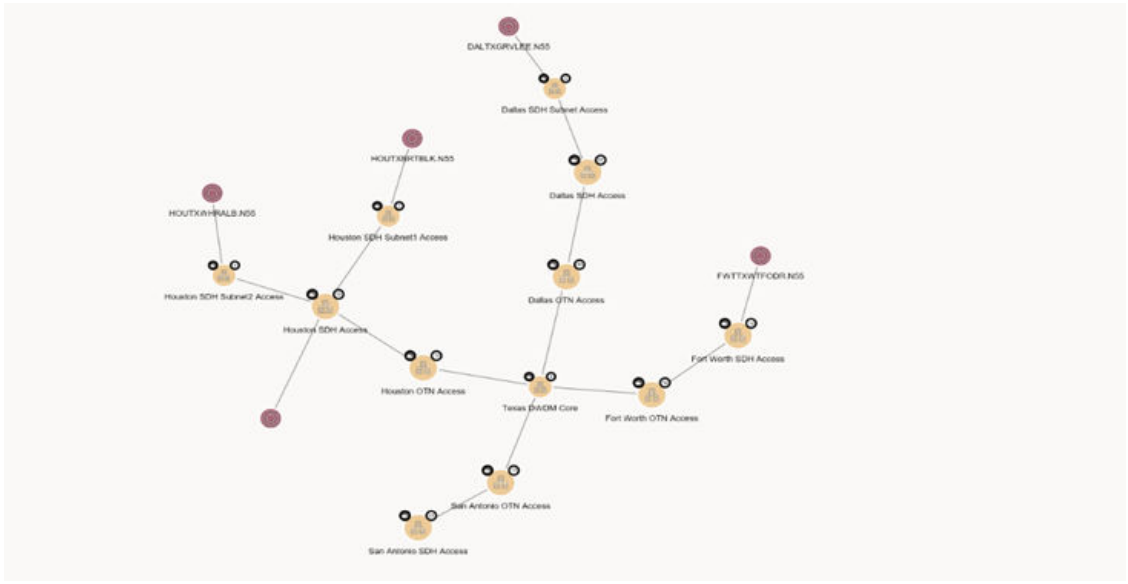
UIM Data Visualization

After the seed data (for DWDM/OTN) has been successfully imported into UIM, the following topology visualizations are available in the UIM application as part of ATA service. These views represent a subset of the complete topology and illustrate the CORBA and SNMP devices that are interconnected and the types of ports that are used.

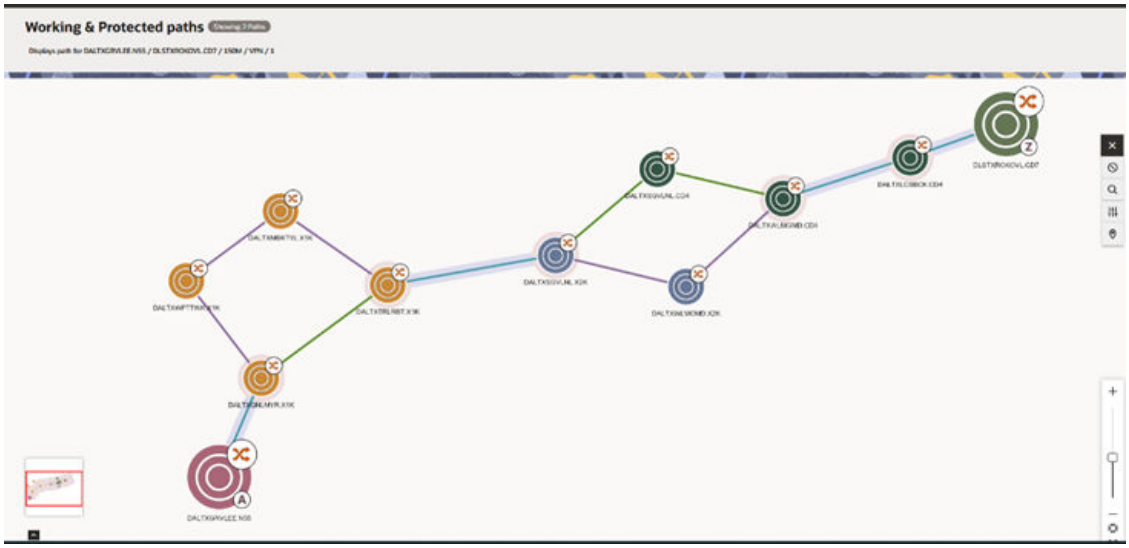
Topology Graph (Geo Map Layout): The topology graph displays the geographical map view of the topology components.



Topology Graph (Forced Layout): The topology graph displays the topology components (such as devices and connectivities) as shown in the following figure, and is the default layout presentation.



Topology Path View: The Topology Path view for Service Connectivity, as shown in the following figure, can be viewed under Service Topology. You must navigate to **Service Topology**, and under it, right-click on **Service Connectivity**, and then click **Show Paths**.



> **Note**
>
> For more information on configuration of the ATA visualization, refer to the *ATA User Guide*.

UIM and ATA Extensions

If you want to send alarms on SNMP node or subnode, you must make changes, as shown in the following example, in the **alarm-consumer-static-config.yaml** file under **$COMMON_CNTK\charts\ata-app\charts\ata\config\alarm-consumer** and restart the Alarm Consumer Microservice.

Example:

```
deviceMapping:
  #inventory:
  #  lookupFields: # The lookup is done according to the provided order.
Supported values are name, id & deviceIdentifier
  #  - name
  #  - id
  #  - deviceIdentifier
  customizeDeviceLookup:
    enabled: true
```

For more information, see *Unified Inventory and Topology Deployment Guide* for Alarm Consumer extensibility configurations.

Configuring Unified Assurance

This section describes the process of configuring Unified Assurance.

Installing Unified Assurance Solution Packages

To install the Unified Assurance solution packages:

1. Log in to the presentation server virtual machine (VM) using SSH.
2. Copy the following package files to the **/opt/assure1/distrib/packages** location.
   Where, **/opt/assure1** is the Unified Assurance installation directory.
   The UA solution packages are:
   - uniopsSmokeTest-rules-<Version>.pkg
   - uniopsSmokeTest-rules-<Version>.def
   - uniopsCorba-rules-<Version>.pkg
   - uniopsCorba-rules-<Version>.def
   - uniopsSnmp-rules-<Version>.pkg
   - uniopsSnmp-rules-<Version>.def
3. Run the following commands:
   Package installation steps:

```
sudo su -
cd /opt/assure1/
source .bashrc
cd bin/
./Package install uniopsSmokeTest-rules-<Version>
./Package install uniopsCorba-rules-<Version>
./Package install uniopsSnmp-rules-<Version>
```

> **Note**
>
> If you are re-installing packages, see “Troubleshooting” for more information.

4. Run the script below in web browser to create the SmokeTest Dashboard.

> **Note**
>
> This step is applicable only for SmokeTest of Unified Assurance package.

```
https://<Presentation Server host>/tools/uniops/dashboard.php
```

5. Click on **Create Device** under the **SmokeTest** dashboard to create a SmokeTest device.
6. Simulate an event for the SmokeTest device by clicking on **Simulate Event** under the dashboard and validate it in both Unified Assurance and UIM.

Unified Assurance Extensibility

This section provides information about Unified Assurance extensibility.

Alarm Filtering

The tmf688-event-processor microservice provides filtering capabilities to retain or discard specific events based on business or functional requirements from northbound applications, such as UIM Inventory. This filtering is disabled by default. Alarm filtering can be enabled and configured with custom filter conditions as shown below.

To enable Alarm filtering:

1. Edit config map for tmf688-event-processor. Set **FILTER_ENABLED** flag to **true** and save the config map:

   ```
   FILTER_ENABLED:
   "true"
   ```

2. Configure the alarm filtering criteria and conditions.
3. Login into Unified Assurance presentation server UI.
4. Navigate to **Configuration** and click **Rules**.
5. Expand **Core Rules**.
6. Expand **Default read-write branch** and click **processing**. Then click **event** and then **tmf688**.
7. Edit the **filter.json** rule to manage the filter conditions and filter criteria as per alarm filtering requirements.
8. Restart the pod for tmf688-event-processor microservice.

   ```
   kubectl delete pod <pod name> -n a1-zone1-pri
   ```

FCOM Rule Overrides

FCOM rules provide the transformation capability to transform fault events coming from NMS or EMS and devices to FCOM Assure1 events. The mappings in these rules can be re-configured through FCOM Rule Overrides.

For more information, refer to “FCOM Overrides” in the *Oracle Communications Unified Assurance Implementation Guide*.

4 Troubleshooting

This chapter describes common issues you may come across while configuring the Trouble to Resolve Reference Solution.

Cleaning an Existing Reference Solution Package

To clean an existing reference solution package:

1. SSH into presentation server VM.
2. Run the following commands:

```
sudo su -
    cd /opt/assure1/distrib/rules/core/processing/event/fcom
    rm -Rf uniops/
    su assure1 -
    cd /opt/assure1/var/checkouts/core/default/processing/event/fcom/
    a1svn delete uniops/
    a1svn commit -m "deleting custom rules dir"
    cd /opt/assure1/var/checkouts/core/RO_LOCKED/processing/event/fcom/
    a1svn delete uniops/
    a1svn commit -m "deleting custom rules dir"
```

3. Log in to the presentation server UI.
4. Navigate to **Configuration**, then to **Databases**, and finally to **Query Tools**.
5. Run the following command on **Assure1** schema:

```
delete from Packages where PackageName like 'uniops%'
```

6. (Optional) Delete the existing **uniops** package files from **/opt/assure1/distrib/packages** (only for cleanup purposes).

> **Note**
>
> - The above steps must be performed carefully to avoid accidentally cleaning core rules or packages.
> - If you are re-installing packages, then rules in the reference solution directory must be manually copied from **read-only branch (RO_LOCKED)** to **read-write branch (default)** into their corresponding sub-directories. This can be done from the Unified Assurance UI. For more information, see “Rules Packages” in *Unified Assurance Developer’s Guide.*
> - The updates to rules files will be placed in the default read-only repository. You can modify this repository only during the initial installation.