Installation and Configuration of NOI: Event Search feature

Speakers:

Elena Leopold
Senior Software Engineer
IBM Cloud Lab

Mark Allegakoen
Senior Software Engineer
IBM Cloud Lab

Mihaela Gheorghe
Senior Software Engineer
IBM Cloud Lab

Victor Diaz
Senior Software Engineer
IBM Cloud Lab

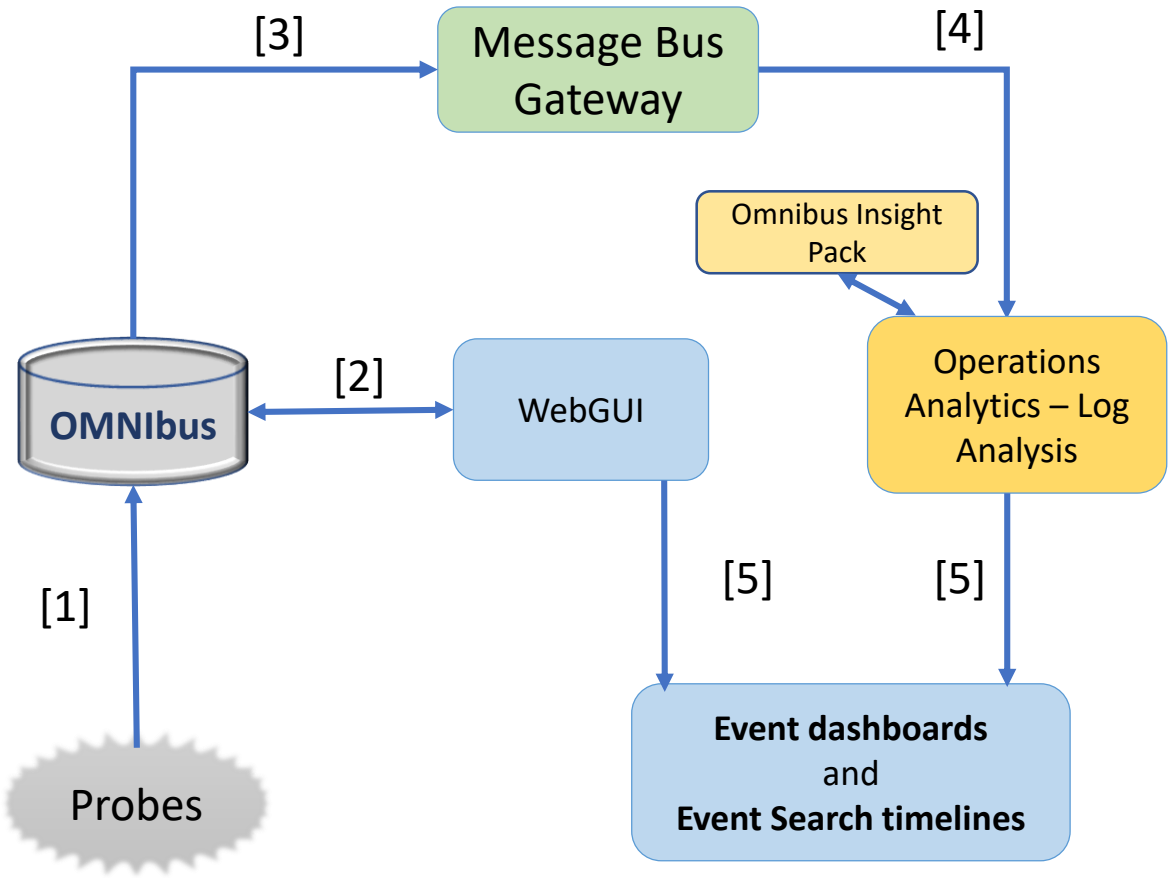
Agenda

- **Installation and configuration of NOI 1.6.0.1 – Event Search feature**
  - **Introduction**
  - **Install Omnibus, JazzSM/WAS, WebGUI and NOI Extension installation**
  - **Log Analysis – install and base configuration**
  - **LDAP and SSO configuration**
  - **Omnibus and Log Analysis integration**
  - **Log Analysis Best Practices**
  - **References**
- **Q&A**

NOI: Event Search feature

Data flow

Introduction: Data flow for NOI Event Search feature



[1] Events captured by the probes are forwarded to the Object Server.

[2] Events are displayed and managed in WebGUI

[3] Events are read from the Object Server by Message Bus Gateway

[4] Message Bus Gateway sends the data to OALA to be indexed. Omnibus Insight Pack parses the event data into a format suitable for OALA.

[5] Event results are visualized in OALA Event dashboards and timelines that are being accessed from WebGUI event lists

NOI: Event Search feature

Information and prerequisites

Introduction

- NOI base solution (Operation Management) - 3 main components and capabilities:

  - ✓ **Event Analytics**
  - ✓ **Event Search**
  - ✓ IBM Connections Integration

- Event Search – applies the search and analysis capabilities of Operations Analytics - Log Analysis to events that are monitored and managed by OMNIbus.

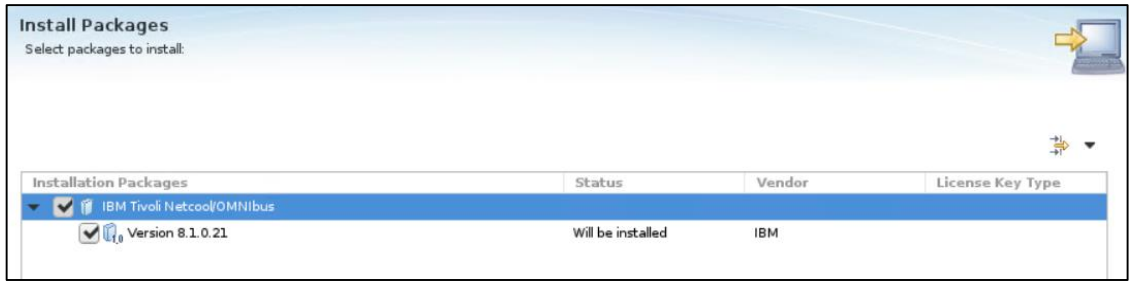
- Event Search feature requires the following products to be installed and configured (NOI 1.6.0.1):

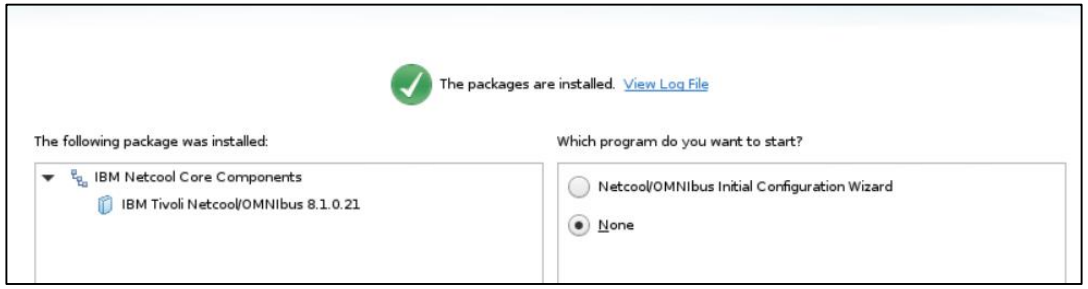
  - ✓ Netcool/OMNIbus core 8.1.0.21
  - ✓ JazzSM/DASH 3.1.3.5
  - ✓ WebSphere 8.5.5.15 and IBM Java SDK 8
  - ✓ WebGUI and Extension for NOI 8.1.0.17
  - ✓ Log Analysis 1.3.6
  - ✓ Message Bus Gateway
  - ✓ Netcool Omnibus Insight Pack

NOI: Event Search feature

Install Omnibus 8.1.0.21

- **New environment:**





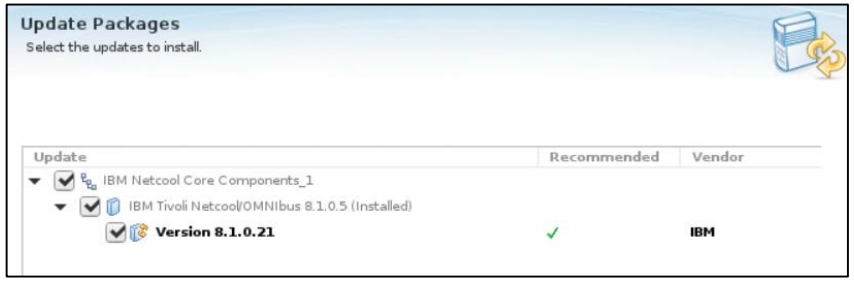
Create Object Server: /opt/IBM/tivoli/netcool/omnibus/bin/nco_dbinit -server NCOMS

Edit omni.dat: vi /opt/IBM/tivoli/netcool/etc/omni.dat

Generate the interface: /opt/IBM/tivoli/netcool/bin/nco_igen

Start Object Server: /opt/IBM/tivoli/netcool/omnibus/bin/nco_objserv -name NCOMS &

- **Existing environment:**



Install Omnibus 8.1.0.21

Response file for updating to Omnibus 8.1.0.21

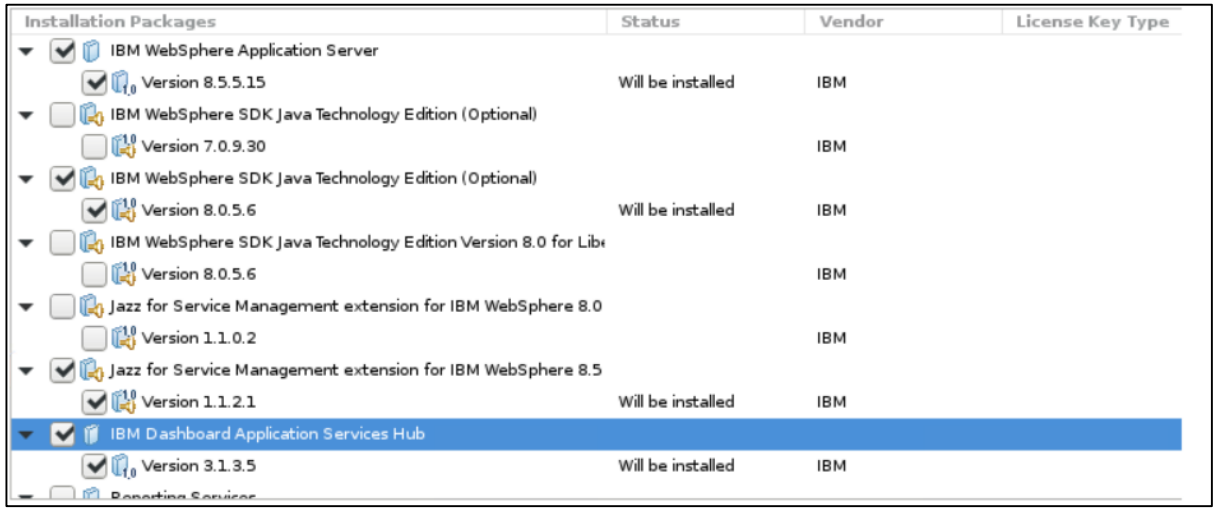
./imcl -input <fullpath>/omnibus_response_file.xml -acceptlicense -log <fullpath>/omnibus_update.log

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IBMIMShared'/>
  </variables>
  <server>
    <repository location='/tmpomnibus21/OMNIbusRepository'/>
  </server>
  <profile id='IBM Netcool Core Components' installLocation='/opt/IBM/tivoli/netcool'>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='user.migratedata,com.ibm.tivoli.omnibus.core' value='false'/>
    <data key='user.omnibus.core.java8warning.accepted,com.ibm.tivoli.omnibus.core' value='true'/>
  </profile>
  <install>
    <!-- IBM Tivoli Netcool/OMNIbus 8.1.0.21 -->
    <offering profile='IBM Netcool Core Components_1' id='com.ibm.tivoli.omnibus.core' version='5.50.88.20190905_0942'
features='nco_core_feature,nco_admin_gui_feature,nco_admin_tools_feature,nco_bridgeserv_feature,nco_extensions_feature,nco_g_objserv_feature,nco_gateways_support_feature
,nco_mib_manager_feature,nco_objserv_feature,nco_operator_gui_feature,nco_pa_feature,nco_probes_support_feature,nco_proxyserv_feature,nco_tec_migration'/>
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
  <preference name='offering.service.repositories.areUsed' value='false'/>
</agent-input>
```

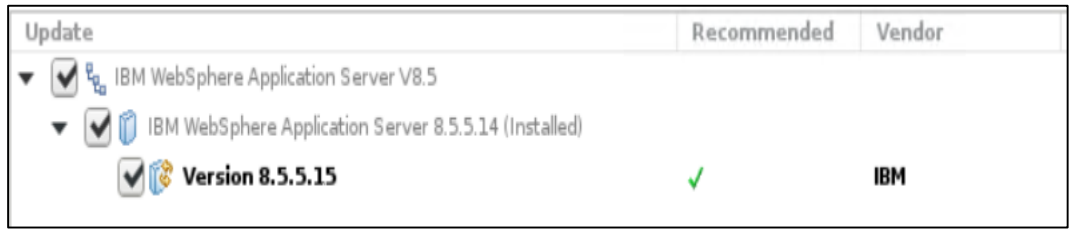
NOI: Event Search feature

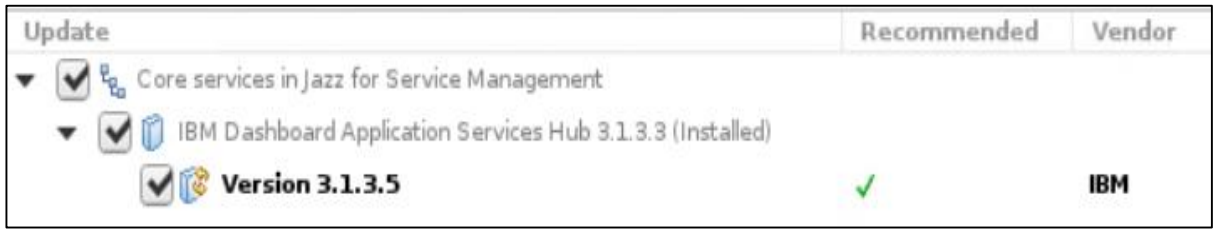
Install JazzSM 1.1.3.5, WAS 8.5.5.15, Java 8.0.5.6

- **New environment:**



- **Existing environment:**





NOI: Event Search feature

Install JazzSM 1.1.3.5, WAS 8.5.5.15, Java 8.0.5.6

Response file for updating to WAS 8.5.5.15

./imcl -input <fullpath>/websphere_response_file.xml -acceptlicense -log <fullpath>/websphere_update.log

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
 <variables>
  <variable name='sharedLocation' value='/opt/IBM/IBMIMShared'/>
 </variables>
 <server>
  <repository location='/mnt/images/ibm/was/8.5.5.15'/>
 </server>
 <profile id='IBM WebSphere Application Server V8.5' installLocation='/opt/IBM/WebSphere/AppServer'>
  <data key='cic.selector.arch' value='x86'/>
  <data key='user.wasjava' value='java8'/>
  <data key='user.internal.use.only.prev.wasjava' value='java8'/>
 </profile>
 <install>
  <!-- IBM WebSphere Application Server 8.5.5.15 -->
  <offering profile='IBM WebSphere Application Server V8.5' id='com.ibm.websphere.BASE.v85'
version='8.5.5015.20190128_1828' features='com.ibm.sdk.6_64bit,core.feature,ejbdeploy,embeddablecontainer,thinclient'/>
 </install>
 <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
</agent-input>
```

NOI: Event Search feature

Install JazzSM 1.1.3.5, WAS 8.5.5.15, Java 8.0.5.6

Response file for updating to DASH 3.1.3.5

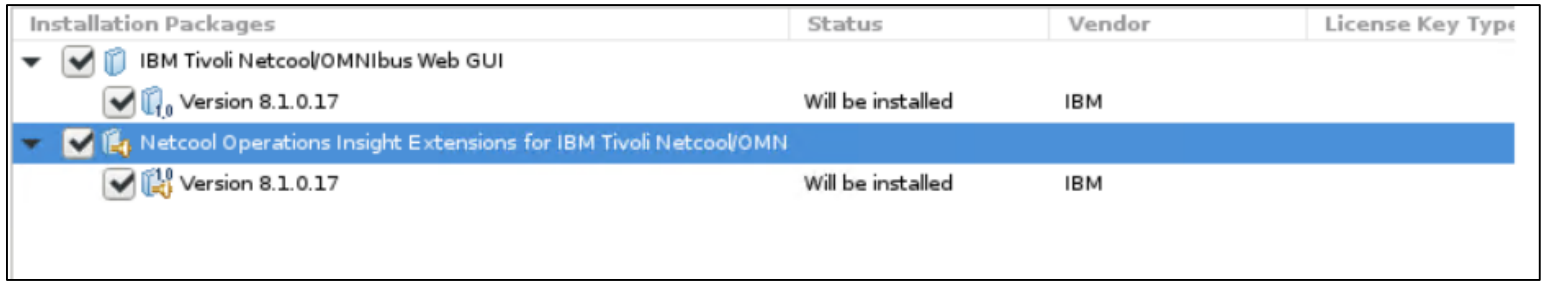
./imcl -input <fullpath>/dash_response_file.xml -acceptlicense -log <fullpath>/dash_update.log

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input> <variables> <variable name='sharedLocation' value='/opt/IBM/IBMIMShared'/> </variables>
 <server> <repository location='/tmpdash5/JazzSMRepository/disk1'/> </server>
 <profile id='Core services in Jazz for Service Management' installLocation='/opt/IBM/JazzSM'>
  <data key='cic.selector.arch' value='x86_64'/> <data key='user.BOOTSTRAP_ADDRESS' value='16312'/>
  <data key='user.CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS' value='16322'/> <data key='user.SOAP_CONNECTOR_ADDRESS' value='16313'/>
  <data key='user.CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS' value='16323'/> <data key='user.DCS_UNICAST_ADDRESS' value='16318'/>
  <data key='user.IPC_CONNECTOR_ADDRESS' value='16314'/> <data key='user.ORB_LISTENER_ADDRESS' value='16320'/>
  <data key='user.WC_defaulthost_secure' value='16311'/> <data key='user.REST_NOTIFICATION_PORT' value='16324'/>
  <data key='user.WC_defaulthost' value='16310'/> <data key='user.WC_adminhost_secure' value='16316'/>
  <data key='user.SAS_SSL_SERVERAUTH_LISTENER_ADDRESS' value='16321'/> <data key='user.WC_adminhost' value='16315'/>
  <data key='user.TIP_CONTEXT_ROOT' value='/ibm/console'/>
  <data key='user.WAS_HOME' value='/opt/IBM/WebSphere/AppServer'/>
  <data key='user.CREATE_NEW_WAS_PROFILE' value='false'/>
  <data key='user.WAS_PROFILE_PATH' value='/opt/IBM/JazzSM/profile'/>
  <data key='user.WAS_PROFILE_NAME' value='JazzSMProfile'/>
  <data key='user.WAS_HOST_NAME' value='craggy1.castle.fyre.ibm.com'/>
  <data key='user.WAS_SERVER_NAME' value='server1'/>
  <data key='user.WAS_NODE' value='JazzSMNode01'/>
  <data key='user.WAS_USER_NAME' value='smadmin'/>
  <data key='user.WAS_CELL' value='JazzSMNode01Cell'/>
  <data key='user.WAS_PASSWORD' value='MKzgom+ucqpj8e5dVuK8Dw=='/>
 </profile>
 <install>
  <!-- IBM Dashboard Application Services Hub 3.1.3.5 -->
  <offering profile='Core services in Jazz for Service Management' id='com.ibm.tivoli.tacct.psc.tip.install' version='3.1.3100.20191018-0333'
features='com.ibm.tivoli.tacct.psc.install.server.feature.tip.install,com.ibm.tivoli.tacct.psc.install.server.feature.tip.config'/>
 </install>
 <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
 <preference name='offering.service.repositories.areUsed' value='false'/>
</agent-input>
```

NOI: Event Search feature

Install WebGUI 8.1.0.17 and Extension for NOI

- **New environment:**



- **Existing environment - only WebGUI component installed without NOI Extension.**

Incorrect procedure:

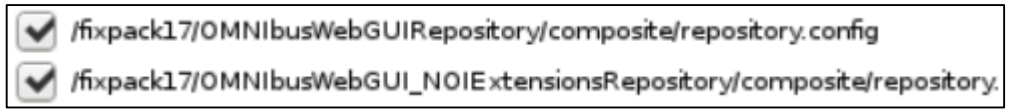
NOI: Event Search feature

Install WebGUI 8.1.0.17 and Extension for NOI

Correct procedure

- Add current WebGUI version repository to IIM and install NOI Extension

- Add repository for WebGUI Fix Pack 17 base and NOI extension and perform the upgrade

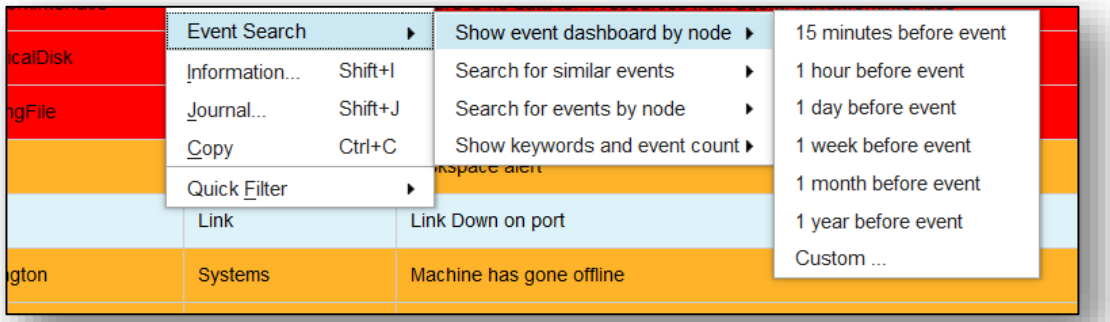


NOI: Event Search feature

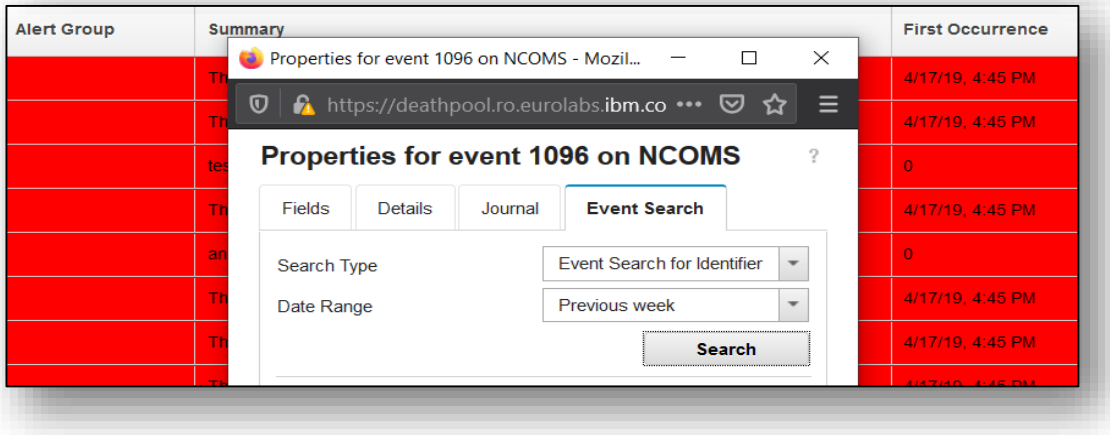
Configure WebGUI for Event Search

Configure server.init file located under /opt/IBM/netcool/gui/omnibus_webgui/etc/server.init as follows:

```
scala.url=https://deathpool.ro.eurolabs.ibm.com:9987/Unity
scala.datasource=omnibus
scala.version=1.3.0.2
scala.app.keyword=OMNIbus_SetSearchFilter
scala.app.static.dashboard=OMNIbus_Event_Distribution
```




```
scala.integratedsearch.enabled:true
scala.user: unityadmin
scala.password: <your_password>
```



Note: To configure search for ITNM network view you can change the below properties:

```
scala.app.event.topology.layer2=NM_Show_Alerts_Between_Two_Nodes_Layer2
scala.app.event.topology.layer3=NM_Show_Alerts_Between_Two_Nodes_Layer3
```

NOI: Event Search feature

Log Analysis

The main purpose - reduce problem diagnosis and resolution time, helping you to manage your infrastructure and applications more effectively

Log Analysis server

- The server where you install Log Analysis. This component contains the UI and all the main components such as the EIF Receiver, any Insight Packs and so on. You can also install the Indexing Engine on the same server. However, for performance reasons, in a typical installation, you install it on a separate server or a cluster of servers.

Indexing Engine servers (SOLR)

- In most installations, you install one or more instances of the Indexing Engine on a different server to the one where you installed the main Log Analysis component.

Remote data collection agents

- In most cases, you install an instance of one of the data collection agents such as the IBM Tivoli Monitoring Log File Agent (LFA) or Logstash on a remote server to collect data and send it back to Log Analysis.

Data storage servers (Standard Edition only)

- You can integrate Log Analysis with **Hadoop for long term data storage**

NOI: Event Search feature

Log Analysis – install and base configuration

1. Install Prerequisites
2. Install procedure (GUI, console and silent mode)
3. Upgrading the License
4. Installing and upgrading insight packs – Omnibus insight pack

NOI: Event Search feature

1. Prerequisites

Verify if you have a supported OS version

- **How to verify :**

cat /etc/redhat-release

- **Currently supported:**
  - ✓Red Hat Enterprise Linux (RHEL) Server 6/7 x86-64 , update 6.7-6.10 & 7.1-7.6
  - ✓Red Hat Enterprise Linux (RHEL) Server 6 IBM z Systems, base only
  - ✓Red Hat Enterprise Linux (RHEL) Server 7 IBM z Systems, update 7.1-7.6
  - ✓Red Hat Enterprise Linux (RHEL) Server 7 POWER System - Little Endian, update 7.1-7.6
  - ✓SUSE Linux Enterprise Server (SLES) 11/12 x86-64, base only
  - ✓SUSE Linux Enterprise Server (SLES) 11/12 IBM z Systems, base only

- **Log Analysis – Operating Systems compatibility report:**

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/osForProduct?deliverableId=B676C3E0B2CC11E9BB2725DFAC7F37BB&osPlatforms=Linux&duComponentIds=S001

Check if you have the necessary libraries and utilities

- **KornShell , yum , unzip**

- **python**-2.4.3-27.el5 and simple JSON rpm, python-simplejson. Python Version 2.6.6 to 2.6.8 include the required rpm.

How to check the python version :

python –version

- **the 64-bit compat-libstdc++ library (REDHAT)**

How to check if you already have it:

sudo /usr/bin/yum --noplugins list installed "libstdc++"

Disabling (SELinux)

- If the Security Enhanced Linux is in enforcing mode, then during the install the LFA component will fail. So, ensure that the SELinux policy is set to a permissive or disabled state.

How to modify:

As root edit /etc/selinux/config and set SELINUX=disabled or SELINUX=permissive. Restart the box

NOI: Event Search feature

1. Prerequisites - continued

Verifying the host server IP address and names

/etc/hosts for a server that uses a static IP address

IP	FQDN	SHORT-HOSTNAME
9.20.210.114	deathpool.ro.eurolabs.ibm.com	deathpool

/etc/hosts for a Dynamic Host Configuration Protocol (DHCP) server that uses a loop back IP address

LOOPBACK-IP	FQDN	SHORT-HOSTNAME
127.0.0.1	deathpool.ro.eurolabs.ibm.com	deathpool

Verify the output of the

- hostname -i -> you should see the IP ; eg 9.20.210.114
- hostname -f -> FQDN as its set in the /etc/hosts eg deathpool.ro.eurolabs.ibm.com .ibm.com
- hostname -> the short-hostname ; eg deathpool

Create a non-root user

How to an non-root user : useradd -m -d /home/netcool netcool

Increase the number of open files and virtual memory

How to check :
ulimit –n and ulimit -v

How to modify:
as root, edit /etc/security/limits.conf and add
<user-id> hard nofile 200000
<user-id> soft nofile 200000
<user-id> hard as unlimited
<user-id> soft as unlimited
where <user-id> is the user id used to install the Indexing Engine on the server, in our example will be netcool

Check/increase the max number of system file descriptors

How to check : cat /proc/sys/fs/file-nr
output : 20896 0 25130

How to increase the max number to 600000
sysctrl -w fs.file-max=600000
Eg output:
20896 0 600000

2. Installing procedure

Before starting the install , run the prerequisite scanner and check the output results of the scanner and resolve any failed checks.

How to use it: *open a terminal*
export ENV_NAME=True
./prereq_checker.sh "ILA 01350000" detail outputDir=<output_directory>

Install in GUI mode

If the Installation Manager is not installed

- ❑ Go to the location where you have transferred the Log Analysis files , eg /home/netcool/kit/LA/, run
- ❑ ./install.sh
- ❑ follow the instructions

If the Installation Manager was previously installed:

- ❑ open it, using : IM_HOME/eclipse/IBMIM
- ❑ Then go to File -> Preferences -> Repository -> Add Repository ;

eg /home/netcool/kit/LA/diskTag.inf

- ❑ Save the changes and press Install and follow the instructions

NOI: Event Search feature

Log Analysis – install and base configuration

2. Installing procedure – console mode

```
./install.sh -c
Starting installation in console mode...
Preprocessing the input.
Loading repositories...
Preparing and resolving the selected packages...
=====> IBM Installation Manager> Install
Select packages to install:
   1. [X] IBM® Installation Manager 1.8.2
   2. [X] IBM Operations Analytics - Log Analysis  1.3.5.0

   O. Check for Other Versions, Fixes, and Extensions
   N. Next,    C. Cancel
-----> [N]
Validating package prerequisites...

=====> IBM Installation Manager> Install> Licenses

Read the following license agreements carefully.
View a license agreement by entering the number:
   1. IBM Installation Manager - License Agreement
   2. IBM Operations Analytics - Log Analysis - License Agreement
Options:
   A. [ ] I accept the terms in the license agreements
   D. [ ] I do not accept the terms in the license agreements

   B. Back,    C. Cancel
-----> [C] A

=====> IBM Installation Manager> Install> Licenses
Read the following license agreements carefully.
View a license agreement by entering the number:
   1. IBM Installation Manager - License Agreement
   2. IBM Operations Analytics - Log Analysis - License Agreement
Options:
   A. [X] I accept the terms in the license agreements
   D. [ ] I do not accept the terms in the license agreements
   B. Back,    N. Next,    C. Cancel
-----> [N] N
```

```
=====> IBM Installation Manager> Install> Licenses> Shared Directory
Installation Manager installation location:
    /home/netcool/IBM/InstallationManager/eclipse

Shared Resources Directory:
    /home/netcool/IBM/IBMIMShared

Options:
   L. Change Installation Manager Installation Location
   M. Change Shared Resources Directory

   B. Back,    N. Next,    C. Cancel
-----> [N]
Finding compatible package groups...

=====> IBM Installation Manager> Install> Licenses> Shared Directory> Location
New package group:
   1. [X] IBM Operations Analytics - Log Analysis

Selected group id: "IBM Operations Analytics - Log Analysis"
Selected location: "/home/bubu/IBM/LogAnalysis"
Selected architecture: 64-bit

Options:
   M. Change Location

   B. Back,    N. Next,    C. Cancel
-----> [N]

=====> IBM Installation Manager> Install> Licenses> Shared Directory> Location> Features

IBM® Installation Manager

IBM Operations Analytics - Log Analysis
   1. [X] IBM Operations Analytics - Log Analysis 1.3.6.0
   2. [X] Apache Solr 5.2.1
   3. [X] IBM Tivoli Log File Agent 06.30.00.04

   B. Back,    N. Next,    C. Cancel
-----> [N]
```

```
=====> IBM Installation Manager> Install> Licenses> Shared Directory>
 Location> Features> Custom panels

---- Configuration for IBM Operations Analytics - Log Analysis 1.3.6.0
Application WebConsole Port:
-----> [9988]
Application WebConsole Secure Port:
-----> [9987]
Database Server Port:
-----> [1627]
EIF Receiver Port:
-----> [5529]
ZooKeeper Port:
-----> [12181]
Apache Solr Search Port:
-----> [8983]
Apache Solr Stop Port:
-----> [7205]

   B. Back,    N. Next,    C. Cancel
-----> [N]

=====> IBM Installation Manager> Install> Licenses> Shared Directory>
 Location> Features> Custom panels> Summary

Target Location:
  Package Group Name      : IBM Installation Manager
  Installation Directory  : /home/netcool/IBM/InstallationManager/eclipse
  Package Group Name      : IBM Operations Analytics - Log Analysis
  Installation Directory  : /home/netcool/IBM/LogAnalysis
  Shared Resources Directory : /home/netcool/IBM/IBMIMShared
Translations:
    English
Packages to be installed:
    IBM® Installation Manager 1.8.2
    IBM Operations Analytics - Log Analysis 1.3.6.0

Options:
   G. Generate an Installation Response File
   B. Back,    I. Install,    C. Cancel

-----> [I]
         25%         50%         75%         100%
----------|-----------|-----------|-----------|
.....................................................
```

2. Installing procedure – silent mode

Obtaining the response file:

1. Use the record option while installing on a box and use the resulting file on different environment .

cd IM_HOME/eclipse
./IBMIM -record /response_files/install_product.xml

2. Manually create the response file
./imcl -silent listAvailablePackages -repositories "/kit/OALA/diskTag.inf" -features -long

Output:

com.ibm.tivoli.scloganalytics_1.3.5.20191018_0247 : IBM Operations Analytics - Log Analysis : 1.3.5.0 : IBM Operations Analytics - Log Analysis,Apache Solr,LOG_FILE_AGENT

Silent install command:

cd IM_HOME/eclipse
./imcl -acceptLicense -showProgress input /response_files/install_product.xml -log product_log.xml

The content of a sample response file - install_product.xml :

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
 <variables>
  <variable name='sharedLocation' value='/opt/IBM/IBMIMShared'/>
 </variables>
 <server>
  <repository location='/kit/OALA'/>
 </server>
 <profile id='IBM Operations Analytics - Log Analysis' installLocation='/home/netcool/IBM/LogAnalysis'>
  <data key='cic.selector.arch' value='x86_64'/>
  <data key='user.unity.port.number,com.ibm.tivoli.scloganalytics' value='9988'/>
  <data key='user.unity.secureport.number,com.ibm.tivoli.scloganalytics' value='9987'/>
  <data key='user.database.port.number,com.ibm.tivoli.scloganalytics' value='1627'/>
  <data key='user.eif.port.number,com.ibm.tivoli.scloganalytics' value='5529'/>
  <data key='user.searchengine.port.number,com.ibm.tivoli.scloganalytics' value='8983'/>
  <data key='user.searchengineQS.port.number,com.ibm.tivoli.scloganalytics' value='7205'/>
  <data key='user.zookeeper.port.number,com.ibm.tivoli.scloganalytics' value='12181'/>
 </profile>
 <install>
  <!-- IBM Operations Analytics - Log Analysis  1.3.6.0 -->
  <offering profile='IBM Operations Analytics - Log Analysis' id='com.ibm.tivoli.scloganalytics'
version='1.3.5.20191018_0247' features='IBM Operations Analytics - Log Analysis,Apache
Solr,LOG_FILE_AGENT'/>
 </install>
 <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
</agent-input>
```

NOI: Event Search feature

Troubleshooting the install

9/10 from all the reported install issues are cause by missing prerequisites

If you need assistance in troubleshooting the issue - open a case and send us :

- IM_HOME/tools/imcl exportInstallData outputFileName.zip
- the logs from the LA_home install directory
- the output of
  - the prerequisite scanner
    export ENV_NAME=True
    ./prereq_checker.sh "ILA 01320000" detail
  - *cat /etc/selinux/config*
  - *cat /etc/hosts*
  - *hostname –f*
  - *hostname -i*
  - *hostname*

- ***CRIMA1217E: A problem occurred during the execution of the /opt/IBM/LogAnalysis/com.ibm.tivoli.scloganalytics.xml file***
- ***CTGLC0605E : An exception was thrown while installing the content. CTGLC0518E : Unity server unavailable: CTGLA1003E : Authentication failed for REST request***
- "***Failed to launch. Could not retrieve OAuth access token.***" when opening a dashboard or Custom Search Dashboard
- If you cannot install the IBM Tivoli Monitoring Log File Agent or the check box is grayed out, you are either missing some of the prerequisites or the IBM Tivoli Monitoring Log File Agent is already installed on the same server. You need to complete one of the following actions:

✓ Check that you have meet all the required prerequisites.
✓ If you do not want to use the existing IBM LFA , you can stop the install and remove it.
✓ If you want to use the IBM LFA to load data into Log Analysis, you can continue with the installation, after you complete it, you need to configure the IBM LFA.

3. Upgrading the license

IBM Operations Analytics Log Analysis Entry edition - with this type of license you can load up to 2 Gigabytes (GBs) of data daily for free. If you need to upgrade to the **Standard edition**, you need to purchase a product license. To purchase a license key, contact your IBM sales representative or go to Passport Advantage at and choose the type of installation you require.

There are two types of enablement keys :

- Based on the amount of Data being ingested into Log Analysis. (CNEM4EN)
- Based on the number of devices (Managed virtual servers and Managed virtual network devices) the data is being ingested into (CNE6FEN) - NOI users are entitled for only Device Based license

To verify your current version, use the unity_VersionInfoUtility.sh utility.

```
/home/netcool/IBM/LogAnalysis/utilities/unity_VersionInfoUtility.sh  | grep EDITION
```

Example output:

```
IBM Operations Analytics - Log Analysis_1_3_5_3_201901030600 STANDARD INGESTION BASED EDITION
```

To upgrade the edition:

```
/home/netcool/IBM/LogAnalysis/utilities/unity_change_edition_util.sh -p <license_file_path> .
```

A restart is required

4. Installing and upgrading an insight pack - Omnibus Insight pack

- ❑ Download the latest Omnibus Insights pack and move it on the Log Analysis box. Make sure the non-root user that you used to install the Log Analysis has permissions over the patch.
- ❑ Create a new OMNIbus directory under $UNITY_HOME/unity_content
- ❑ Copy the Netcool/OMNIbus Insight Pack installation package to $UNITY_HOME/unity_content/OMNIbus.

❖ To install the Omnibus Insight Pack, use the following command as an example:

```
cd /home/netcool/IBM/LogAnalysis/utilities/
./pkg_mgmt.sh -install /home/netcool/IBM/LogAnalysis/unity_content/OMNIbus/OMNIbusInsightPack_v1.3.0.2.zip
```

❖ If you need to upgrade the Omnibus Insight Pack, you can use the following command :

```
cd /home/netcool/IBM/LogAnalysis/utilities/
./pkg_mgmt.sh -upgrade /home/netcool/IBM/LogAnalysis/unity_content/OMNIbus/OMNIbusInsightPack_v1.3.1.0.zip
```

Doc reference: https://www.ibm.com/support/knowledgecenter/en/SSPFMY_1.3.6/com.ibm.scala.doc/extend/iwa_extend_pkg_mgmt_cmd_c.html

Troubleshooting the install or update of an insight pack

In case of failure is best to start from the messages listed in console where you have ran the script. Make sure that you are installing the latest insights packs available .

Most of the times, the reported issues were caused by the pkg_mgmt.sh & pkg_mgmt.xml (package management scripts) manual modifications or when there were permissions problems.

Anyway, in case of failure, its advised first to check if there are any leftovers on the environment. So, First, use the pkg_mgmt.sh -list command to determine whether the Insight Pack was previously installed.

To list the currently installed insight packs:
cd /home/netcool/IBM/LogAnalysis/utilities/
./the pkg_mgmt.sh –list

and check if the insight pack is listed. If its not, then reattempt the install/upgrade

If its listed, its better to remove the entry first, then reattempt the install/upgrade

To uninstall an insight pack:
./pkg_mgmt.sh -uninstall /home/netcool/IBM/LogAnalysis/unity_content/OMNIbusInsightPack_v1.3.1.0

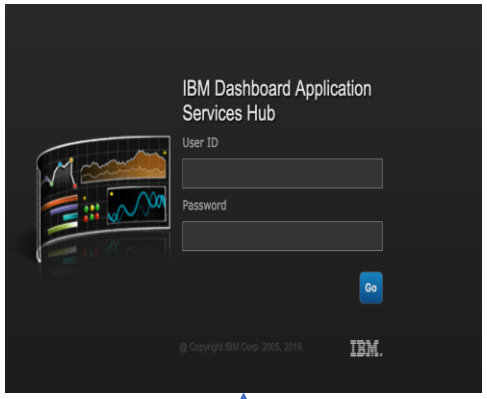
NOI: Event Search feature

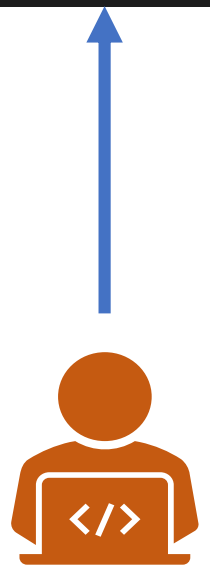
Log Analysis – LDAP and SSO configuration

1. **LDAP configuration**
2. **SSO configuration**

NOI: Event Search feature

LDAP Configuration





Event Viewer

Edit View Alerts Tools Help

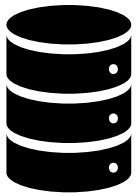
Default

Sev	Ack	Node	Alert Group	Summary
		NtMonitoredLogsReport		There is no data for 1 resources fro
		4		There is no data for 1 resources fro
				test event
				There is no data for 1 resources fro
				another test event
		.eurolabs.ibm.cc	WebGUI Status	ALERT: Web GUI NCOMS data sou
		tionStatus		There is no data for 2 resources fro
				ALERT: Web GUI Security Reposit
				s fro
				s fro
	No	NtProcessor		s fro
	No	deathpool.ro.eurolabs.ibm.cc	WebGUI Status	a sou
	No	NtNetworkInterface		There is no data for 1 resources fro

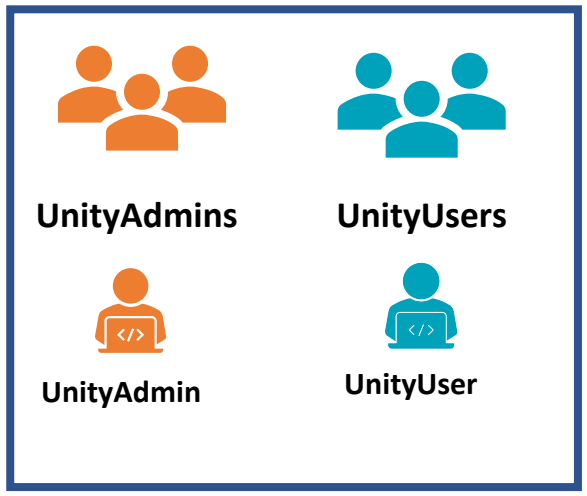
- Acknowledge ⌘A
- De-acknowledge ⌘D
- Prioritize
- Suppress/Escalate
- Take ownership
- User Assign
- Group Assign
- Delete
- Ping
- Event Search
  - Show event dashboard by node
  - Search for similar events
    - 15 minutes before event
    - 1 hour before event
    - 1 day before event
    - 1 week before event
    - 1 month before event
    - 1 year before event
    - Custom ...
  - Search for events by node
  - Show keywords and event count
- Information... ⇧I
- Journal... ⇧J
- Copy ⌘C
- Quick Filter

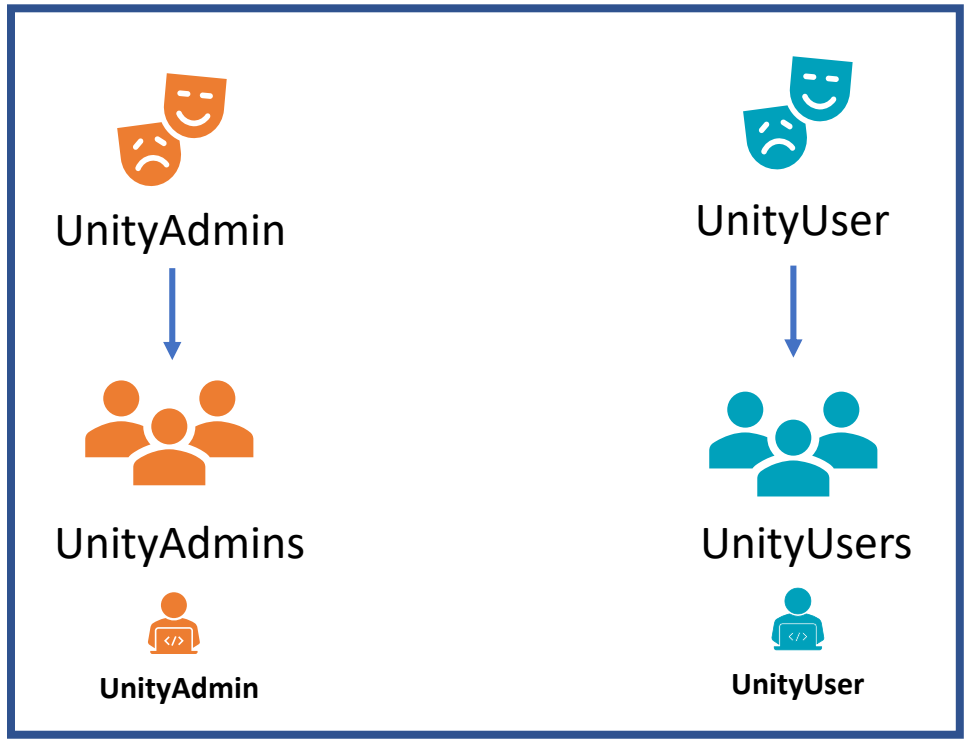
NOI: Event Search feature

LDAP Configuration



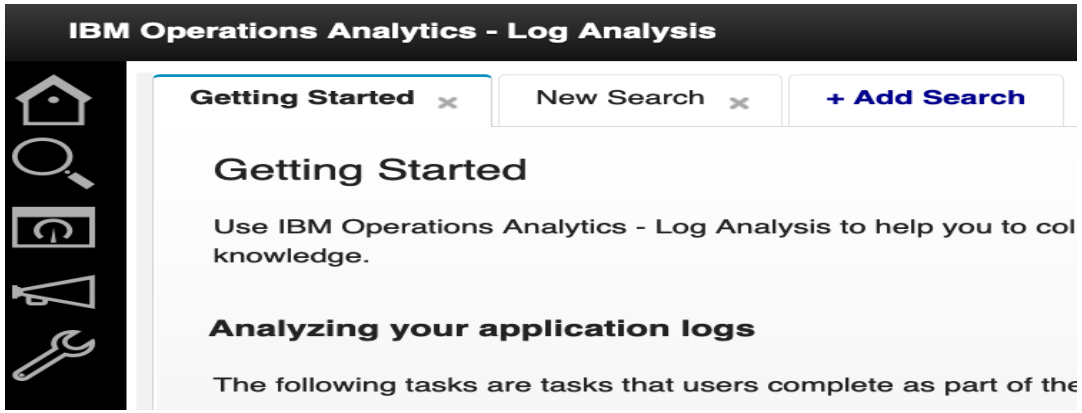
LDAP



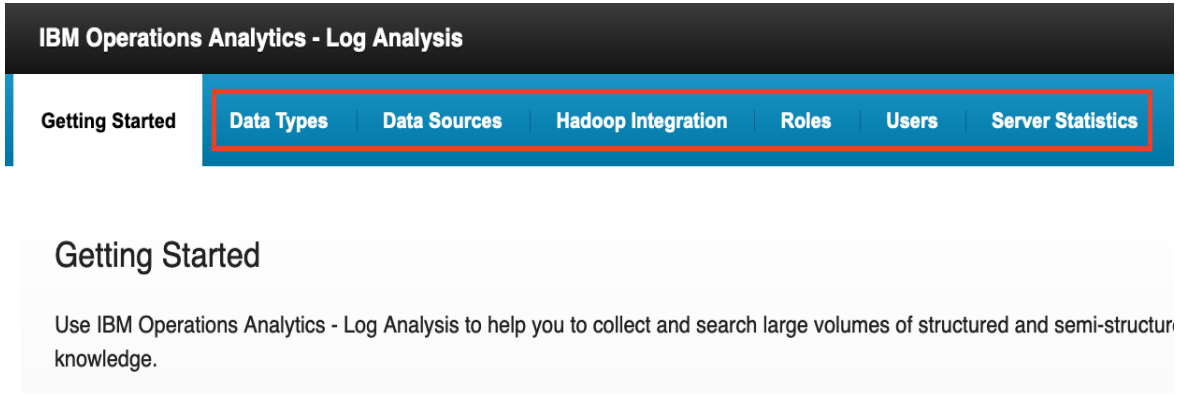


LDAP configuration

Users with the unityuser role can access the search workspace.



Users with the unityadmin role can access the search and administration workspaces.



By default, all users are assigned the unityuser role.

NOI: Event Search feature

LDAP Configuration - scripted

*<HOME>/IBM/LogAnalysis/utilities/**ldapRegistryHelper.sh*** *config | enable*

*<HOME>/IBM/LogAnalysis/utilities/**ldapRegistryHelper.properties***

*<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/**ldapRegistry.xml***

ldap_hostname_property=9.20.210.113
ldap_port_property=389
ldap_baseDN_property=CN=Users,DC=eurolabs,DC=ibm,DC=com
ldap_bindDN_property=CN=Admin,CN=Users,DC=eurolabs,DC=ibm,DC=com
ldap_bindPassword_property=myPassword *
ldap_realm_property=SampleLdapIDSRealm **
ldap_id_property=LdapRegistryId
ldap_ignoreCase_property=true
ldap_recursiveSearch_property=true

* The bindPassword value will be encrypted by the *ldapRegistryHelper* script and will appear in its encrypted form in the resulting ldapRegistry.xml file. The password from this file will automatically be removed at the completion of the script processing.

** The ldap_realm_property value should be the same that was set for JazzSM, while setting the AD as user repository.

NOI: Event Search feature

LDAP Configuration - manual

*<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/**ldapRegistry.xml***

- With the server connectivity properties:
  - **ID**
  - **realm**
  - **host**
  - **port**
  - **baseDN**
  - **bindDN**

```
<server>
  <ldapRegistry
    host="9.20.210.113"
    port="389"
    baseDN="CN=Users,DC=eurolabs,DC=ibm,DC=com"
    bindDN="CN=smadminad,CN=Users,DC=eurolabs,DC=ibm,DC=com"
    bindPassword="{xor}GjM6MT5xbm9xEzowLzAzOw=="
    realm="SampleLdapIDSRealm"
    id="LdapRegistryId"
    ignoreCase="true"
  recursiveSearch="true"
    activedFilters="unityactivedfilters"
    ldapType="Microsoft Active Directory">
  </ldapRegistry>
```

- and the filters to the object classes relevant to the schema of the LDAP implementation, in this case, AD:

```
 <activedLdapFilterProperties id="unityactivedfilters"
    userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
    groupFilter="(&amp;(cn=%v)(objectcategory=group))"
    userIdMap="user:sAMAccountName"
    groupIdMap="*:cn"
    groupMemberIdMap="memberOf:member"/>
</server>
```

- LDAP binding password can be encoded using utility:

<HOME>/IBM/LogAnalysis/bin/encode myPassw0rd

NOI: Event Search feature

LDAP Configuration - manual

- Disable the database-managed custom user registry:

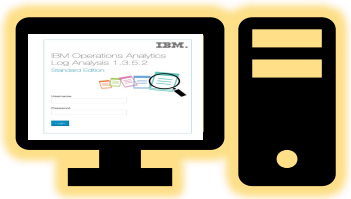
<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/server.xml

```
<!-- Include the basic registry predefined with default users and groups -->
<!-- <include optional="true" location="${server.config.dir}/ unityUserRegistry.xml"/>
 -->
```

- Add an include tag to replace the reference to the custom user registry with a reference to the *ldapRegistry.xml* file.

```
...
<feature>ldapRegistry-3.0</feature>
</featureManager>
<!-- Include the basic registry predefined with default users and groups -->
<!-- <include optional="true" location="${server.config.dir}/unityUserRegistry.xml"/> -->
<!-- Include the LDAP registry -->
<include optional="true" location="${server.config.dir}/ldapRegistry.xml"/>
```

LDAP configuration – LDAP groups to security role mapping



To map groups to the security roles, replace *<Group_name>* with the group names. For example:

<HOME>/IBM®/LogAnalysis/wlp/usr/servers/Unity/UnityConfig.xml

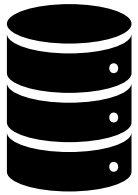
```
<security-role name="UnityUser”>
                        <group name="UnityUsers"/>
                        <group name="UnityAdmins" />
                        <group name="<Group_name1>"/>
                        <group name="<Group_name2>"/>
            </security-role>
 <security-role name="UnityAdmin">
                        <group name=" UnityAdmins "/>
                        <group name="TestLAAdmin"/>
            </security-role>
```

We need to add custom groups to the OAuth security role to enable access to Log Analysis.

```
<oauth-roles>
            <authenticated>
                        <group name="UnityUsers"/>
                        <group name="UnityAdmins"/>
                        <group name ‘TestLAAdmin “/>
                        <group name="<Group_name2>/>
             </authenticated>
</oauth-roles>
```

NOI: Event Search feature

LDAP Configuration - LDAP users mapping



LDAP

- **UnityAdmins** (CN= **UnityAdmins**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – LA admin group
- **UnityUsers** (CN= **UnityUsers**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – La group
- **TestLAAdmin** (CN= **TestLAAdmin**,CN=Users,DC=eurolabs,DC=ibm,DC=com) LA custom group
- **smadminad** (CN=**smadminad**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – bind user
- **unityadmin** (CN= **unityadmin**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – LA admin user
- **unityuser** (CN= **unityuser**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – LA user
- **TestUser** (CN= **TestUser**,CN=Users,DC=eurolabs,DC=ibm,DC=com) - LA custom user

LDAP configuration – LDAP users mapping

Create the AD users in the GUI

UnityAdmins (CN= **UnityAdmins**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – LA admin group

UnityUsers (CN= **UnityUsers**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – La group

TestLAAdmin (CN= **TestLAAdmin**,CN=Users,DC=eurolabs,DC=ibm,DC=com) LA custom group

smadminad (CN=**smadminad**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – bind user

unityadmin (CN= **unityadmin**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – LA admin user

unityuser (CN= **unityuser**,CN=Users,DC=eurolabs,DC=ibm,DC=com) – LA user

TestUser (CN= **TestUser**,CN=Users,DC=eurolabs,DC=ibm,DC=com) - LA custom user

IBM Operations Analytics - Log Analysis

Getting Started | Data Types | Data Sources | Hadoop Integration | Roles | Users

You can create and modify users to assign role-based access control to individual users in the Users worksp

User Name	Display Name
unityadmin	unityadmin
unityuser	unityuser
Admin	Admin
TestUser	TestUser

Manage Users

Search for Users

Search by: User ID | Search for: * | Maximum results: 100

Search

17 users matched the search criteria.

Create... | Delete | Select | Select an action...

Select	User ID	First name	Last name	E-mail	Unique Name
	Admin				CN=Admin,CN=Users,DC=eurolabs,DC=ibm,DC=com
	Elana	Elena	Elana		CN=Elena Elana,CN=Users,DC=eurolabs,DC=ibm,DC=com
	Guest				CN=Guest,CN=Users,DC=eurolabs,DC=ibm,DC=com
	InaLogin	Ina			CN=Ina,CN=Users,DC=eurolabs,DC=ibm,DC=com
	PItest	PItest			CN=PItest,CN=Users,DC=eurolabs,DC=ibm,DC=com
	Testuser	test			CN=TestUser,CN=Users,DC=eurolabs,DC=ibm,DC=com
	dexterkerb	dexterkerb			CN=dexterkerb,CN=Users,DC=eurolabs,DC=ibm,DC=com
	displayname	Firstname	Lastname		CN=Firstname Lastname,CN=Users,DC=eurolabs,DC=ibm,DC=com
	elena	elena			CN=elena,CN=Users,DC=eurolabs,DC=ibm,DC=com
	itadmin				CN=itadmin,CN=Users,DC=eurolabs,DC=ibm,DC=com
	krbtgt				CN=krbtgt,CN=Users,DC=eurolabs,DC=ibm,DC=com
	smadmin	smadmin	smadmin		uid=smadmin,o=defaultWIMFileBasedRealm
	smadminad	smadminad			CN=smadminad,CN=Users,DC=eurolabs,DC=ibm,DC=com
	superuser	superuser			CN=superuser,CN=Users,DC=eurolabs,DC=ibm,DC=com
	unityadmin	unityadmin			CN=unityadmin,CN=Users,DC=eurolabs,DC=ibm,DC=com

LDAP configuration – Changing the default administrative user

Need IBM® Operations Analytics Log Analysis 1.3.3 Fix Pack 1 or later

- Edit file:

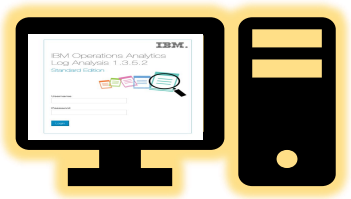
  <HOME>/IBM/LogAnalysis/utilities/authorization/admin.properties

- LDAP_USER_NAME=TestUser
- DISPLAY_NAME=LA Administrator
- DESCRIPTION=Admin for LA and LDAP

- Run script:

<HOME>/IBM/LogAnalysis/utilities/authorization/makeLAadmin.sh admin.properties

LDAP configuration – Changing the default administrative user



Following this change, we must generate a new password:

$ cd <HOME>/IBM/LogAnalysi/utilities

$ ./unity_securityUtility.sh encode MynewLApass
Using keystore file unity.ks.
/home/netcool/IBM/LogAnalysis/utilities/../wlp/usr/servers/Unity/keystore/unity.ks
{aes}CEDD2A7F55E54FC6EDC96DBCEE43C68710B523B1E1261518E194248600BCBD75

And update the following files with the new user and password:

- /home/netcool/IBM/LogAnalysis/utilities/datacollector-client/javaDatacollector.properties
- /home/netcool/IBM/LogAnalysis/remote_install_tool/config/rest-api.properties
- /home/netcool/IBM/LogAnalysis/UnityEIFReceiver/config/unity.conf
- /home/netcool/IBM/LogAnalysis/utilities/pkg_mgmt.sh
- /home/netcool/IBM/LogAnalysis/solr_install_tool/scripts/register_solr_instance.sh

NOI: Event Search feature

LDAP configuration – configure DASH / WAS

Log to WAS console - https://hostname.domain.com:16313/ibm/console and go to

Security -> Global Security -> Under User account repository click on *Configure*

Global security

Use this panel to configure administration and the default application security policy. This security configurat
default security policy for user applications. Security domains can be defined to override and customize the s

Security Configuration Wizard | Security Configuration Report

Administrative security

Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

Enable application security

Java 2 security

Use Java 2 security to restrict application access to local resources

Warn if applications are granted custom permissions

Restrict access to resource authentication data

User account repository

Realm name: SampleLdapIDSRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories | Configure... | Set as current

Authentication

Authentication mechar

LTPA

Kerberos and LTPA

Kerberos configur

SWAM (deprecated

Authentication cache s

Web and SIP secur

RMI/IIOP security

Java Authenticatio

Enable Java Authe

Providers

Use realm-qualifie

- Security domains
- External authorizat
- Programmatic sess
- Custom properties

NOI: Event Search feature

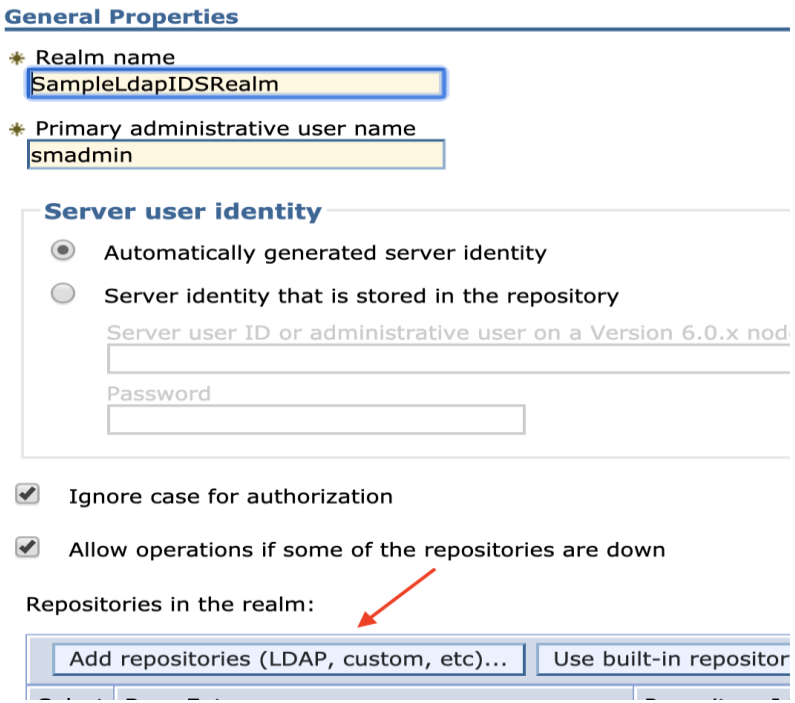
LDAP configuration – configure DASH / WAS

Log to WAS console - https://hostname.domain.com:16313/ibm/console and go to

Security -> Global Security -> Under User account repository click on *Configure*

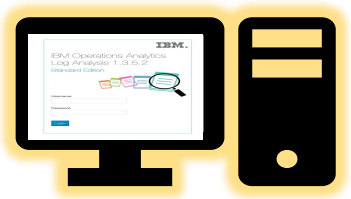
1. **Set the Realm name to SampleLdapIDSRealm**

Primary administrative user name: *smadmin*
Select both options: 'Ignore case for authorization' and 'Allow operations if some of the repositories are down'



NOI: Event Search feature

LDAP configuration – configure DASH / WAS



2. **Add a new repository, type LDAP and enter the AD details: host, port, bind credentials**

Global security > **Federated repositories** > **LDAP1**

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

Repository identifier

LDAP1

Repository adapter class name

com.ibm.ws.wim.adapter.ldap.LdapAdapter

LDAP server

Directory type

Microsoft Windows Active Directory

Primary host name

[redacted]

Port

389

Failover server used when primary is not available:

Security

Bind distinguished name

CN=smadminad,CN=Users,DC=eurolabs,DC=ibm,DC=com

Bind password

•••••••

Federated repository properties for login

uid

LDAP configuration – Configure DASH/LA to use SSO

1. Log on the WebSphere administrative console– https://dash_jazzsm:16316/ibm/console
2. go to Security -> Global Security -> Web and SIP security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security poli
default security policy for user applications. Security domains can be defined to override and customize the security policies for user applic

Security Configuration Wizard | Security Configuration Report

Administrative security

- [x] Enable administrative security
  - Administrative user roles
  - Administrative group roles
  - Administrative authentication

Application security

- [x] Enable application security

Java 2 security

- [ ] Use Java 2 security to restrict application access to local resources
  - [ ] Warn if applications are granted custom permissions
  - [ ] Restrict access to resource authentication data

User account repository

Authentication

Authentication mechanisms and expiration

- (•) LTPA
- ( ) Kerberos and LTPA
  - Kerberos configuration
- ( ) SWAM (deprecated): No authenticated communic

Authentication cache settings

Web and SIP security

- General settings
- Single sign-on (SSO)
- SPNEGO web authentication
- Trust association
- SIP digest authentication

LDAP configuration – Configure DASH/LA to use SSO

3. Insert the domain name, cookie name, and enable SSO, then save the changes

Global security

Global security > Single sign-on (SSO)

Specifies the configuration values for single sign-on.

General Properties

- [x] Enabled
- [ ] Requires SSL

Domain name
.ro.eurolabs.ibm.com

- [ ] Interoperability mode

LTPA V1 cookie name

LTPA V2 cookie name
LtpaToken2

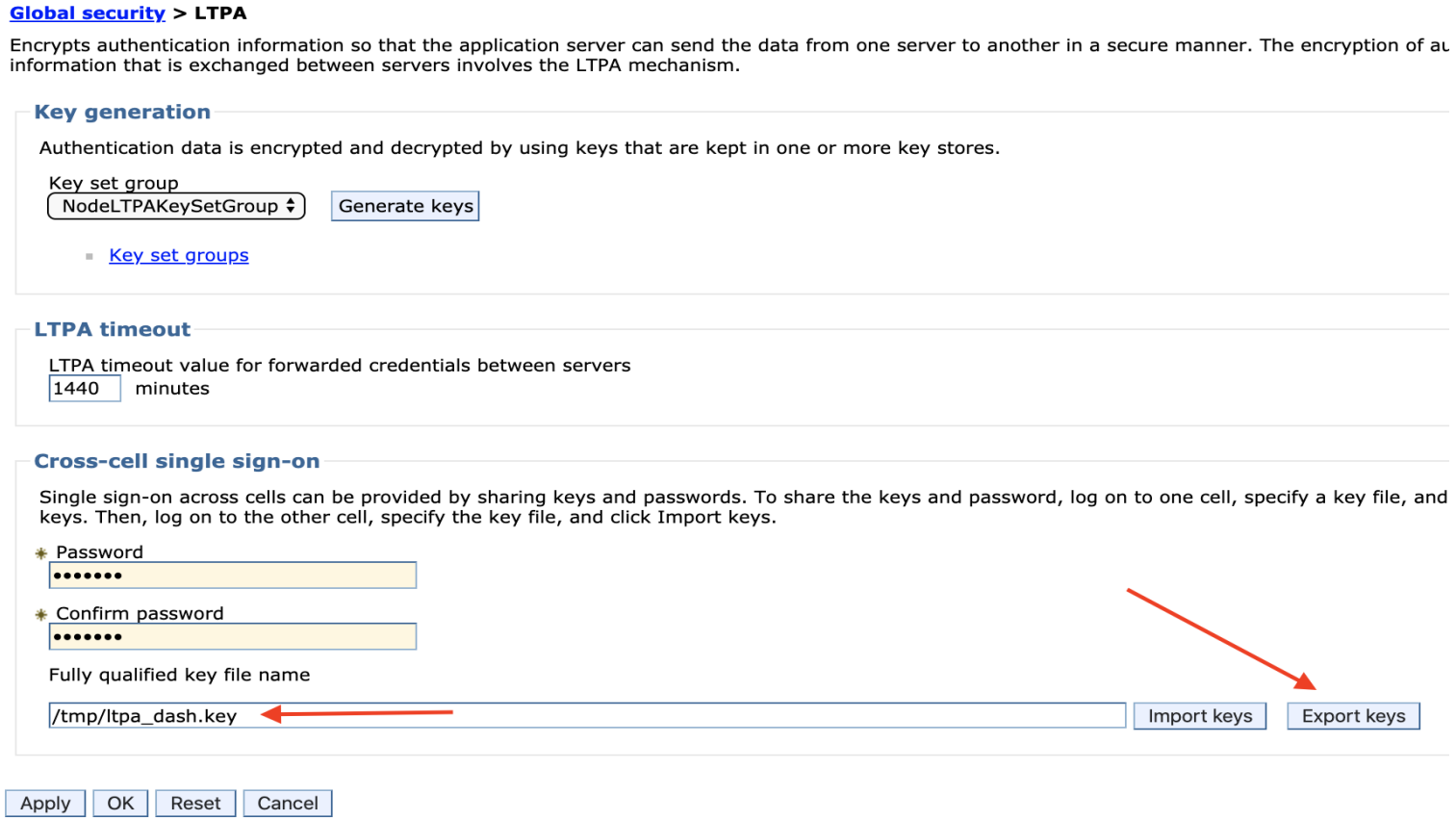
- [x] Web inbound security attribute propagation
- [ ] Set security cookies to HTTPOnly to help prevent cross-site scripting attacks

Apply OK Reset Cancel

LDAP configuration – Configure DASH/LA to use SSO

4. Export the DASH LTPA key:

From the WebSphere administrative console– https://dash_jazzsm:16316/ibm/console
Security -> Global Security



LDAP configuration – Configure DASH/LA to use SSO

- Copy the LTPA key file (ltpa_dash.key) exported from JazzSM

/tmp/ltpa_dash.keys

<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/resources/security

- Generate the encrypted text for the password needed to access the *ltpa_dash.key* file

$ cd <HOME>/IBM/LogAnalysis/wlp/bin
./securityUtility encode ltpapassword
{xor}MysvPi8+LCwoMC07

- Add the sso details into the server.xml. Make a backup first. You will need to add the below links between the </oauthProvider> and </server tags>

<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/server.xml

eg

```
</oauthProvider>
<webAppSecurity ssoDomainNames=".ro.eurolabs.ibm.com" />
<ltpa keysFileName="${server.output.dir}/resources/security/ltpa_dash.keys" keysPassword="{xor}MysvPi8+LCwoMC07" expiration="1440" />
                </server>
```

- Restart Unity

<HOME>/IBM/LogAnalysis/utilities/unity.sh -restart

LDAP configuration – Troubleshooting :: logging

Log files

<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/logs

- **messages.log**
- **console.log**

Log collection tool

<HOME>/IBM/LogAnalysis/utilities/collect_logs

Common LDAP errors to look out for:

***CWIML4529E**: The login operation could not be completed. The password verification for the unityadmin principal name failed. Root cause: javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]; resolved object com.sun.jndi.ldap.LdapCtx@810c9eea. Specify the principal name and the password correctly and check that the account is enabled and not locked.*

***CWWKS9104A**: Authorization failed for user CN=SVC-UNITYADMIN-BIZ,OU=Service Users,OU=PROD,OU=NetCool,OU=Applications,OU=Data Center EMEA,OU=IBM Service,OU=EMEA Region,OU=IBM Group,DC=biz,DC=IBM,DC=com while invoking Unity on /. The user is not granted access to any of the required roles: [**UnityUser**, **UnityAdmin**]*

***CWIML0515E**: The user registry operation could not be completed. The uid=smadmin,o=defaultWIMFileBasedRealm entity is not in the scope of the defined realm. Specify an entity that is in the scope of the configured realm in the server.xml file. com.ibm.ws.security.authentication.jaas.modules.TokenLoginModule 84" at ffdc_19.11.22_12.49.27.0.log*

LDAP configuration – Troubleshooting :: tracing

Add tracing to capture LDAP messages

/home/netcool/IBM/LogAnalysis/wlp/usr/servers/Unity/server.xml

```
</oauthProvider>

    <logging
    traceSpecification="com.ibm.ws.security.*=all:com.ibm.ws.webcontainer.security.*=all"
    traceFileName="trace.log"
    maxFileSize="20"
    maxFiles="10"
    traceFormat="BASIC"
    />

<webAppSecurity ssoDomainNames=".ro.eurolabs.ibm.com" />
```

<HOME>/IBM/LogAnalysis/wlp/usr/servers/Unity/logs

messages.log
console.log
trace.log

LDAP configuration – Troubleshooting :: diags

- use `**ldapsearch**`, if not installed:

*$ yum install openldap**

- to troubleshoot server authentication binding or directory tree / group membership:

$ ldapsearch -h Hostname -p <port> -D 'LDAPBindDN' -W

TechNotes on `ldapsearch`:

https://www.ibm.com/support/pages/using-ldapsearch-test-tivoli-netcoolomnibus-ldap-connection

https://www.ibm.com/support/pages/using-ldapsearch-debug-ldap-configuration-problems

NOI: Event Search feature

Omnibus and Log Analysis integration

A. Object server configuration

B. Configure the SSL connection for XML Gateway

C. Netcool XML Gateway configuration

D. Log Analysis configuration - datasource

E. Troubleshooting

F. Extending Omnibus Insight pack

G. Updating a custom insight pack

NOI: Event Search feature

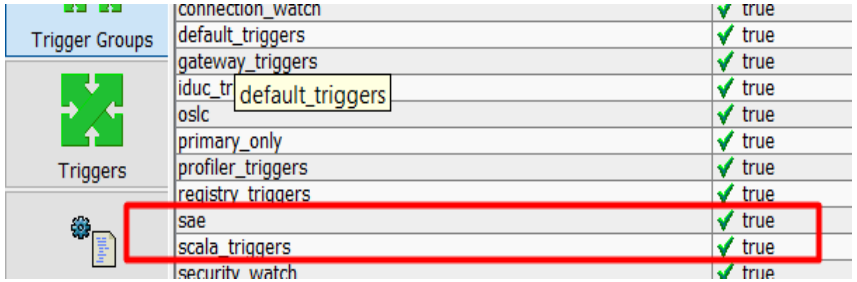
Omnibus and Log Analysis integration

A. Object server configuration

- **From GUI :**

$OMNIHOME/bin/nco_config

or open the Administrator from a remote client install

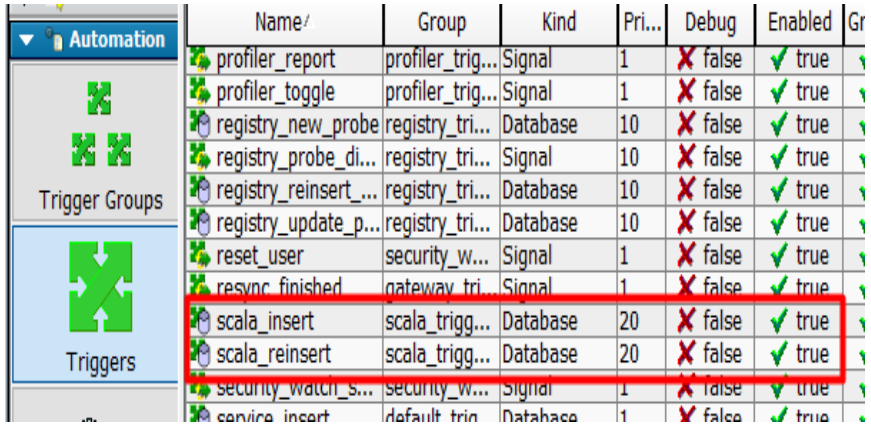


Enable the Omnibus triggers:

scala_triggers (group) & scala_reinsert, scala_insert

- **Fom command line:**

```
$OMNIHOME/bin/nco_sql –server NCOMS –user root –password my4pass
alter trigger scala_insert set enabled true;
alter trigger scala_reinsert set enabled true;
alter trigger group scala_triggers set enabled true;
go
```



NOI: Event Search feature

Omnibus and Log Analysis integration

B. Configure the SSL connection

Create the structure where the client and trust store will be located

```
mkdir /opt/IBM/tivoli/netcool/omnibus/java/security
```

Create a client keystore

```
/opt/IBM/tivoli/netcool/platform/linux2x86/jre_1.8.0/jre/bin
./keytool -genkey -alias omnibus -keystore
  /opt/IBM/tivoli/netcool/omnibus/java/security/client.jks
Enter keystore password: mykeypass
Re-enter new password: mykeypass
What is your first and last name?
[Unknown]: Test
…….
Enter key password for <omnibus>: mykeypass
(RETURN if same as keystore password):
```

NOTE :

Enter the same password at the beginning and at the end. If you press Enter, at the end, it will set the default password which is 'changeit' and this will cause the below error during the gateway flush

Unexpected communication failure to data collector 'https://LAhost.ibm.com:9987/Unity/DataCollector' detected. Exception Msg = [java.security.NoSuchAlgorithmException: Error constructing implementation (algorithm: Default, provider: IBMJSSE2, class: com.ibm.jsse2.aj)], Exception Type = [java.net.SocketException]

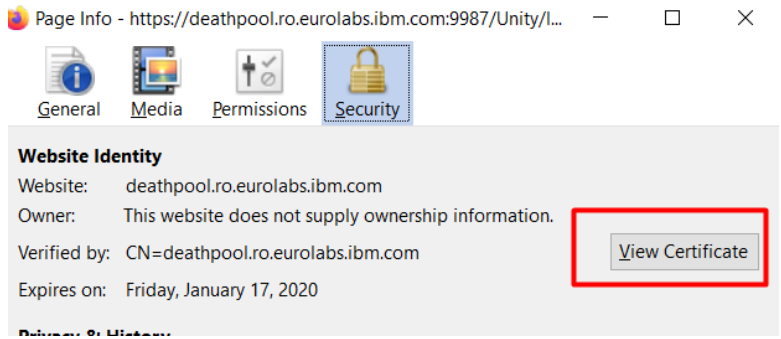
NOI: Event Search feature

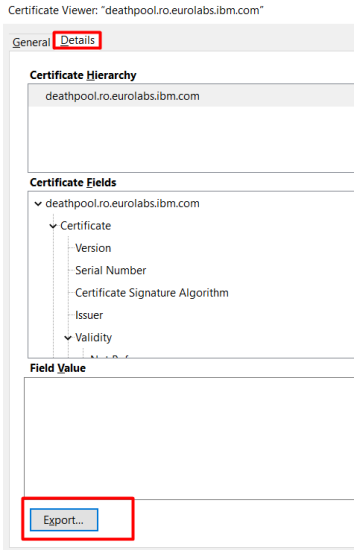
Omnibus and Log Analysis integration

B. Configure the SSL connection

Open a browser and go to : https://LAhost.ibm.com:9987/Unity/DataCollector ; click the padlock and click More Information

Export the server certificate from the host where the Log Analysis runs





Copy the certificate on the box where you have the Log Analysis installed

Import the certificate into the Omnibus truststore

```
/opt/IBM/tivoli/netcool/platform/linux2x86/jre_1.8.0/jre/bin
./keytool -import -keystore /opt/IBM/tivoli/netcool/omnibus/java/security/cacerts.jks -file
  /home/netcool/LAhost.crt -alias loganalysis
```

Output :

Enter keystore password mykeypass
Re-enter new password: mykeypass
.
Trust this certificate? [no]: yes
Certificate was added to keystore

NOI: Event Search feature

Omnibus and Log Analysis integration

C. Configure the XML gateway

The generic gateway configuration from the $OMNIHOME/gates/xml/scala/. A common practice is to copy them to OMNIHOME/etc location and rename them using the name of the gateway, in your case LA_GATE.

```
cd $OMNIHOME/gates/xml/scala/
cp xml1302.map $OMNIHOME/etc/LA_GATE.map
cp G_SCALA.props  $OMNIHOME/etc/LA_GATE.props
cp xml.reader.tblrep.def  $OMNIHOME/etc/LA_GATE.reader.tblrep.def
cp xml.startup.cmd $OMNIHOME/etc/LA_GATE.startup.cmd
cp scalaTransport.properties $OMNIHOME/java/conf
cp scalaTransformers.xml $OMNIHOME/java/conf
```

Update the LA_GATE.props file with

```
# SCALA configuration
MessageLog                          : '$OMNIHOME/log/LA_GATE.log'
Name                                : 'LA_GATE'
Gate.Reader.Description             : 'SCALA Gateway Reader'
Gate.Reader.Server                  : 'NCOMS'
Gate.Reader.TblReplicateDefFile     : '$OMNIHOME/etc/LA_GATE.reader.tblrep.def'
Gate.MapFile                        : '$OMNIHOME/etc/LA_GATE.map'
Gate.StartupCmdFile                 : '$OMNIHOME/etc/LA_GATE.startup.cmd'
Gate.XMLGateway.TransformerFile     : '$OMNIHOME/java/conf/scalaTransformers.xml'
Gate.XMLGateway.TransportFile       : '$OMNIHOME/java/conf/scalaTransport.properties'
Gate.XMLGateway.TransportType       : 'SCALA'
Gate.XMLGateway.DateFormat          : 'yyyy-MM-dd\'T\'HH:mm:ssZ'
```

Edit the LA_GATE.reader.tblrep.def'. Locate the following line:

REPLICATE INSERT, UPDATE FROM TABLE 'alerts.status'

And change it into

REPLICATE FT_INSERT,FT_UPDATE FROM TABLE 'alerts.status'

Note: INSERT/UPDATE vs FT_INSERT/FT_UPDATE ; The meaning of the FT is Fast Track, and it causes the gateway to immediately replicate the insert from source to destination without waiting for an IDUC cycle.

Configure scalaTransport.properties

```
scalaURL=https://deathpool.ro.eurolabs.ibm.com:9987/Unity/DataCollector
keyStore=/opt/IBM/tivoli/netcool/omnibus/java/security/client.jks
keyStorePassword=mykeypass
trustStore=/opt/IBM/tivoli/netcool/omnibus/java/security/cacerts.jks
trustStorePassword=mykeypass
username =unityadmin
password = ***********
jsonMsgPath = NCOMS
jsonMsgHostname = deathpool
```

Configure scalaTransformers.xml – set the Log Analysis URL

```
<tns:transformer name="netcoolEvents" type="northbound" endpoint="https://deathpool.ro.eurolabs.ibm.com:9987/Unity/DataCollector"
className="com.ibm.tivoli.netcool.integrations.transformer.XSLTThreadTransformer">
<tns:property name="xsltFilename" type="java.lang.String" value="$OMNIHOME/java/conf/netcool2scala.xsl" description="XSLT file for
converting Netcool events to Scala Data Collector CSV format."/>
```

NOI: Event Search feature

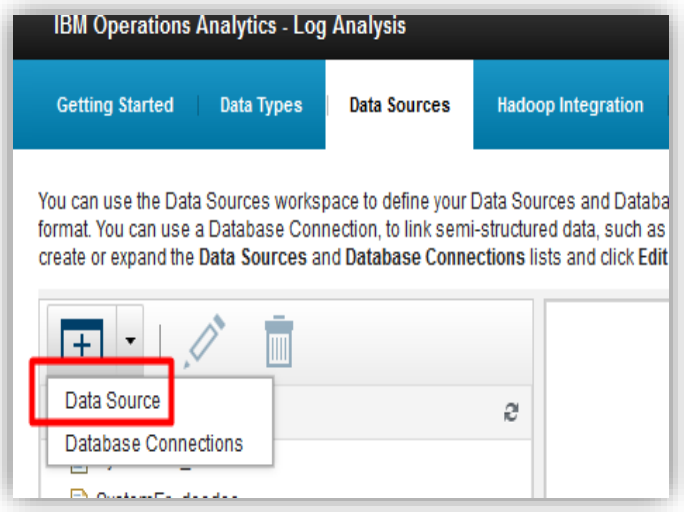
Omnibus and Log Analysis integration

D. Log Analysis configuration – Omnibus datasource

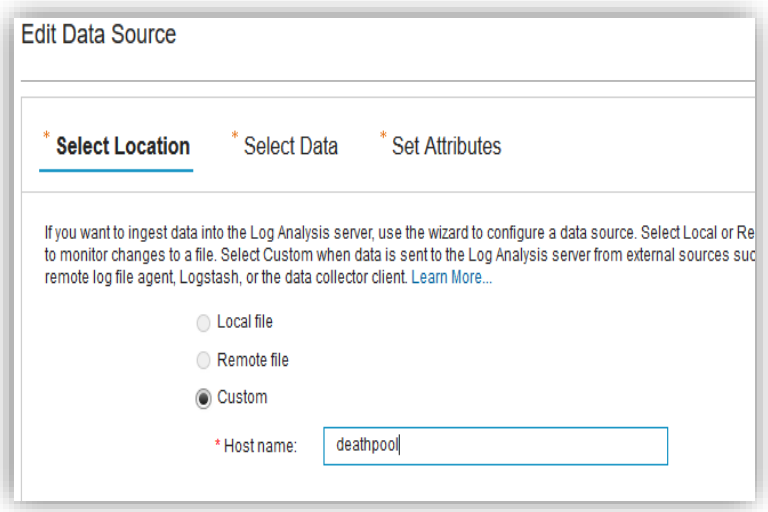
Connect to Log Analysis https://deathpool.ro.eurolabs.ibm.com:16311/ibm/console

Go to Administrative settings and click on the Data Sources tab

Create a new datasource



Select 'Custom and in the Host name field enter the same value as the one used in scalaTransport.properties, for the parameter jsonMsgHostname .

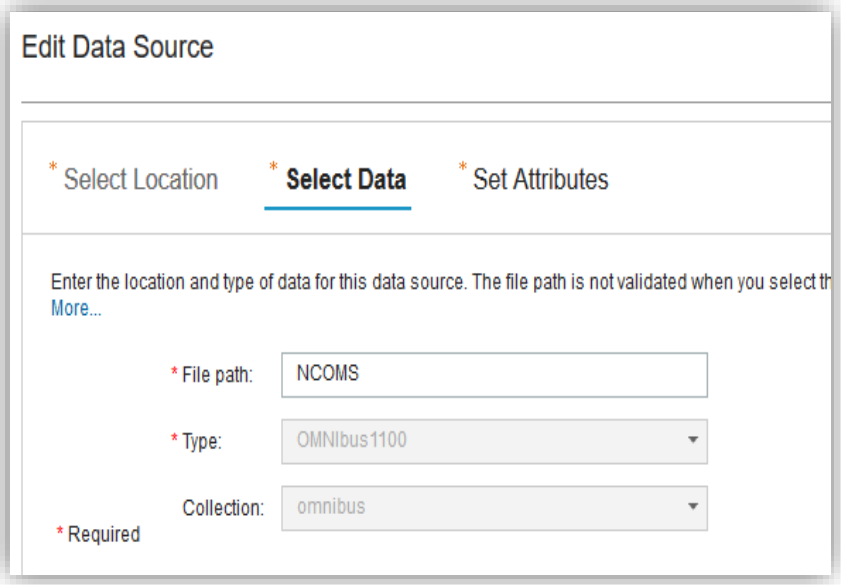


NOI: Event Search feature

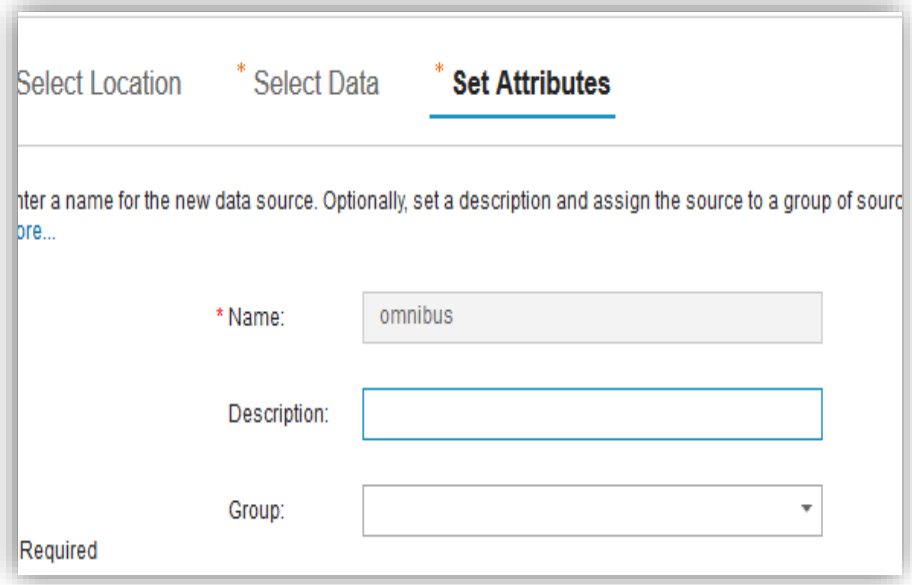
Omnibus and Log Analysis integration

D. Log Analysis configuration – Omnibus datasource

In the File path , enter the same value as the one used in **scalaTransport.properties**, for the parameter **jsonMsgPath** , for Type OMNIbus1100 and for the Collection - omnibus



Name : **omnibus** ; this is the default name of the datasource and its used for displaying data in the box of the box Omnibus Dashboards . You can use a different name for your datasource, but you will have to create new dashoards, or modify the default ones and set the new datasource name



NOI: Event Search feature

Omnibus and Log Analysis integration

E. Troubleshooting

Issues with the access to Log Analysis	2019-11-22T09:28:17: Error: E-GJA-000-000: [ngjava]: XMLGateway:[THREAD=29]: Unexpected communication failure to data collector 'https://localhost:9987/Unity/DataCollector' detected. Exception Msg = [java.security.NoSuchAlgorithmException: **SSLContextDefault implementation not found**:], Exception Type = [java.net.SocketException]
Incorrect map files being used	2019-11-22T08:20:23: Error: E-GOB-102-088: [ngobjserv]: Reader: **Failed to find column 'NmosObjInst'** that is specified in map 'StatusMap' for the source table 'alerts.status'. (0:No error)
Datasources not match or exist in Log Analysis	2013-09-06T12:22:42: Error: E-GJA-000-000: [ngjava]: XMLGateway: [THREAD=23]:Failed to send batch to data collector. HTTP response code != 200. [{responseCode:404 responseMessage:NotFound responseException:nullauthenticationRequired:falsecookieJar:nullresponseContent:{ "BATCH_STATUS":"NONE","RESPONSE_MESSAGE":"CTGLA0401E : **Missing data source** ","RESPONSE_CODE":404}
Issues with the GW key/truststores	2019-11-22T08:28:03: Error: E-GJA-000-000: [ngjava]: XMLGateway: [THREAD=49]: Unexpected communication failure to data collector 'https://localhost:9987/Unity/DataCollector' detected. Exception Msg = [java.security.NoSuchAlgorithmException: **Error constructing implementation** (algorithm: Default, provider: IBMJSSE2, class: com.ibm.jsse2.aj)], Exception Type = [java.net.SocketException]

NOI: Event Search feature

Omnibus and Log Analysis integration

F. Extending Omnibus insight pack

- ❑ Omnibus Insight pack version should be 1.3.1 and higher
- ❑ LA versions 1.3.3 and higher
- ❑ Create a custom dataSoureType

- ✓ edit the **LA_home/unity_content/OMNIbusINsightPack_v1.3.1/docs/omnibus1100_template.properties** and update with the new column names
- ✓ Update the “moduleName” to reflect the name of the new dataSourceType
- ✓ Update the “version” to show a new version number for the custom pack
- ✓ Run **LA_home unity_content/OMNIbusINsightPack_v1.3.1/docs/addIndex.sh –i**

This should have installed the new customer Omnibus Insight pack and the new dataSourceType

- ✓ Delete the old datasource and create a new datasource named “omnibus” as per previous instructions. Use the dataSourceType that was added to “moduleName”.
- ✓ Modify the XML GW mapping file to reflect the new custom columns

Omnibus1100.properties

```
[SCALA_server]
scalaHome: $HOME/IBM/LogAnalysis

[DSV_file]
delimiter: ,
moduleName: OMNIbus
version: 1.3.1.5

[field0_indexConfig]
name: logRecord
dataType: TEXT
retrievable: true
retrieveByDefault: true
sortable: false
....
[field18_indexConfig]
name: ServerSerial
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true
# ----------------------------------
#Insert new fields after this point.
# ----------------------------------
[field19_indexConfig]
name: newField
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true
```

LA_GATE.map section :

```
CREATE MAPPING StatusMap
(
      'LastOccurrence’  =    '@LastOccurrence' NOTNULL '',
      'Summary'         =   '@Summary' NOTNULL '',
      'NmosObjInst'     =   '@NmosObjInst',
      'Node'            =   '@Node',
      'NodeAlias'       =   '@NodeAlias' NOTNULL '@Node',
      'LastOccurrence’  =    '@LastOccurrence' NOTNULL '',
      'Severity'        =   Lookup('@Severity', 'SeverityLkTable'),
      'AlertGroup'      =   '@AlertGroup',
      'AlertKey'        =   '@AlertKey',
      'Identifier'      =   '@Identifier',
      'Location'        =   '@Location',
      'Type'            =   Lookup('@Type', 'TypeLkTable'),
      'Tally'           =   '@Tally',
      'Class'           =  Lookup('@Class', 'ClassLkTable'),
      'OmniText'        =  '@Manager' + ' ' + '@Agent',
      'ActionCode'      =  ACTION_CODE,
      'ServerName'      =   '@ServerName',
      'ServerSerial’    =   '@ServerSerial',
      'newField’        =    '@newField'

);
```

NOI: Event Search feature

G. Upgrading a customized insight pack

- The custom sourceType is only there to deal with the additional/custom fields that are being sent
- All other aspects of the Omnibus insight pack, such as dashboards, etc. are still being served from original insight pack
- If a new version of the Omnibus insight pack is released, the pkg_mgmt.sh tool should be used with the upgrade option to upgrade the regular pack
- If there are new columns/fields in the upgraded properties file, these fields could be added to the custom pack properties file and then upgraded by running the command "addIndex.sh -u" to update the custom pack
- For example, if the updated Omnibus insight pack had new fields X,Y and Z , you would add those fields to the custom pack properties file, then increment the version in this file , and run "addIndex.sh -u".

NOI: Event Search feature

H. Log Analysis – Best Practices

- Retain no more than 30-60 days worth of data in LA
- Reports for long term data (more than 60 days) should be ideally run from the Reporter database (not LA)
- If long term data is still needed, the LA/Hadoop integration should be implemented
- All LA related configuration should be completed after LA has been integrated with LDAP

NOI: Event Search feature

References:

Install NOI
https://www.ibm.com/support/knowledgecenter/SSTPTP_1.6.0/com.ibm.netcool_ops.doc/soc/integration/task/soc_int_installingbaseonpremises.html

Custom insight pack
https://www.ibm.com/support/knowledgecenter/SSTPTP_1.5.0/com.ibm.netcool_ops.doc/soc/ipack/task/ip_updating-custom-datasource-type.html

XML GW Configuration
https://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/xmlintegration/wip/concept/xmlgw_config_scala.html
https://www.ibm.com/support/knowledgecenter/en/SSSHTQ/omnibus/gateways/xmlintegration/wip/reference/xmlgw_config_sslloganalyzer.html

Configuring Event Search
https://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/xmlintegration/wip/concept/xmlgw_config_scala.html

LDAP & SSO
https://www.ibm.com/support/pages/using-ldapsearch-test-tivoli-netcoolomnibus-ldap-connection
https://www.ibm.com/support/pages/using-ldapsearch-debug-ldap-configuration-problems

Prerequisites
https://www.ibm.com/support/knowledgecenter/en/SSPFMY_1.3.5/com.ibm.scala.doc/install/iwa_prerequisites.html

Configuring the Hadoop Integration for Log Analysis
https://www.ibm.com/support/knowledgecenter/SSPFMY_1.3.5/com.ibm.scala.doc/config/iwa_config_hadoop_ovw_c.h

Q&A

Thank You!