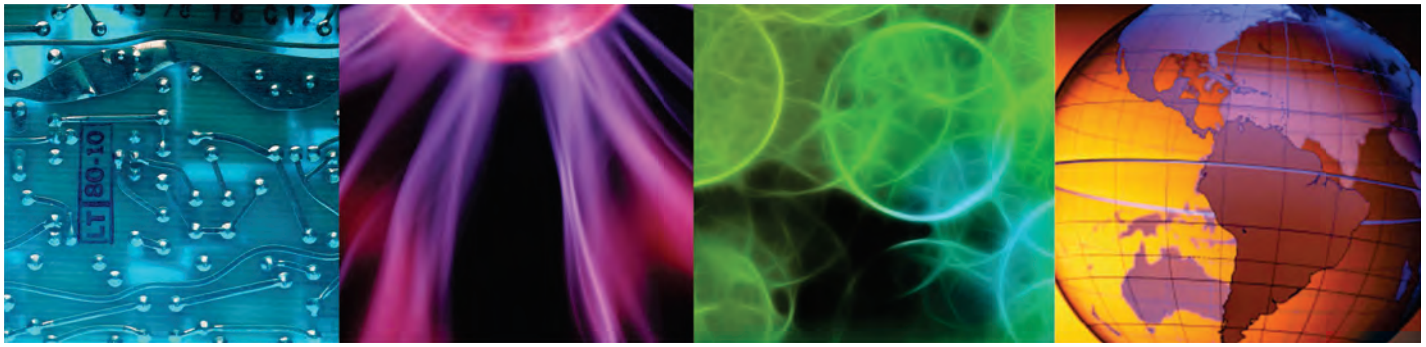
IBM Training

IBM Operations Analytics Log Analysis 1.3 Administration

Student Exercises

Course code TN630G ERC 1.0

April 2016



ibm.com/training

Authorized IBM Training

All files and material for this course are IBM copyright property covered by the following copyright notice.

© Copyright IBM Corp. 2016. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results.

Contents

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

About these exercises

These exercises use two virtual machine images for the lab environment:

host2: This virtual machine runs the IBM® Operations Analytics Log Analysis application. The host name is **host2.tivoli.edu**. The IP address is **192.168.100.161**.

bivm: This virtual machine runs the IBM InfoSphere® BigInsights® software. The host name is **bivm.ibm.com**. The IP address is **192.168.100.166**.

host image details (host2.tivoli.edu)

The following table describes the user names and passwords that are used with the **host2.tivoli.edu** virtual machine (host2).

User name	Password	Description
netcool	object00	Operating system user
root	object00	Operating system super user
unityadmin	unityadmin	Operations Analytics Log Analysis super user
unityuser	unityuser	Operations Analytics Log Analysis user

Python version 2.6.6 is installed on this host. Use the following command to verify the Python version:

```
python -V
```

host image details (bivm.ibm.com)

The following table describes the user names and passwords that are used with the **bivm.ibm.com** virtual machine.

User name	Password	Description
biadmin	object00	Operating system user
root	object00	Operating system super user
biadmin	object00	InfoSphere BigInsights user

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

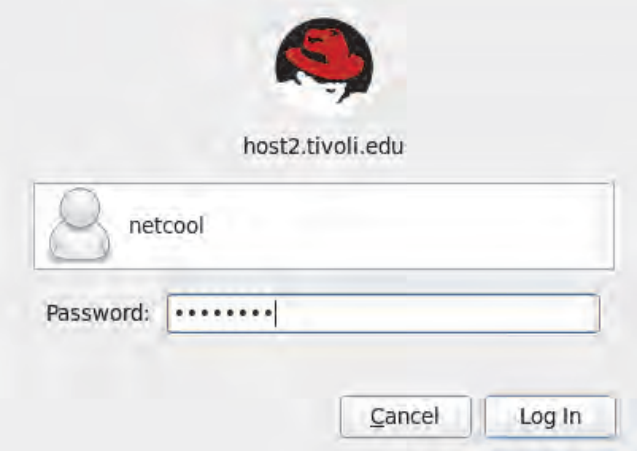
1 Overview and basic administration exercises

In these exercises, you perform basic administration tasks, including application management, user management, and data storage housekeeping.

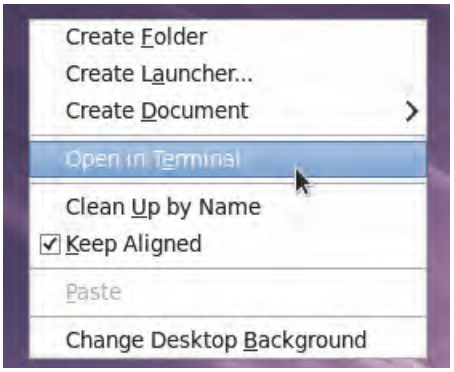
Exercise 1 Managing the application and users

In this exercise, you start and stop the application and add users.

1. Log in to the host2 virtual machine (host2.tivoli.edu) with the user name **netcool** and the password **object00**.



2. Right-click the desktop and select **Open In Terminal**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

3. Use the following command to verify that you are logged in to the correct host:

```
hostname
host2.tivoli.edu
```

4. Run the following command to verify that IBM Operations Analytics Log Analysis is running.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -status
```

5. Stop all IBM Operations Analytics Log Analysis components. Verify that they are stopped. Use the following commands.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -stop

/opt/IBM/LogAnalysis/utilities/unity.sh -status
Mon Apr  6 15:41:08 UTC 2016
IBM Operations Analytics - Log Analysis v1.3.0.0 Application Services Status:
---------------------------------------------------
No.  Service                    Status   Process ID
---------------------------------------------------
1    Derby Network Server       DOWN
2    ZooKeeper                  DOWN
3    Websphere Liberty Profile  DOWN
4    EIF Receiver               DOWN
5    Log File Agent instance    DOWN
---------------------------------------------------
Getting status of Solr on host2.tivoli.edu
Status of Solr Nodes:
----------------------------------------------------------------
No. Instance Name            Host              Status  State
----------------------------------------------------------------
1   SOLR_NODE_LOCAL          host2.tivoli.edu  DOWN    ACTIVE
----------------------------------------------------------------
All Application Services are in Stopped State
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6. Start the IBM Operations Analytics Log Analysis components. Verify that they are running. Use the following commands.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -start

/opt/IBM/LogAnalysis/utilities/unity.sh -status
Mon Apr  6 15:46:13 UTC 2015
IBM Operations Analytics - Log Analysis v1.3.0.0 Application Services Status:
---------------------------------------------------
No.  Service                    Status   Process ID
---------------------------------------------------
1    Derby Network Server       UP       8432
2    ZooKeeper                  UP       8476
3    Websphere Liberty Profile  UP       8638
4    EIF Receiver               UP       8810
5    Log File Agent instance    UP       9057
---------------------------------------------------
Getting status of Solr on host2.tivoli.edu
Status of Solr Nodes:
-----------------------------------------------------------------
No. Instance Name           Host              Status  State
-----------------------------------------------------------------
1   SOLR_NODE_LOCAL         host2.tivoli.edu  UP      ACTIVE
-----------------------------------------------------------------
All Application Services are in Running State
Checking server initialization status: Server has initialized!
```

7. Use the `unity.sh` utility again to show product version information. Run the following command.

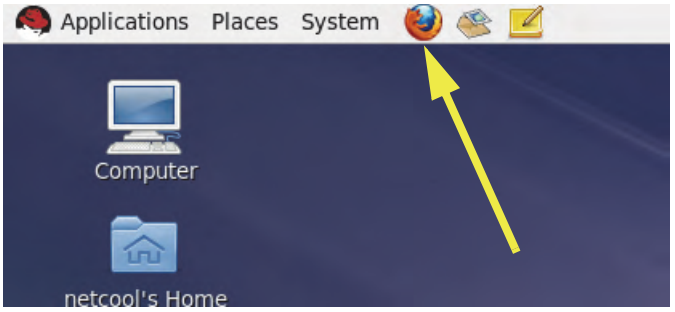
```
/opt/IBM/LogAnalysis/utilities/unity.sh -version

Product: IBM Operations Analytics - Log Analysis
Version: 1
Release: 3
Modification: 0
Fix pack: 0
Build Id: 201503090631
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

8. Verify that you can log in to the IBM Operations Analytics Log Analysis user interface. Use the user name **unityadmin** and the password **unityadmin**.
   a. Double-click the **Firefox** icon on the desktop.



   b. Browse to the following address.

      `https://host2.tivoli.edu:9987/Unity`

   c. Log in to the user interface with the user name **unityadmin** and the password **unityadmin**. This action verifies that the user interface is running. Log out when you finish.

You add users to IBM Operations Analytics Log Analysis by editing the basic user registry file. This file is named `unityUserRegistry.xml`. Passwords in this file are encoded.

9. Edit the basic user registry file and add the following two users. Make the password for both users **object00**.
   - **admin**: Add this user to the UnityAdmins and the UnityUsers groups.
   - **loguser**: Add this user to the UnityUsers group.

   a. Use the following commands to encode the password **object00**. The output of the command is the encoded version of the password. Record the encoded password.

```
cd /opt/IBM/LogAnalysis/wlp/bin
./securityUtility encode object00
{xor}MD01Ojwrb28=
```

   b. Open the `unityUserRegistry.xml` file in a text editor. This example uses `vi`.

```
cd /opt/IBM/LogAnalysis/wlp/usr/servers/Unity
vi unityUserRegistry.xml
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Add the following five lines to the file. Make the `unityUserRegistry.xml` file look like the following example.

```
<server>
  <basicRegistry id="basic" realm="UnityRealm">
     <user name="unityuser" password="{xor}KjE2KyYqLDot" />
     <user name="unityadmin" password="{xor}KjE2KyY+OzI2MQ==" />
     <user name="admin" password="{xor}MD01Ojwrb28=" />
     <user name="loguser" password="{xor}MD01Ojwrb28=" />
     <group name="UnityUsers">
         <member name="unityuser" />
         <member name="unityadmin" />
         <member name="admin" />
         <member name="loguser" />
     </group>
     <group name="UnityAdmins">
         <member name="unityadmin" />
         <member name="admin" />
     </group>
  </basicRegistry>
</server
```

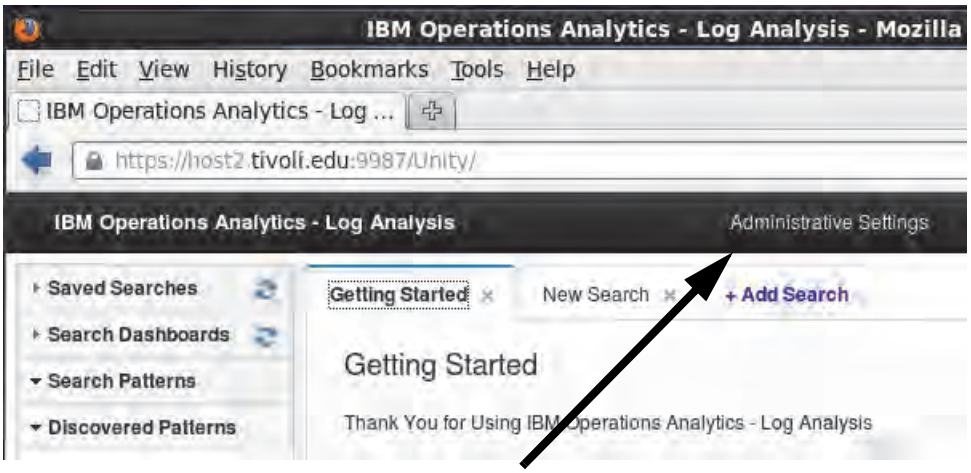
```
<server>
  <basicRegistry id="basic" realm="UnityRealm">
     <user name="unityuser" password="{xor}KjE2KyYqLDot" />
     <user name="unityadmin" password="{xor}KjE2KyY+OzI2MQ==" />
     <user name="admin" password="{xor}MD01Ojwrb28=" />
     <user name="loguser" password="{xor}MD01Ojwrb28=" />
     <group name="UnityUsers">
         <member name="unityuser" />
         <member name="unityadmin" />
         <member name="admin" />
         <member name="loguser" />
     </group>
     <group name="UnityAdmins">
         <member name="unityadmin" />
         <member name="admin" />
     </group>
  </basicRegistry>
</server>
~
```

d. Save and exit the file after you finish editing it.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

10. Test the new users.
    a. Open a Firefox browser and browse to `https://host2.tivoli.edu:9987/Unity`. Log in to the user interface with the user name **admin** and the password **object00**.
    b. Verify that there is an **Administrative Settings** link in the user interface, which means that the **admin** user has administrative privileges. Log out of the user interface.



    c. Log back in to the user interface with the user name **loguser** and the password **object00**. Notice that **loguser** does not have a link to the Administrative Settings page.
    d. Log out of the user interface.

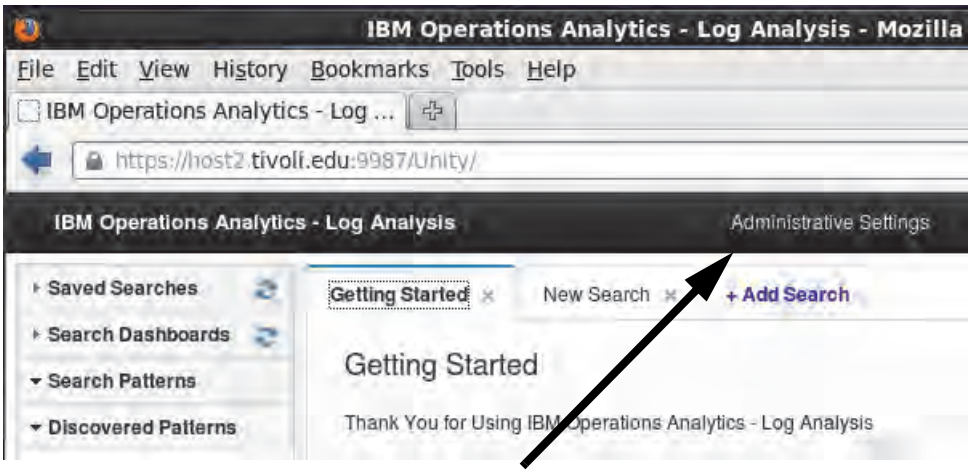
Exercise 2 Adding data sources

In this exercise, you add some data sources and view log data in the user interface.

1. Open the administration user interface.
    a. Double-click the **Firefox** icon on the desktop.
    b. Browse to the following address.
    `https://host2.tivoli.edu:9987/Unity`
    c. Log in to the user interface with the user name **unityadmin** and the password **unityadmin**.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Click **Administrative Settings**. The administration user interface opens in a new Firefox tab.



Adding a WebSphere SystemOut data source

A ***data source*** is a reference to a log file.

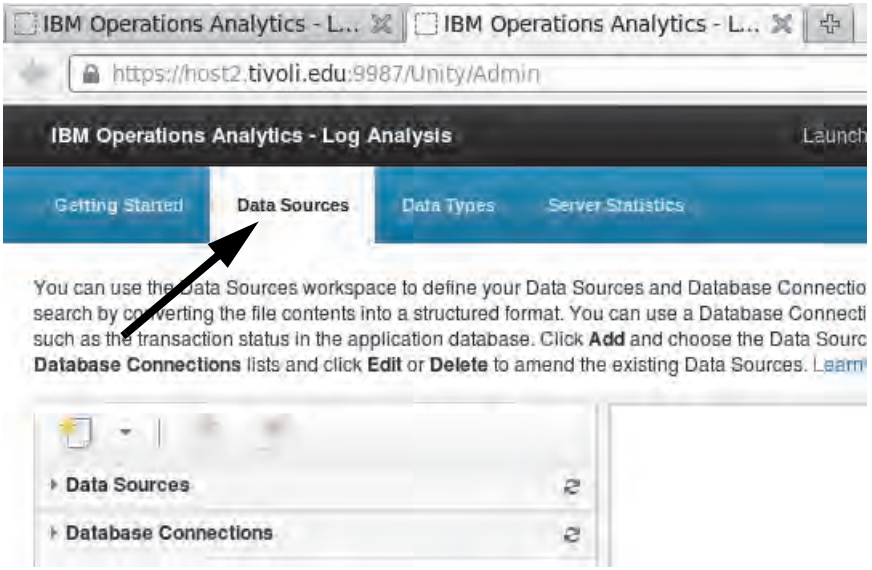
2. Create a data source named **WAS_SystemOut**. Use the values in the following table to complete the data source wizard.

Field	Value
Location	Select Local file
Host name	host2.tivoli.edu
File Path	`/software/log_samples/WAS_logs/SystemOut.log`
Type	WASSystemOut
Collection	Leave this field blank
Name	WAS_SystemOut
Description	This source uses WAS SystemOut logs
Group	Leave this field blank

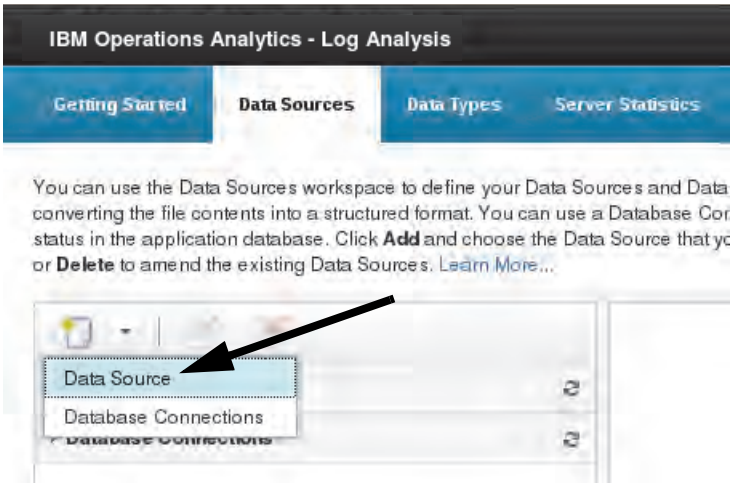
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

a. Click the **Data Sources** tab in the administration user interface. The administration user interface is in the second Firefox tab.

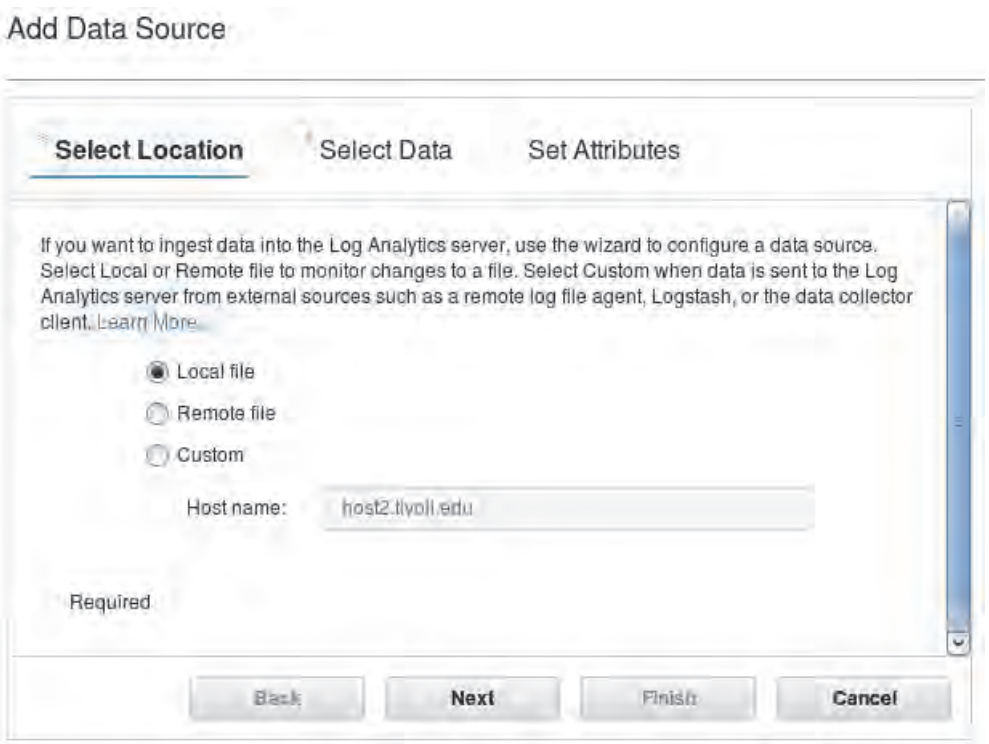


b. Click **Add > Data Source**.

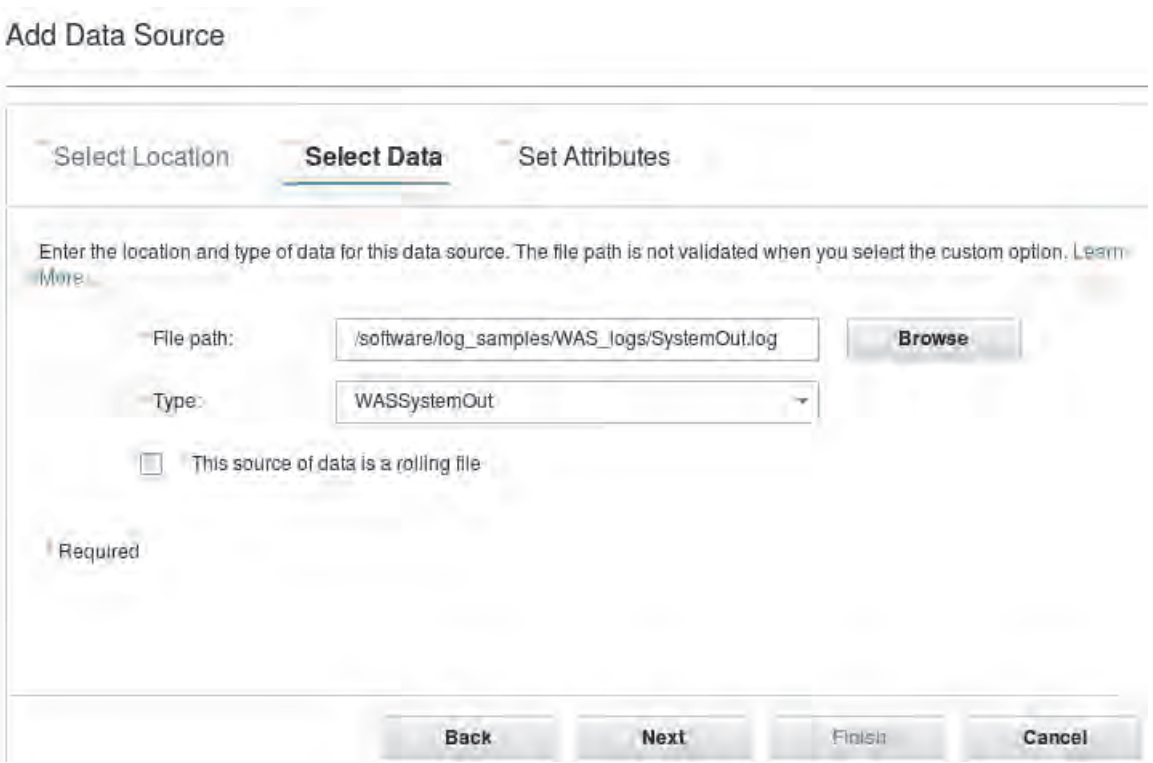


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Select **Local file**. Click **Next**.

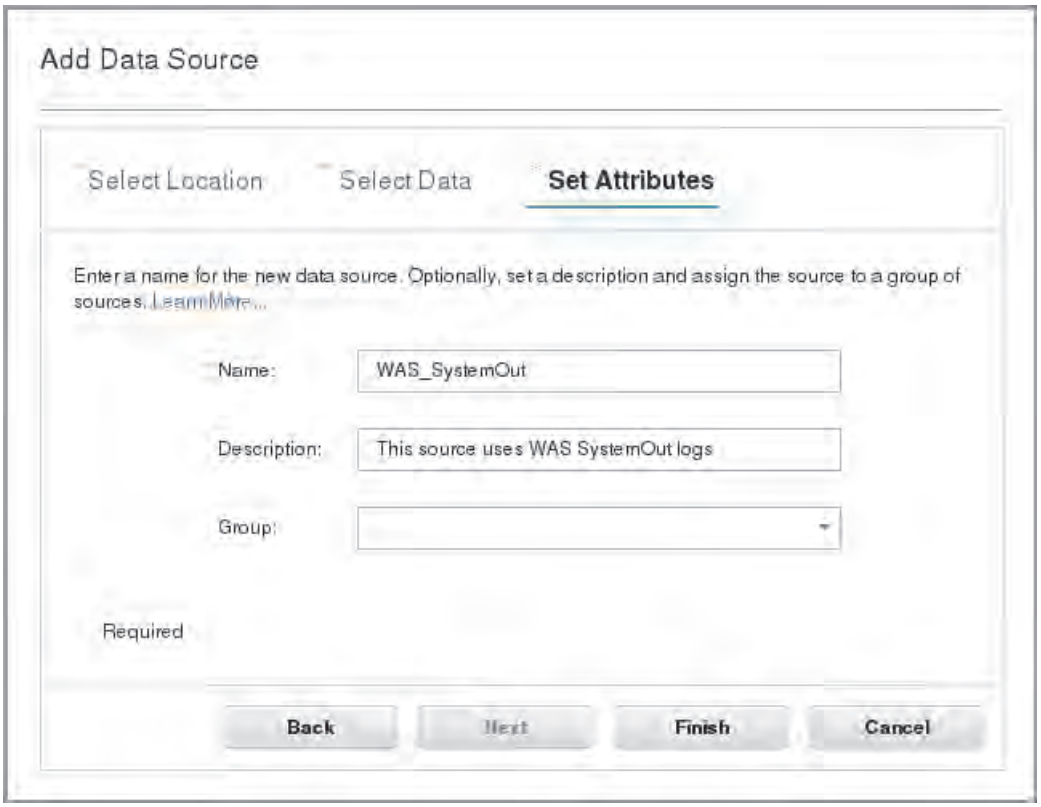


d. Enter `/software/log_samples/WAS_logs/SystemOut.log` as the file path. Select **WASSystemOut** as the type. Click **Next**.

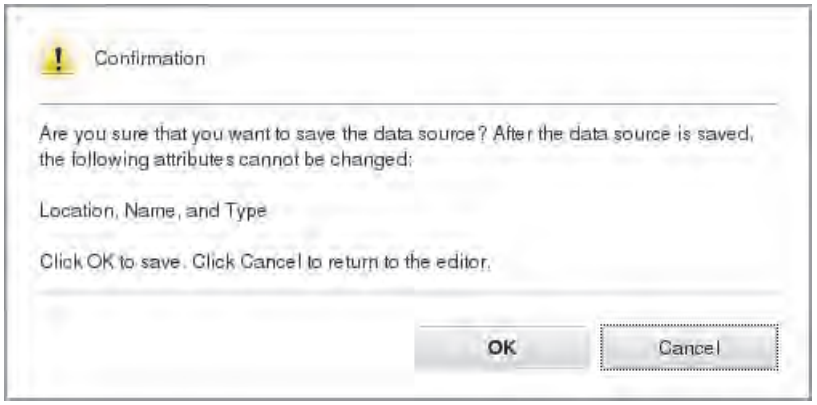


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Enter **WAS_SystemOut** as the name of the data source. Use the description from the preceding table. Click **Finish**.



f. Click **OK** in the confirmation windows.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Adding a WebSphere SystemErr Data source

3. Create a data source named **WAS_SystemErr**. Use the values in the following table to complete the data source wizard.

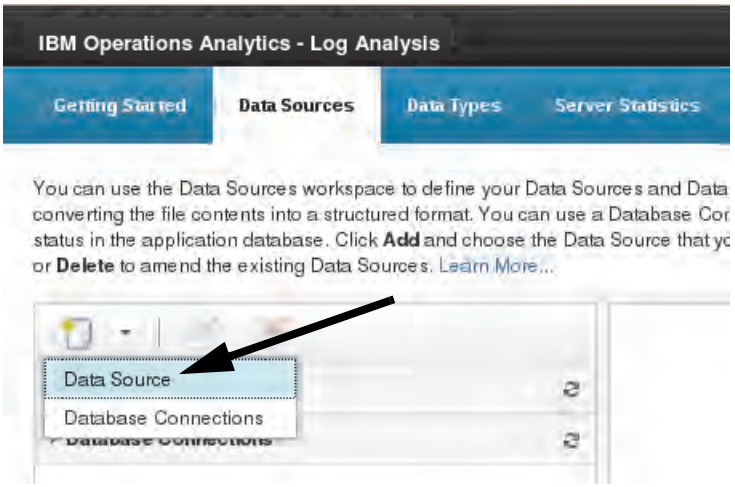
Field	Value
Location	Select Local file
Host name	host2.tivoli.edu
File Path	`/software/log_samples/WAS_logs/SystemErr.log`
Type	WASSystemErr
Collection	Leave this field blank
Name	WAS_SystemErr
Description	This source uses WAS SystemErr logs
Group	Leave this field blank

© Copyright IBM Corp. 2016

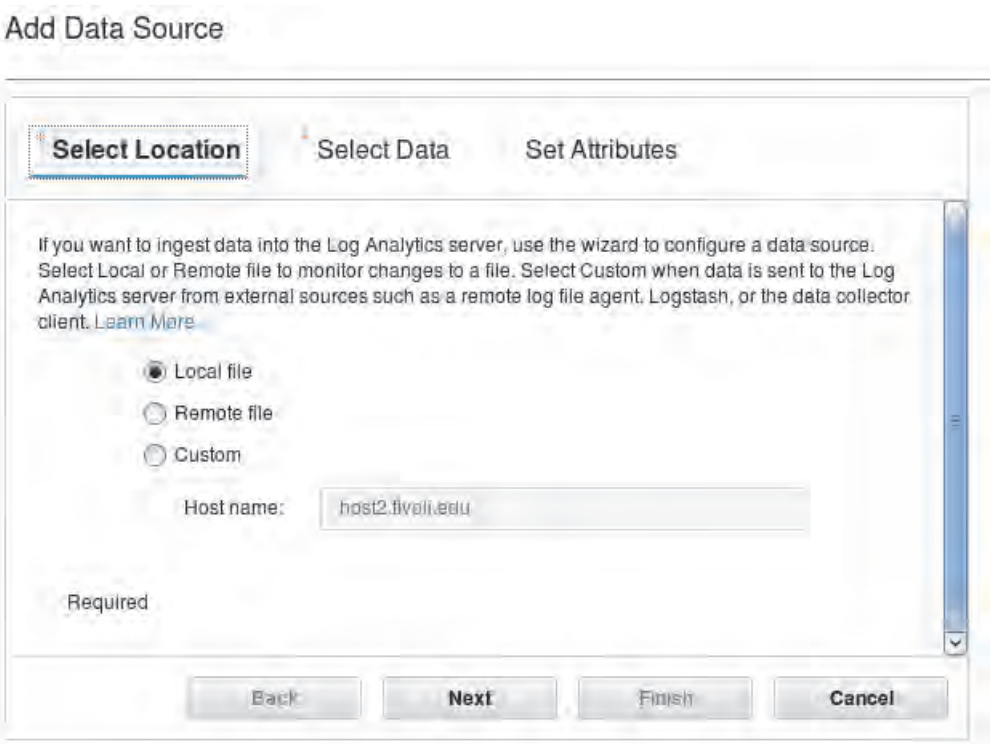
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

a. Click the **Data Sources** tab in the administration user interface. The administration user interface is in the second Firefox tab.

b. Click **Add > Data Source**.

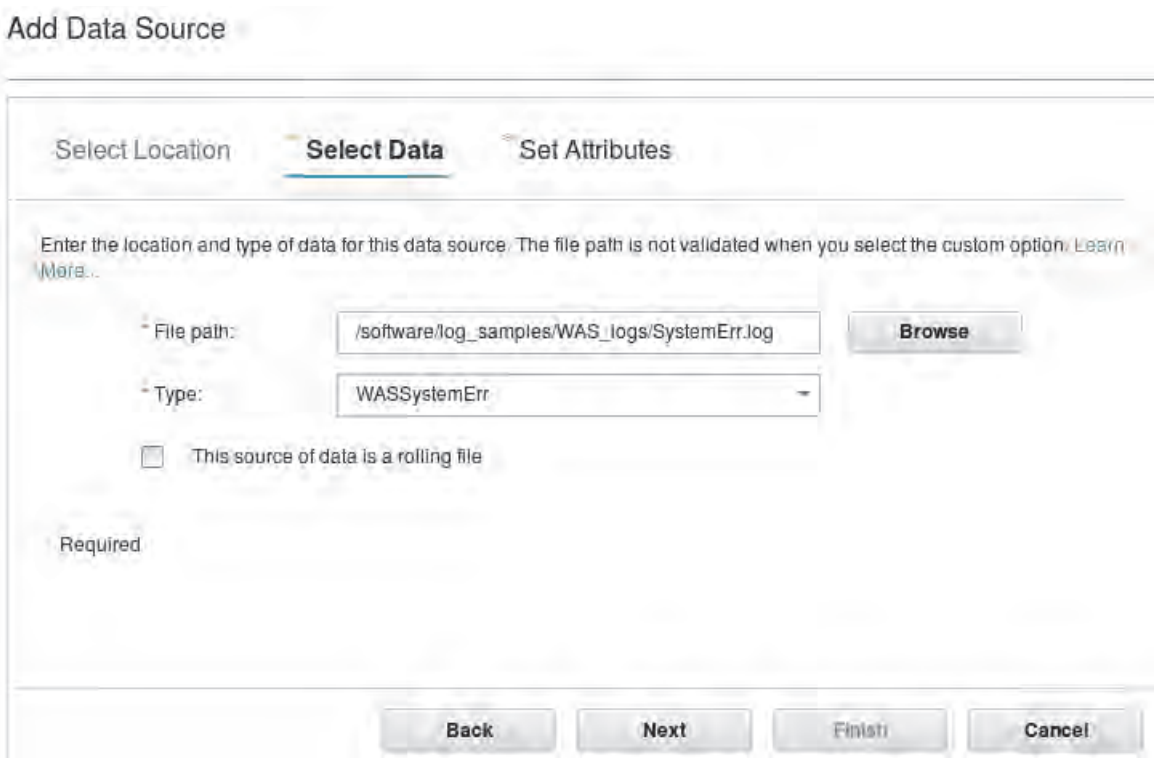


c. Select **Local file**. Click **Next**.

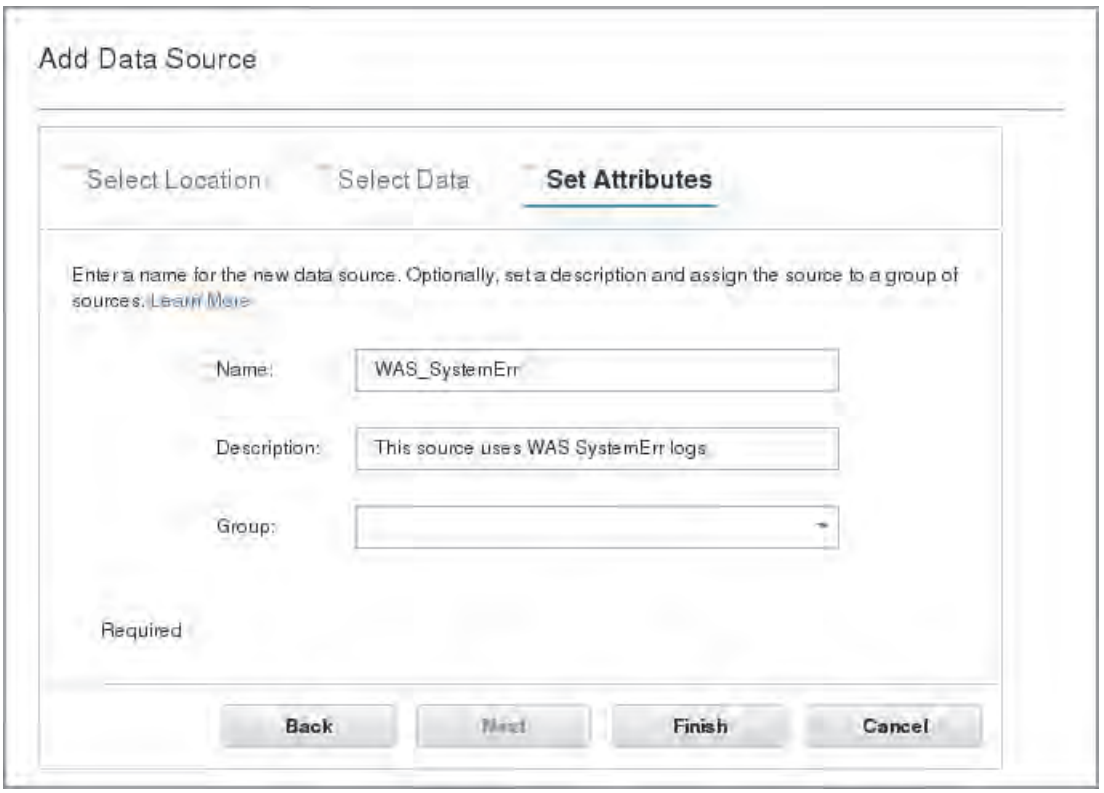


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Enter `/software/log_samples/WAS_logs/SystemErr.log` as the file path. Select **WASSystemErr** as the Type. Click **Next**.



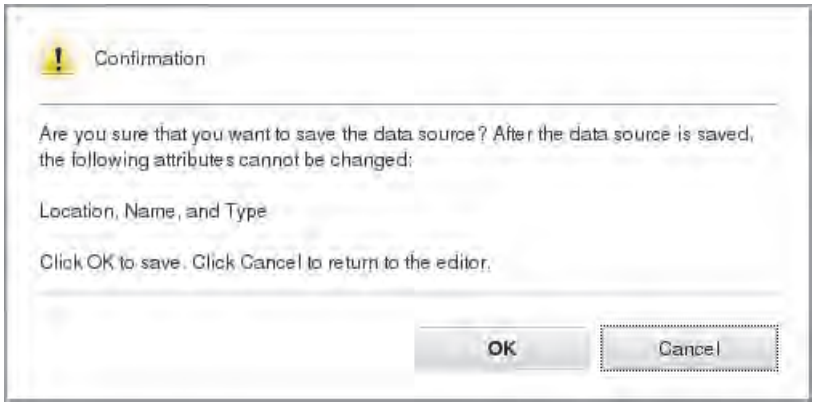
e. Enter **WAS_SystemErr** as the name of the data source. Use the description from the preceding table. Click **Finish**.

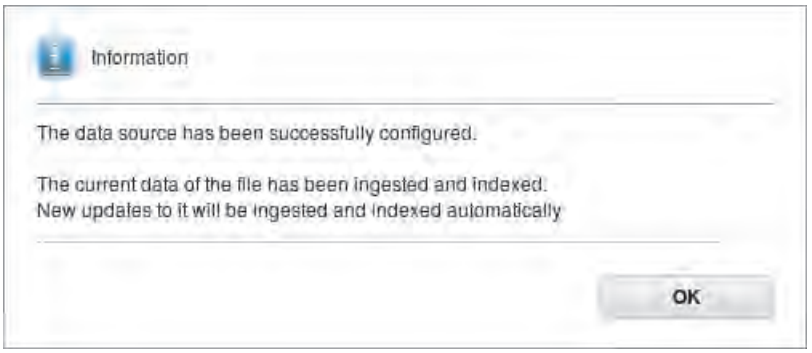


© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

f. Click **OK** in the confirmation windows.





Adding a web access data source

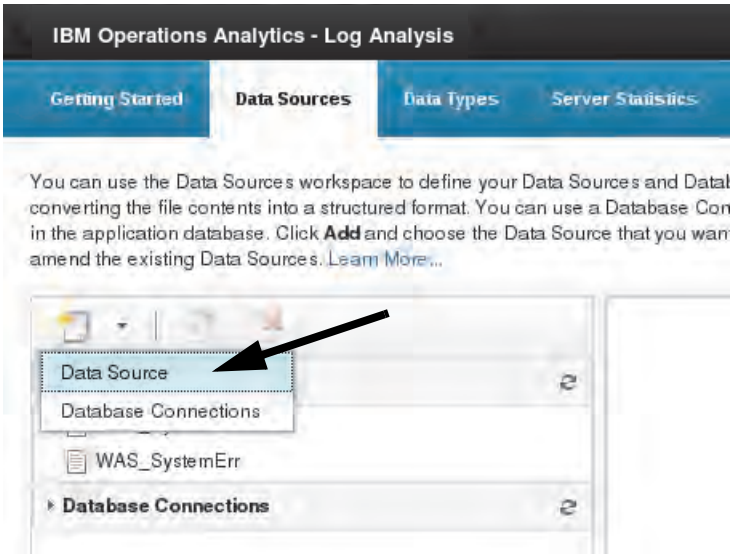
4. Create a data source named **Web_Server**. Use the values in the following table to complete the data source wizard.

Field	Value
Location	Select Remote file
Host name	host2.tivoli.edu
User name	**netcool**
Password	**object00**
File Path	`/software/log_samples/IHS_logs/IHS-access.log`
Type	WebAccessLog
Collection	Leave this field blank
Name	Web_Server
Description	This source uses an IBM HTTP Server log
Group	Leave this field blank

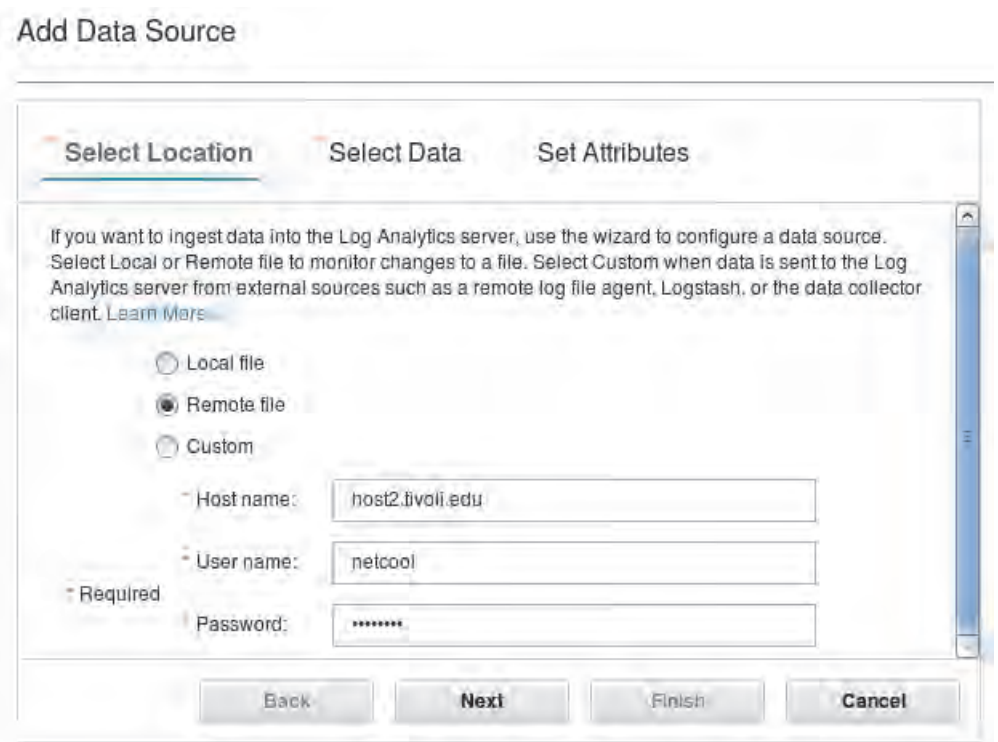
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

a. Click the **Data Sources** tab in the administration user interface. The administration user interface is in the second Firefox tab.

b. Click **Add > Data Source**.

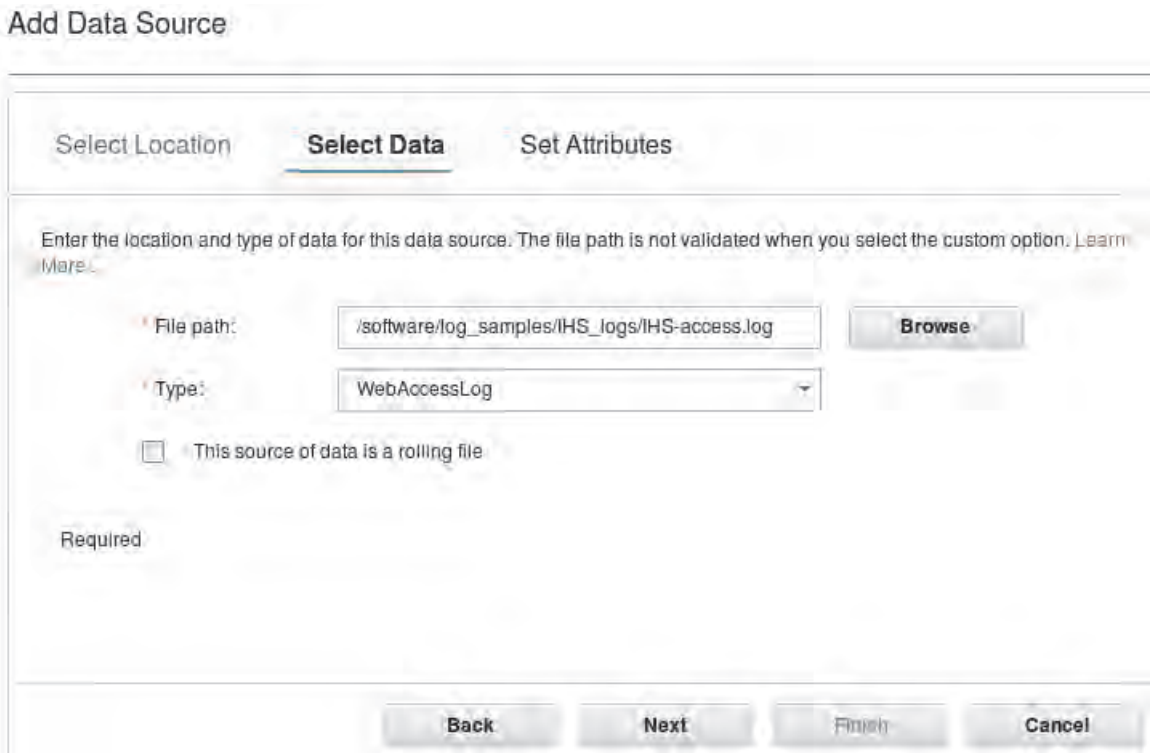


c. Select **Remote file**. Enter `host2.tivoli.edu` as the host name. Enter **netcool** and **object00** as the user name and the password. Click **Next**.

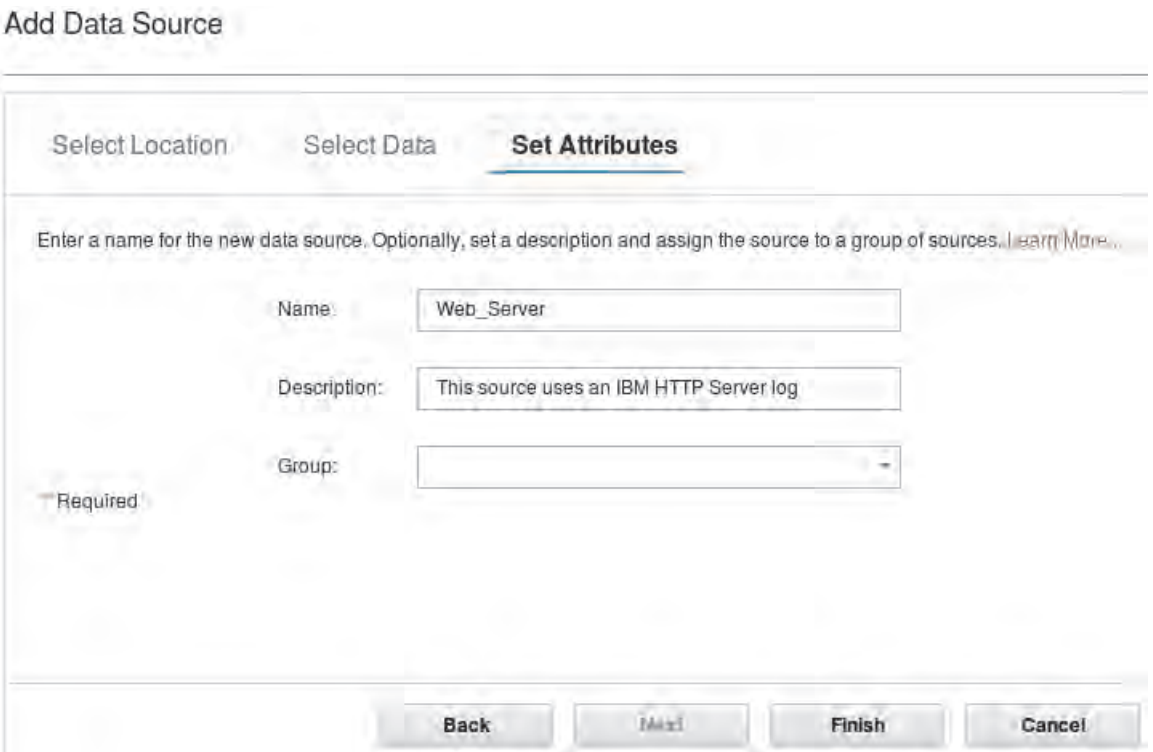


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Enter `/software/log_samples/IHS_logs/IHS-access.log` as the file path. Select **WebAccessLog** as the Type. Click **Next**.

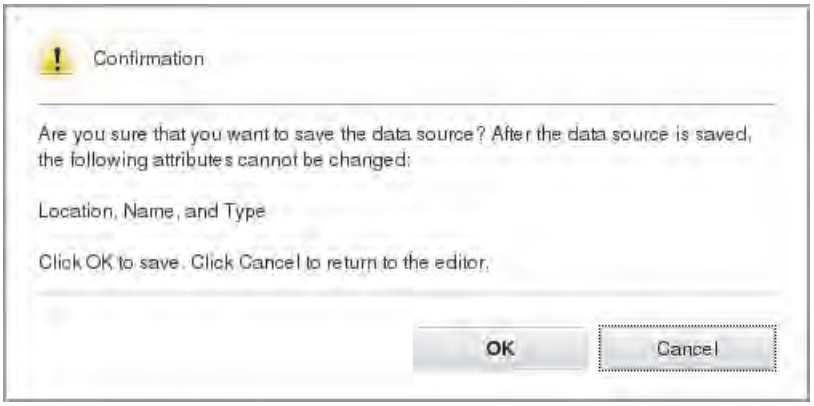


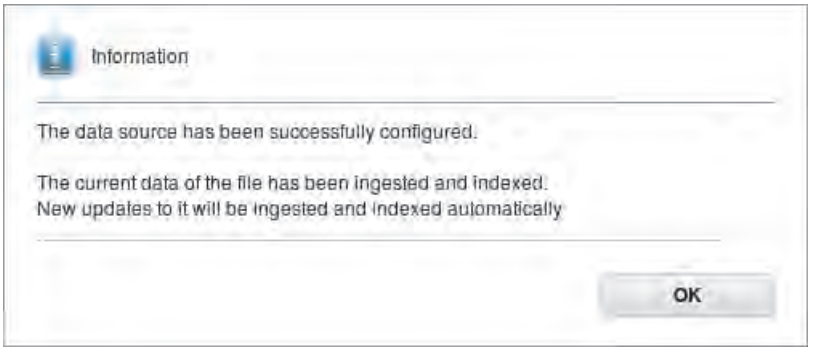
e. Enter **Web_Server** as the name of the data source. Use the description from the preceding table. Click **Finish**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

f. Click **OK** in the confirmation windows.





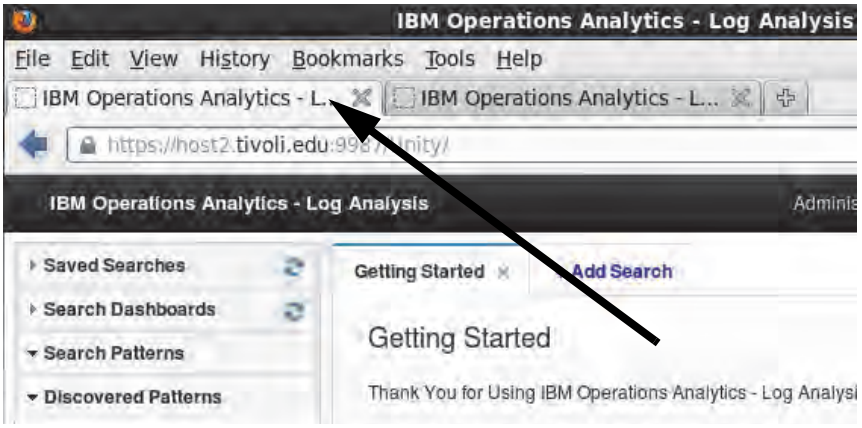
Testing the data sources

The WebSphere® log files, `SystemOut.log` and `SystemErr.log`, for this lab are generated by scripts.

5. Return to a terminal window. Run the following command to generate events in the WebSphere log files.

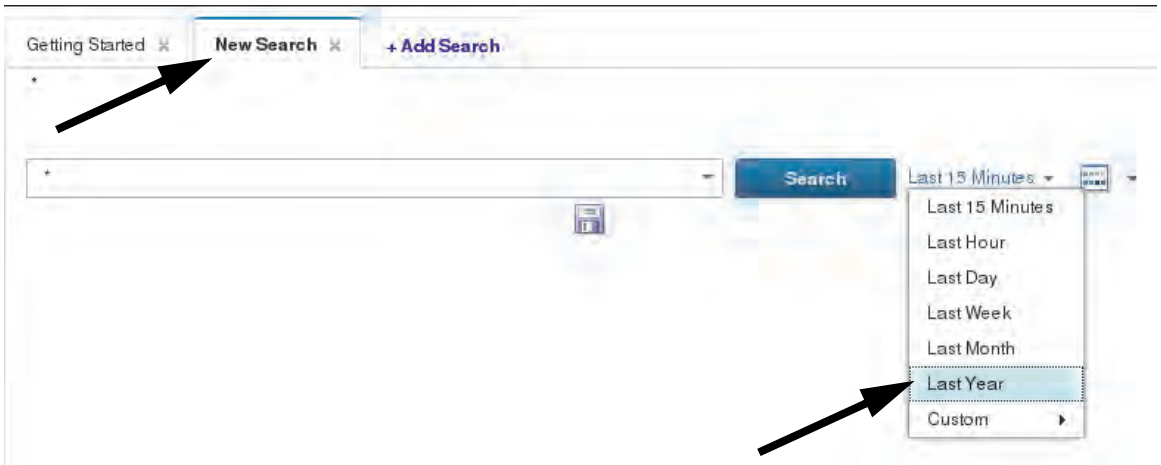
   `/software/log_samples/scripts/WAS_Logs.sh`

6. Return to the user interface by clicking the first Firefox tab.

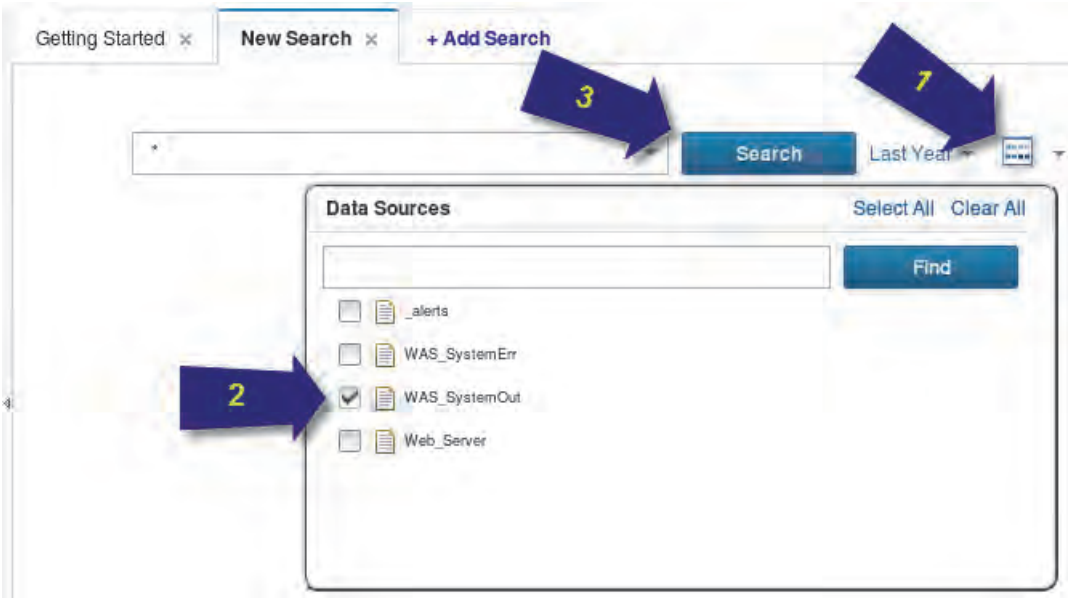


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

7. Search through the WebSphere logs.
   a. Click the **New Search** tab. Select **Last Year** as the time filter.



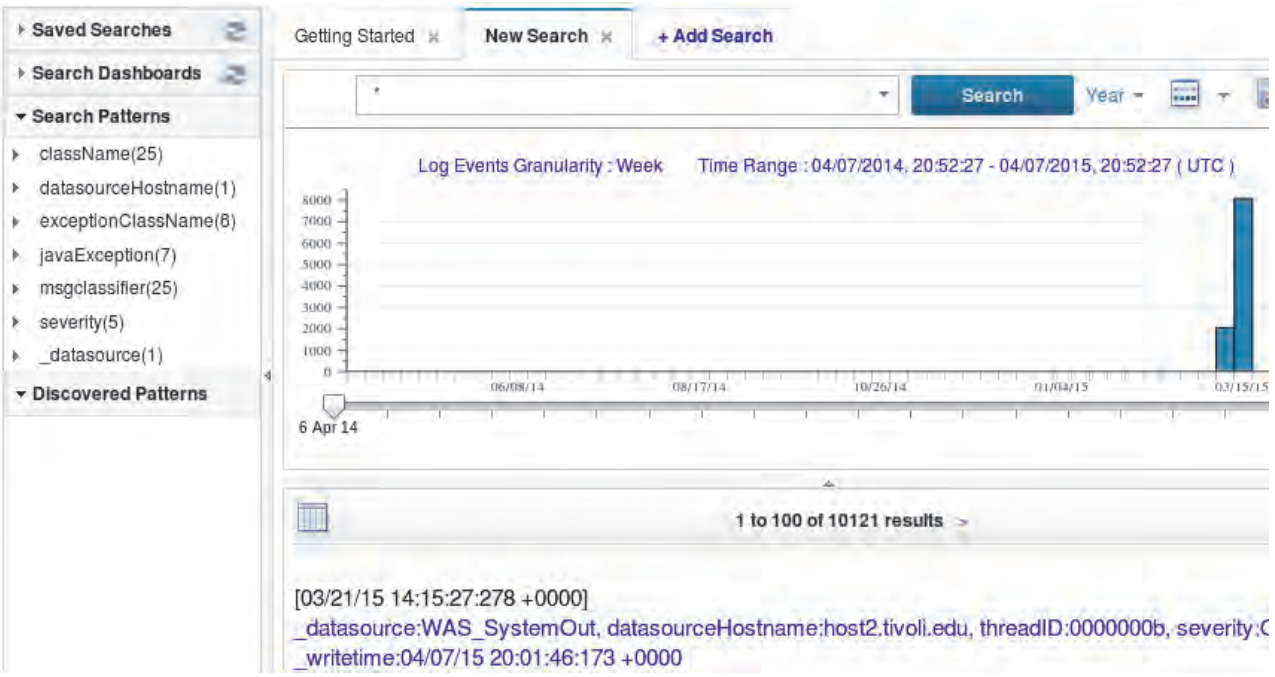
   b. Select only **WAS_SystemOut** as the log source. Click **Search**.



   c. Log events load in to the user interface. There are many events in this sample. Notice the summary on the left of the window. This summary shows the patterns that are found in the log file and the number of events that follow these patterns.

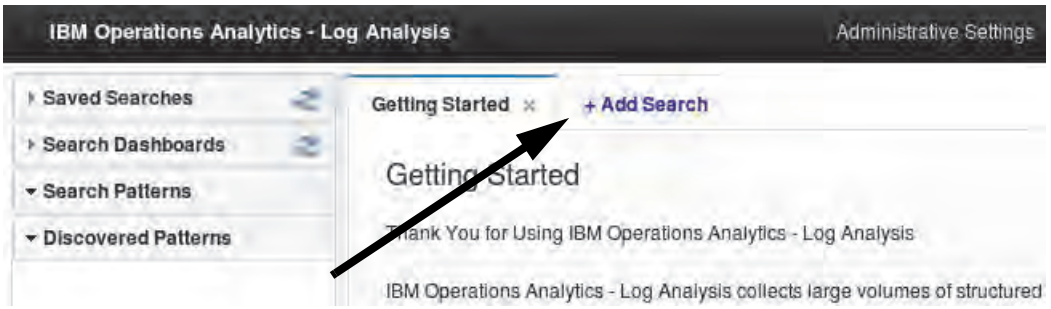
Note: New messages in the log file are processed only after a time-out setting expires. If you do not see any events in the search results, wait 90 seconds and try the search again.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

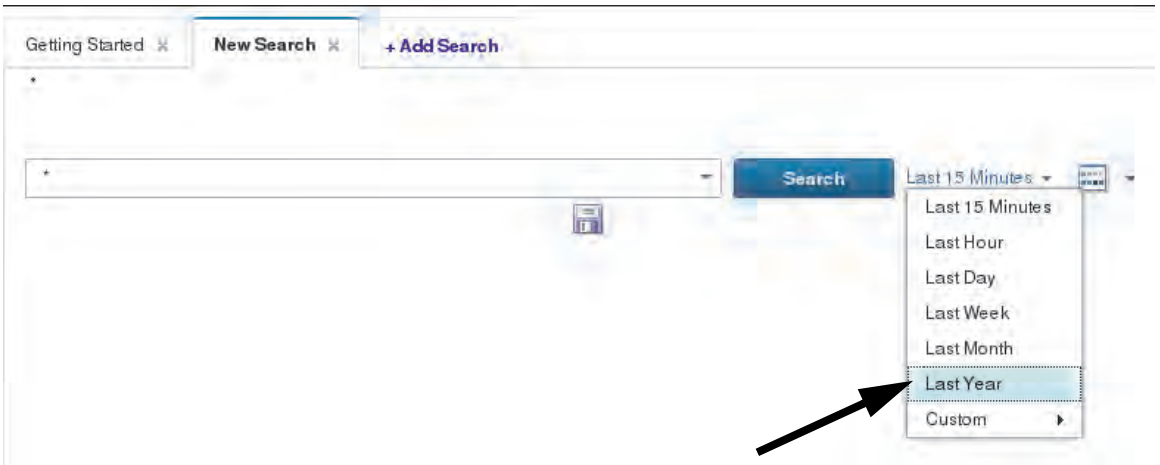


d. Close the **New Search** tab. Click **OK** to confirm.

e. Click **Add Search.** A new search tab opens.



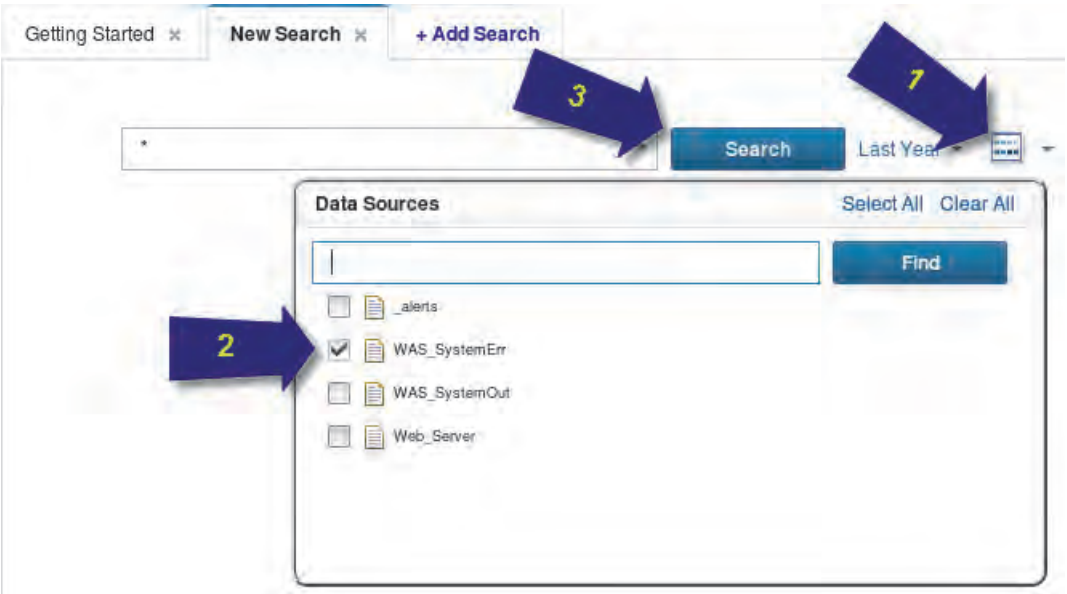
f. Select **Last Year** as the time filter.



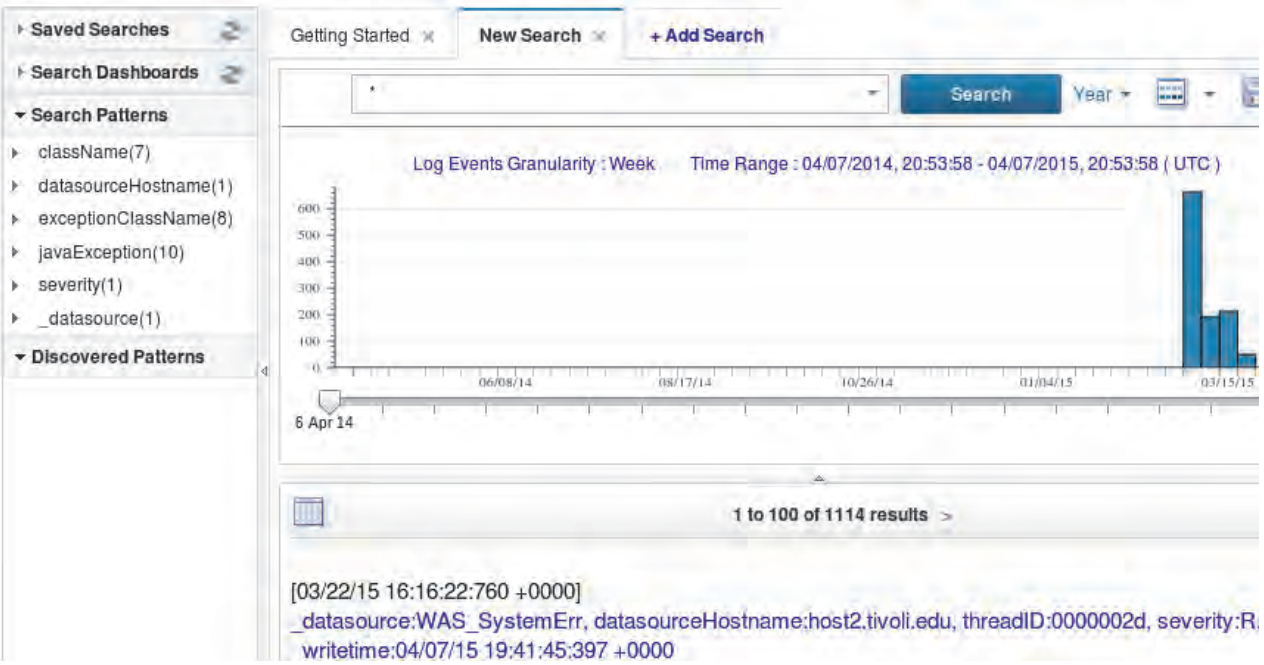
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

g. Select only **WAS_SystemErr** as the log source. Click **Search**.



h. Log events load in to the user interface. There are many events in this sample. Close the **New Search** tab when you finish.

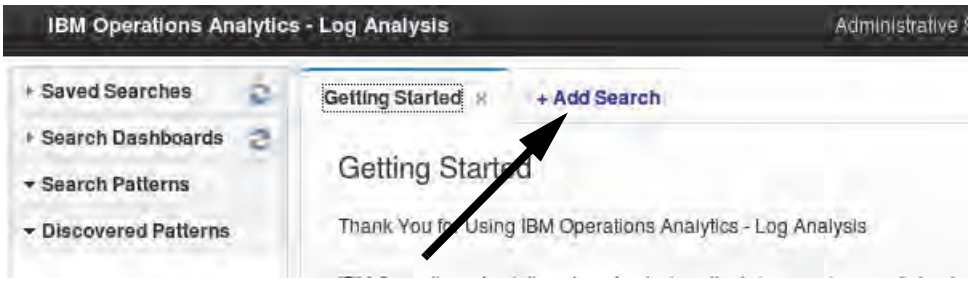


8. Run the following command to generate events in the web access log.

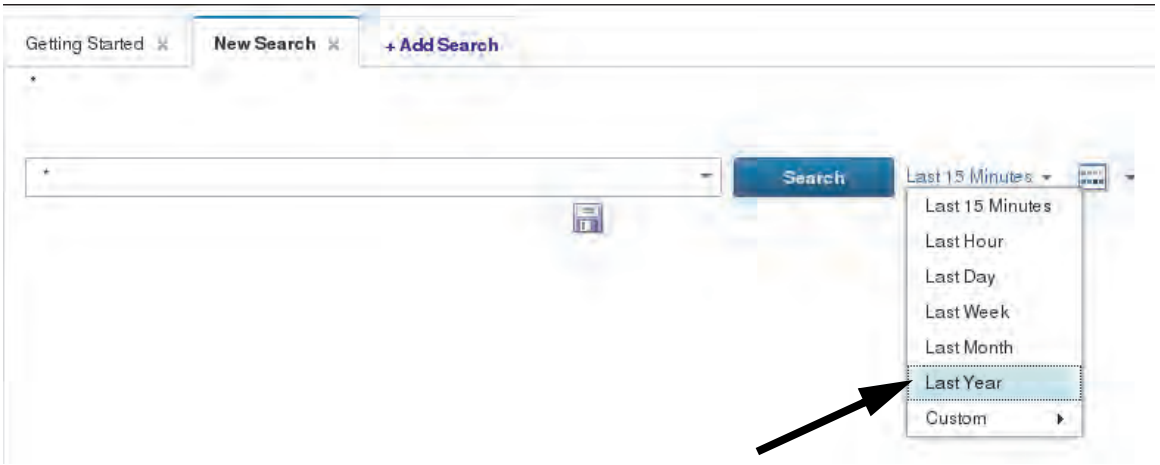
```
/software/log_samples/scripts/Web_Logs.sh
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

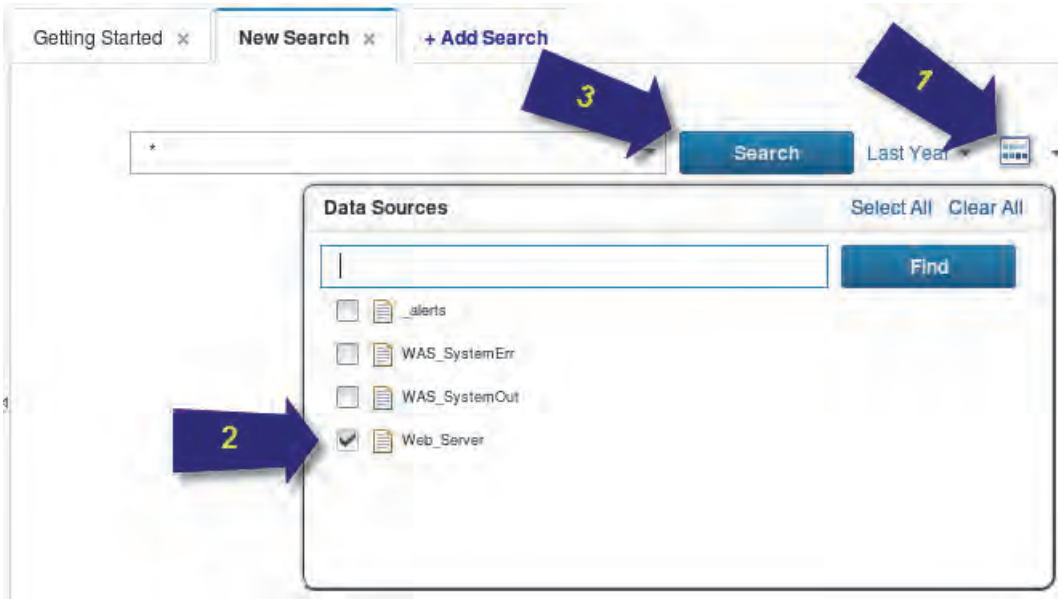
9. Search through the web access log.
   a. Click **Add Search.** A **New Search** tab opens.



   b. Select **Last Year** as the time filter.

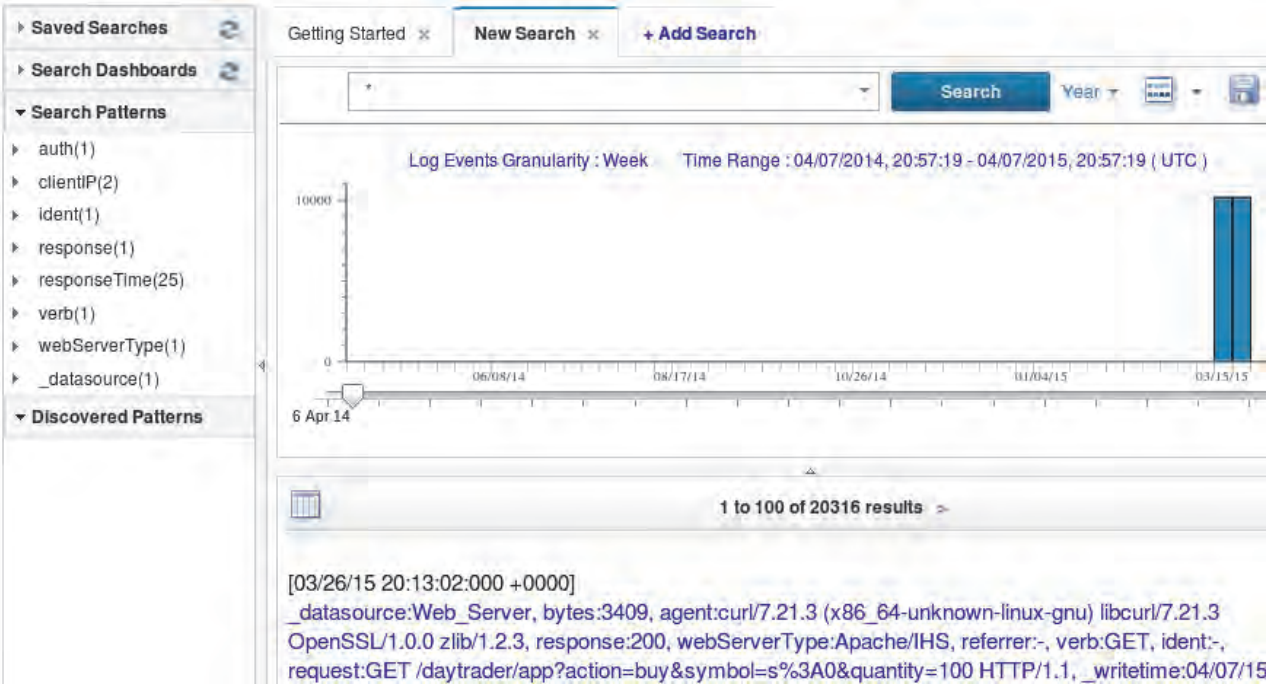


   c. Select only **Web_Server** as the log source. Click **Search**.



Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Log events load in to the user interface. Close the **New Search** tab when you finish.



Configuring search dashboards

Search dashboards show event data in charts and graphs. You must configure the dashboards that are included with Insight Packs before you can use them.

10. Edit the WebSphere search dashboard to match your environment.

    a. Return to the terminal window. Run the following commands to back up the WebSphere dashboard.

    ```
    cd /opt/IBM/LogAnalysis/AppFramework/Apps/WASAppInsightPack_v1.1.0.3
    cp WAS_Troubleshooting.app WAS_Troubleshooting.app.orig
    ```

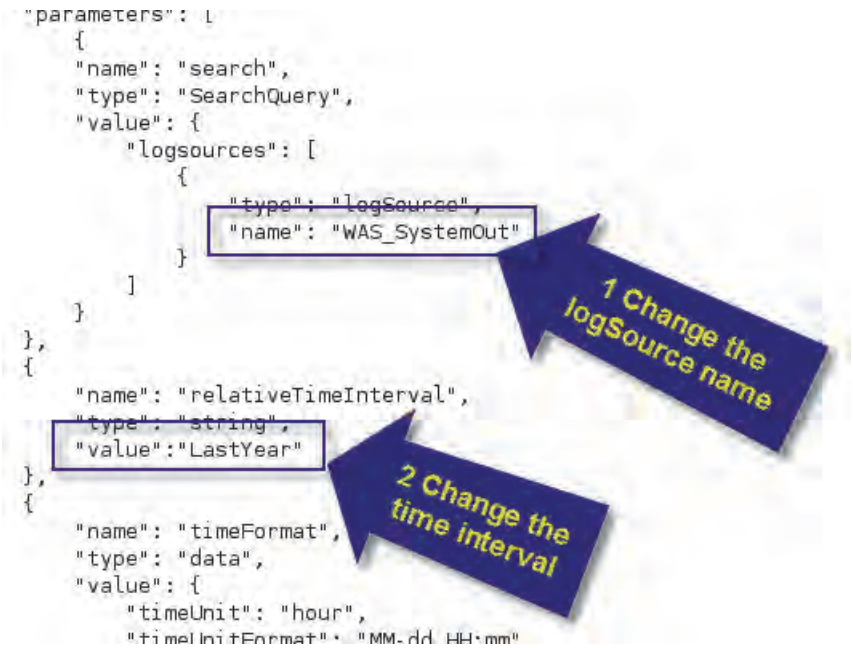
    b. Open the `WAS_Troubleshooting.app` file in a text editor. This example uses `vi`.

    ```
    vi WAS_Troubleshooting.app
    ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Change the following two lines in the file. Make the `WAS_Troubleshooting.app` file look like the following example.

- Change the name of the **logSource** to `WAS_SystemOut`.
- Change the **relativeTimeInterval** to **LastYear**.



d. Save and exit the file after you finish editing it.

11. Edit the Web Health Check dashboard to match your environment.

a. Run the following commands to back up the Web Health Check dashboard.

```
cd /opt/IBM/LogAnalysis/AppFramework/Apps/WebAccessLogInsightPack_v1.1.0.2/
cp Web\ Health\ Check.appExmpl Web\ Health\ Check.app
```

b. Open the `Web\ Health\ Check.app` file in a text editor. This example uses `vi`.

```
vi Web\ Health\ Check.app
```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

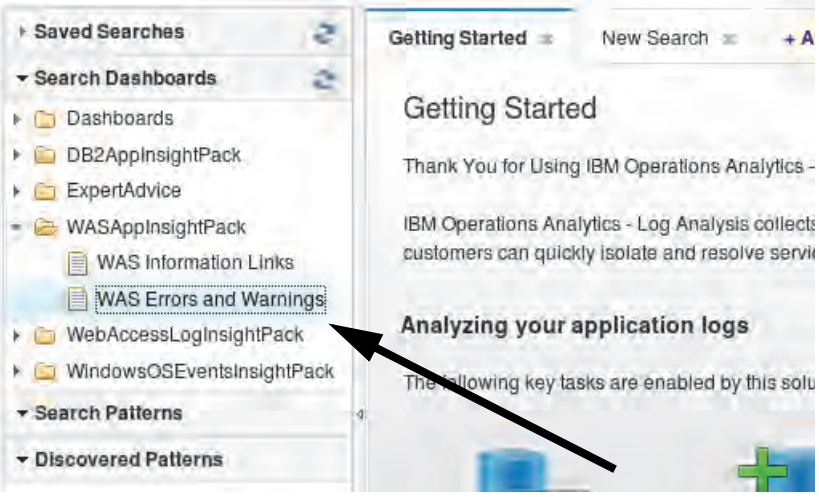
c. Change the following 10 lines in the file. Make the `Web\ Health\ Check.app` file look like the following example.

- Change **lastnum** to **365**. There are five instances of this line in the file. Change all instances.
- Change the name of **logSource** to **Web_Server**. There are five instances of this line in the file. Change all instances.

d. Save and exit the file after you finish editing it.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

12. Return to the user interface. Test the WebSphere dashboard.
    a. Double-click **Search Dashboards > WASAppInsightPack > WAS Errors and Warnings** on the left of the window.



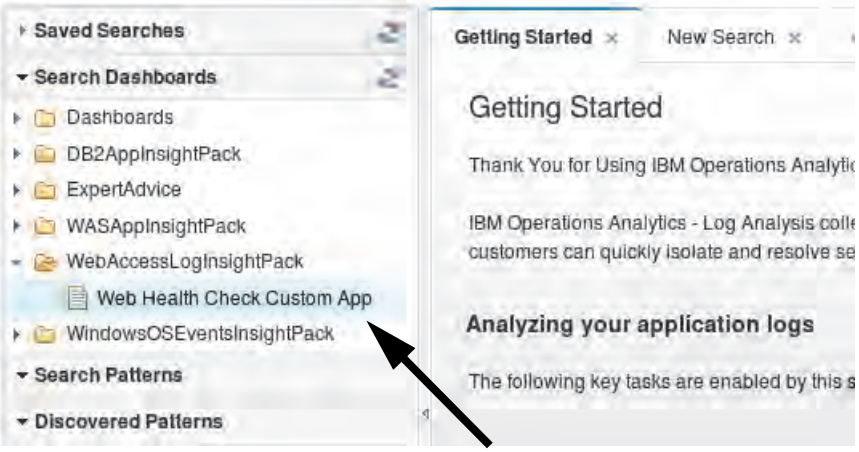
    b. Scroll down and look at the WAS Errors and Warnings page. This page shows useful troubleshooting graphics, such as number of errors and warnings or top five message counts.

    c. Close the dashboard page.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

13. Test the Web Health Check dashboard.
    a. Double-click **Search Dashboards > WebAccessLogInsightPack > Web Health Check Custom App** on the left of the window.



    b. Scroll down and look at the Web Health Check dashboard page.

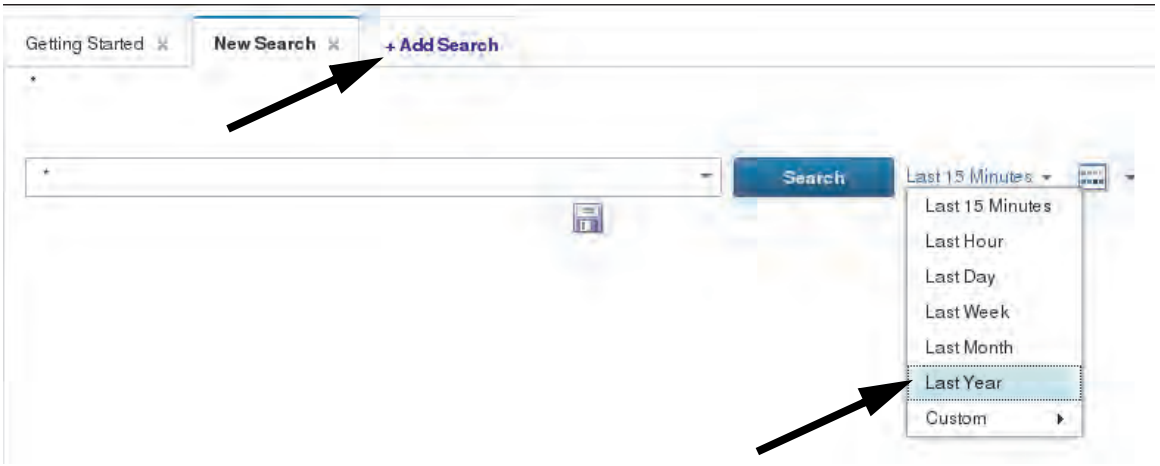
       This page shows useful troubleshooting graphics, such as response time or number of requests. The charts on this page are customizable. The data points in these charts are interactive. You can drill down to specific log messages from this dashboard.

    c. Close the dashboard page.

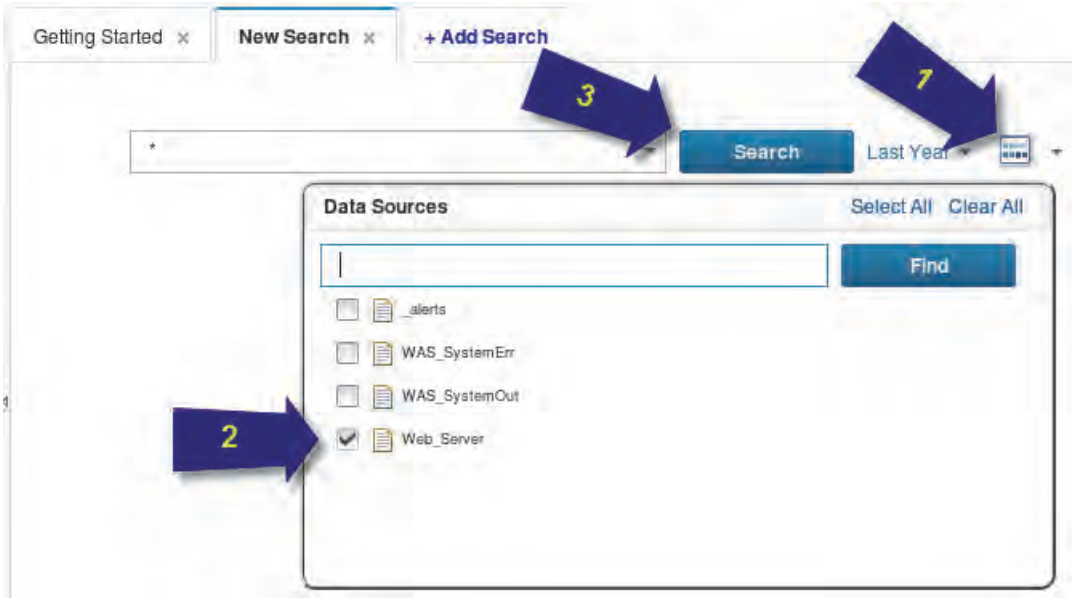
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Saving searches and creating dashboards

14. Search through the web server log:
    a. Click the **Add Search** tab. Select **Last Year** as the time filter.



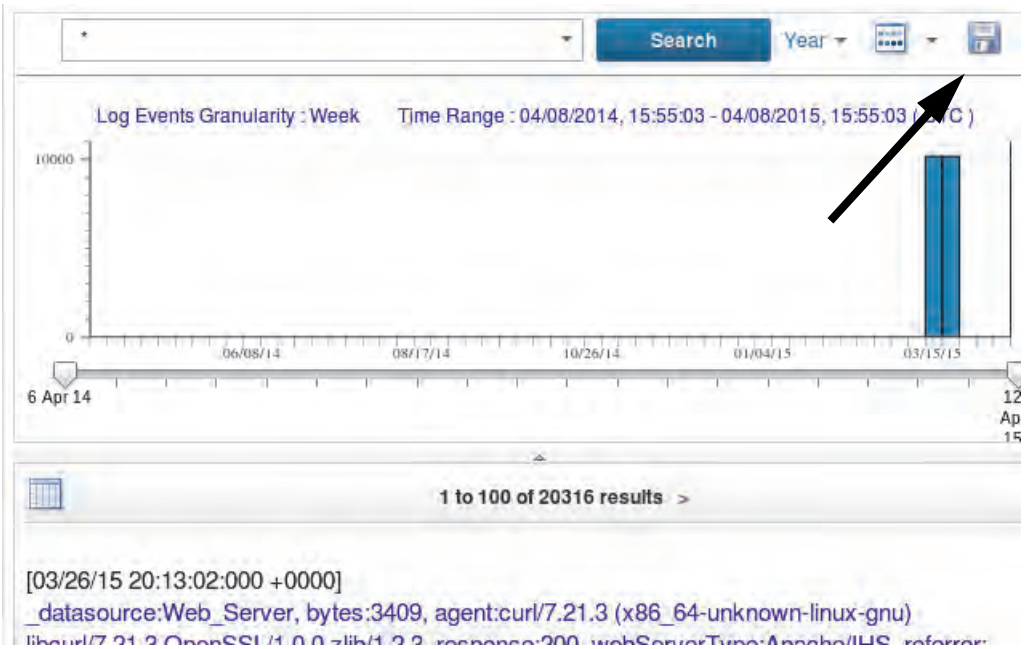
    b. Select only **Web_Server** as the source. Click **Search**.



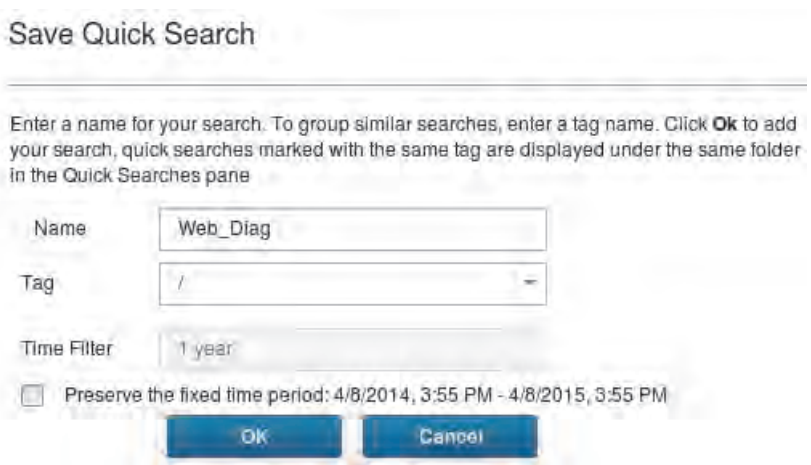
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

15. Log events load in to the user interface. Save your search:
    a. Click the **Save** button.

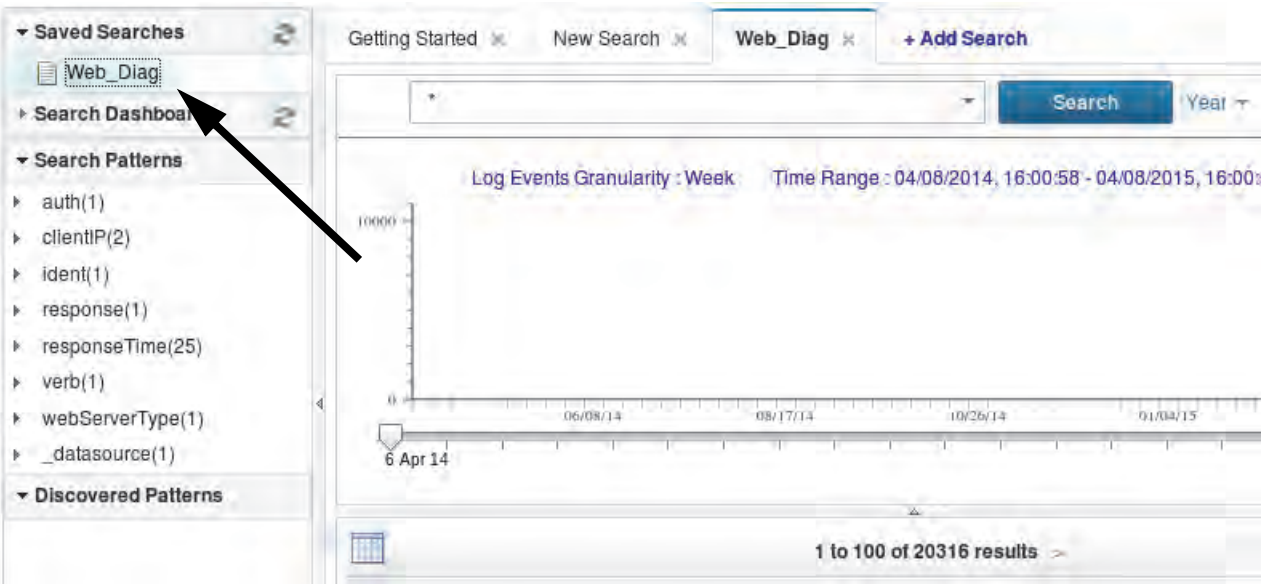


    b. Enter `Web_Diag` as the **Name** and click **OK**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

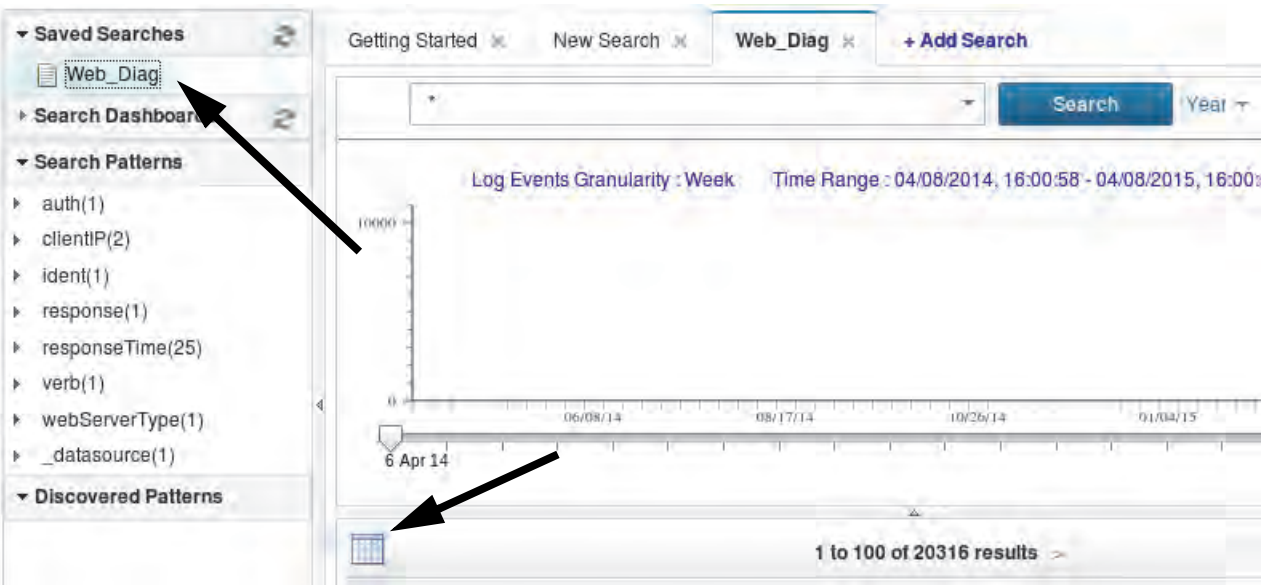
c. Double-click the **Saved Searches > Web_Diag** link to verify that the search was saved.



Dashboard pages contain charts that show log data. You can create charts and dashboards from any log file. In this example, you use a web access log file.

16. Create a dashboard page with two charts that show data from the web access log:

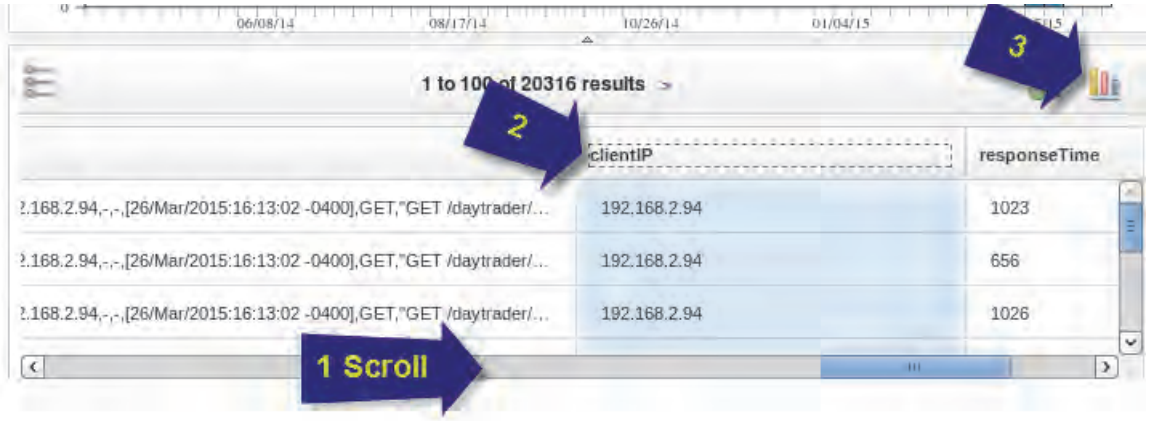
a. Configure the first chart to show the number of messages by client IP. Run the **Web_Diag** saved search. Click the **Grid View** button.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

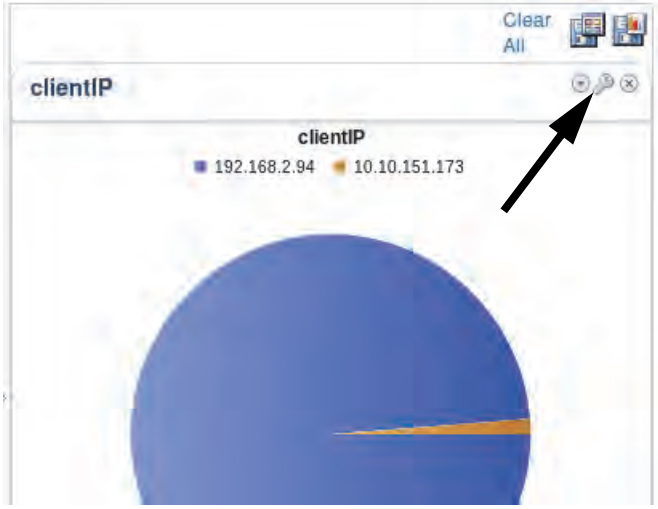
b. Scroll to the right in the search results and click the **clientIP** column. Click the **Plot Column** button.



c. Select **Generate Counts**.

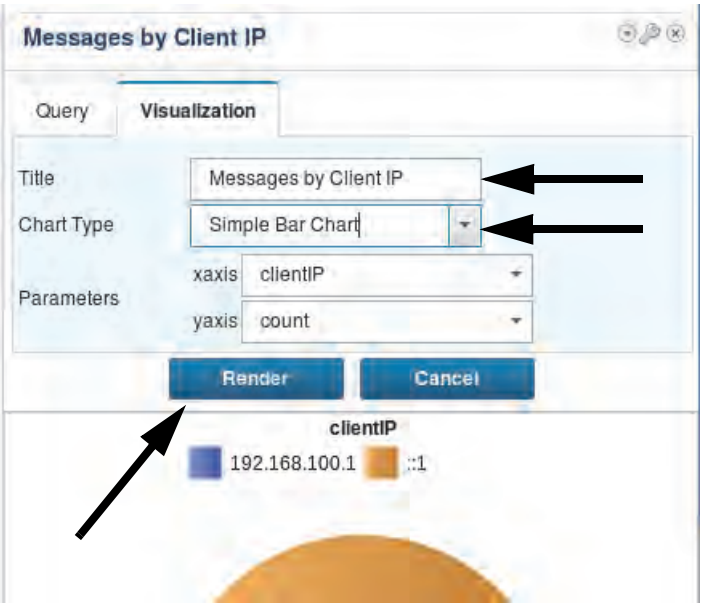
d. Click **Plot Chart (All Data)**.

e. Edit the chart by clicking the **Settings** button at the upper right of the chart.

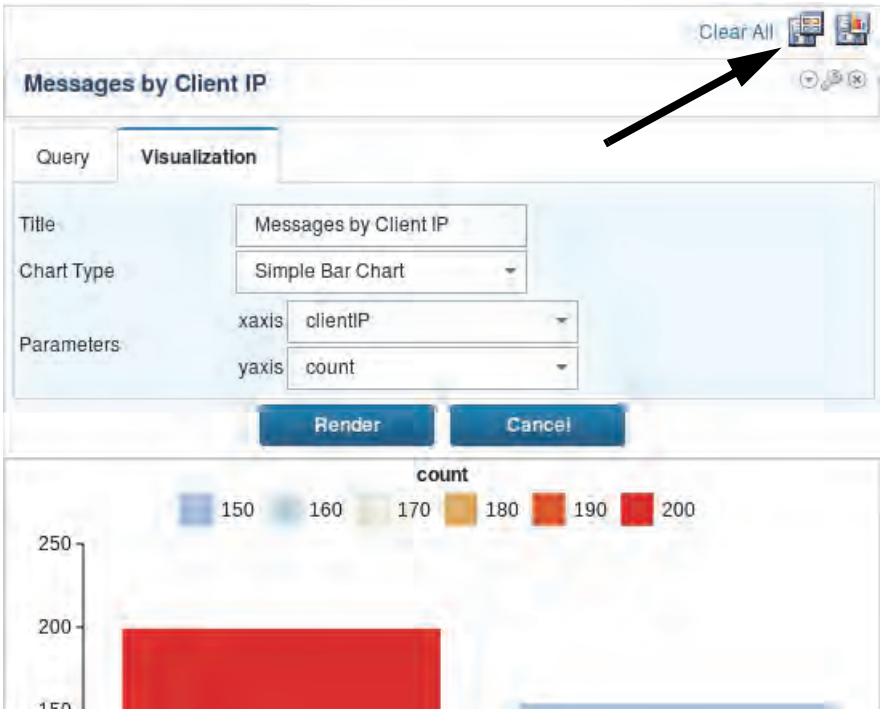


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

f. Change the title to `Messages by Client IP`. Change the chart type to **Simple Bar Chart**. Click **Render**.



g. Click the **Create New Dashboard** button at the top of the chart.

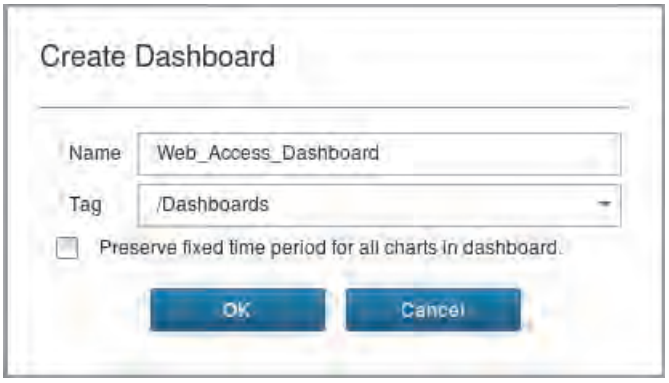


h. Enter `Web_Access_Dashboard` for the dashboard name.

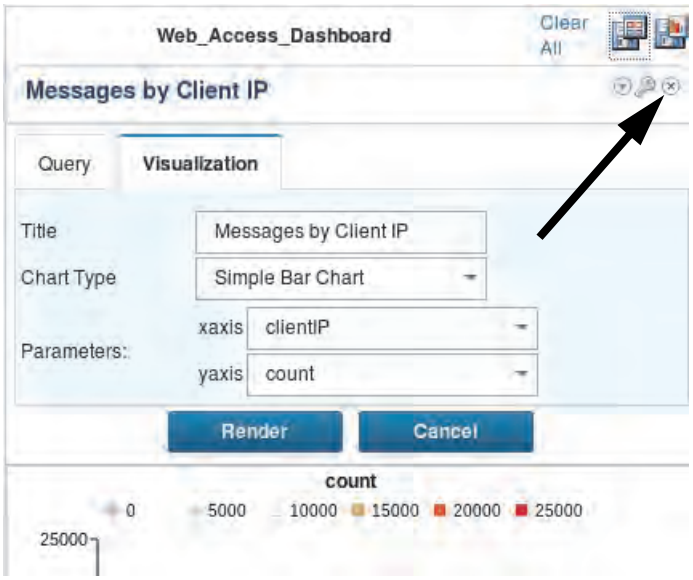
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

i. Enter `/Dashboards` into the **Tag** field and click **OK**.



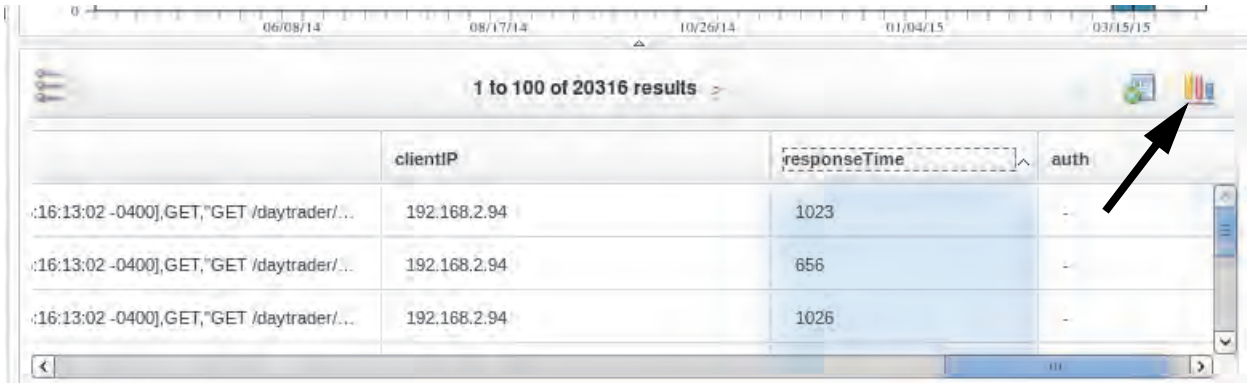
j. Close the chart page. After you close the chart page, you return to the search results.



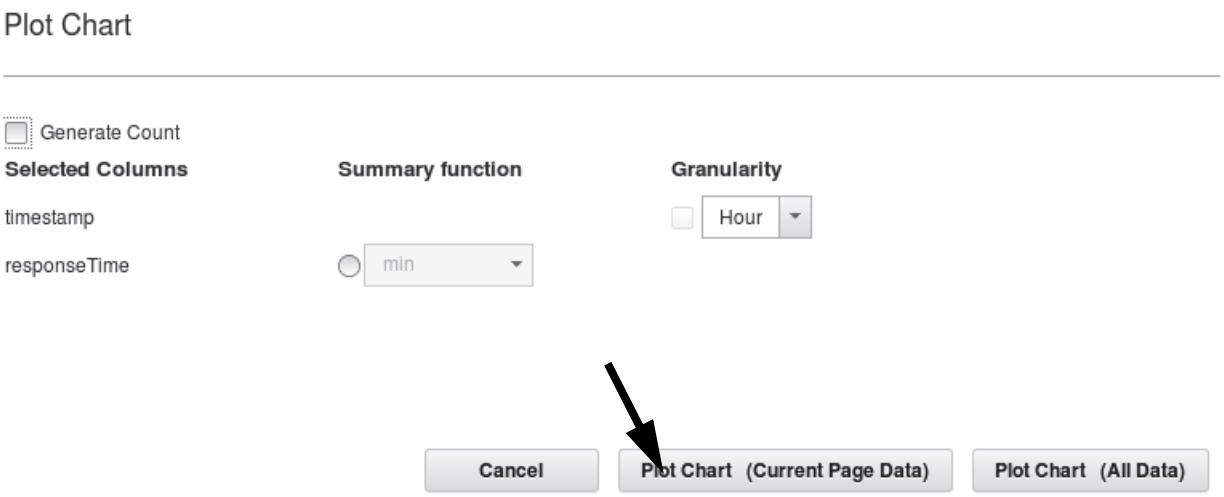
k. Create the second chart. Scroll in the search results and select these two column titles: **timestamp** and **responseTime**. Use the Ctrl key to select multiple columns. Click the **Plot Column** button.

Note: If you click the **timestamp** column first, it is used as the *x*-axis of the chart.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.



l. Click **Plot Chart (Current Page Data)**.

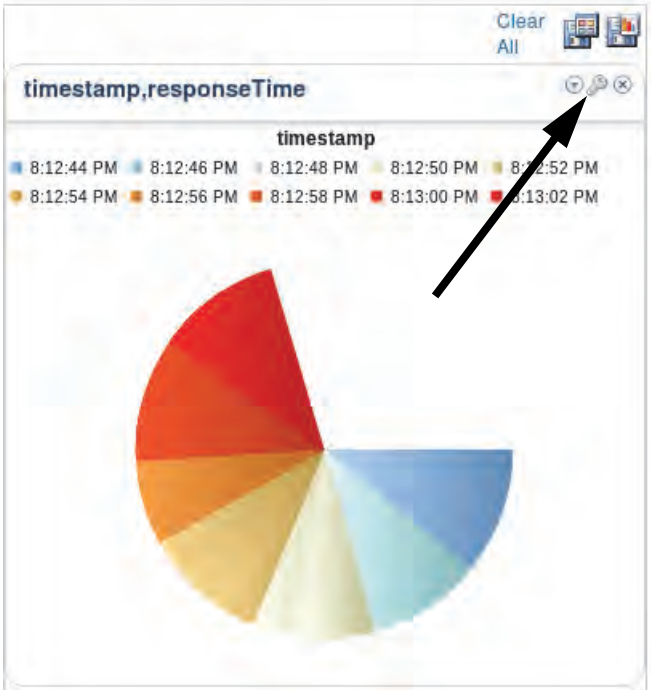


m. Click **Close** on the hint about granularity.

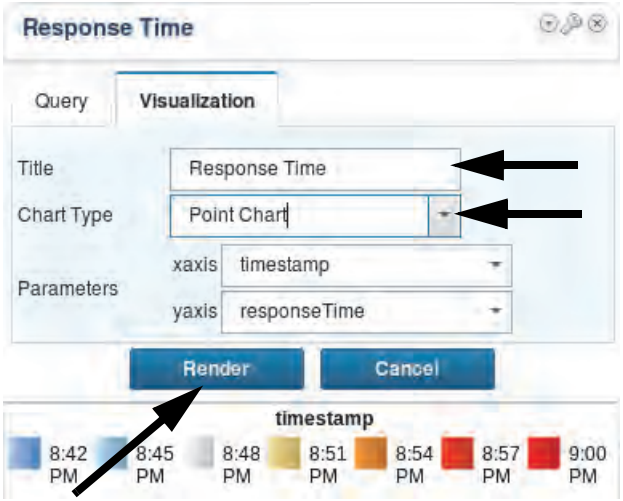
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

n. Edit the chart by clicking the **Settings** button at the upper right of the chart.

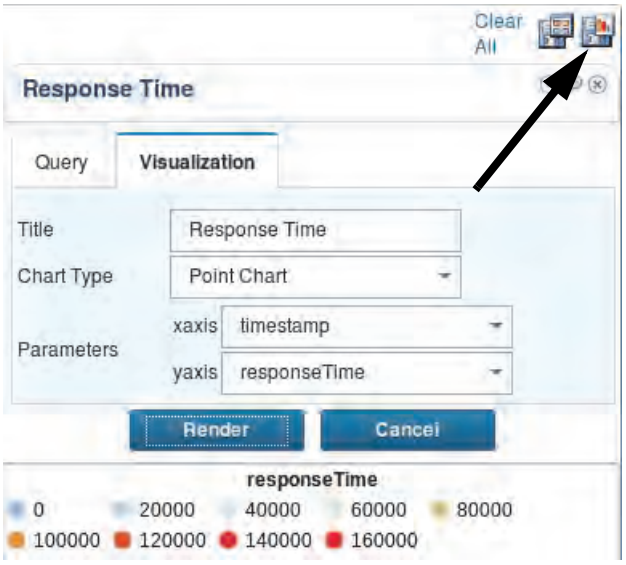


o. Change the title to `Response Time`. Change the chart type to **Point Chart**. Click **Render**.

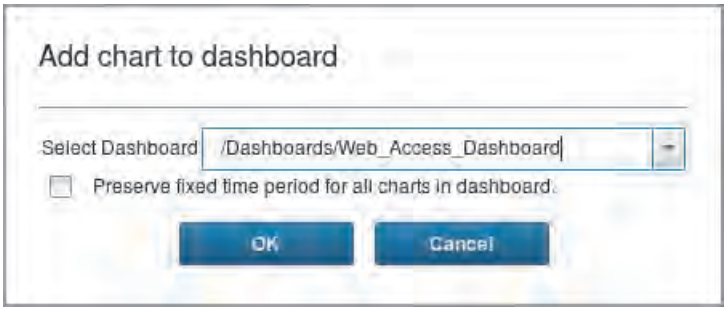


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

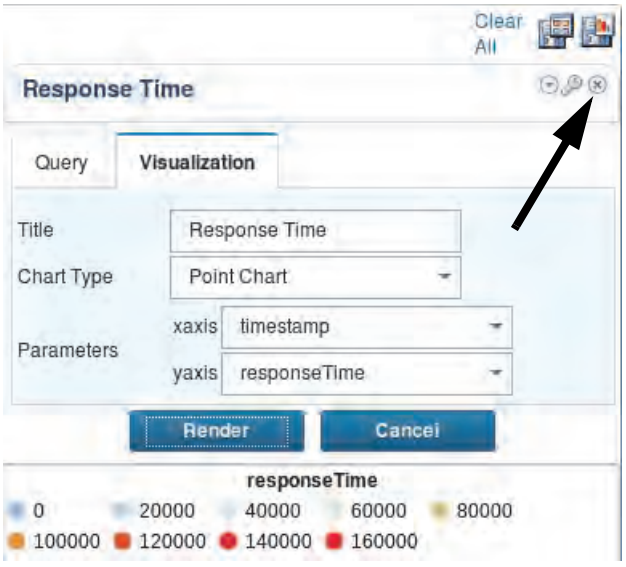
p. Click the **Add Chart** button at the top of the chart.



q. Select **/Dashboards/Web_Access_Dashboard** and click **OK**.



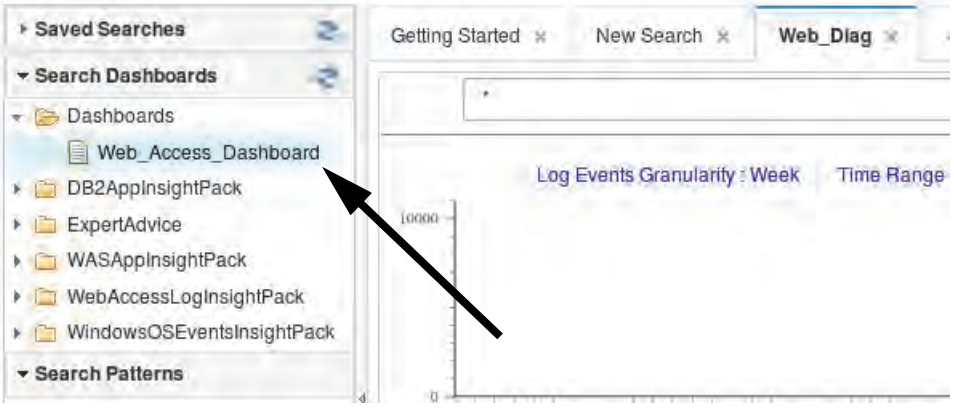
r. Close the chart page.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

17. Test the dashboard:
    a. Expand **Search Dashboards > Dashboards** on the left side of the window. Double-click **Web_Access_Dashboards**.



    b. Verify that both charts are on the dashboard page. Leave the page open.

    c. Run the following command to generate more events in the web access log.

```
/software/log_samples/scripts/Web_Logs.sh
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Return to the dashboard page. Click **Actions > Auto-Refresh > Every 1 minutes**.

e. Wait 1 minute for the page to refresh. Notice that the *y*-axes of the charts change as more log messages are processed.

Hint: This lab uses different types of log files. Create dashboards for the other log types if you want more practice using the charting and dashboard features.

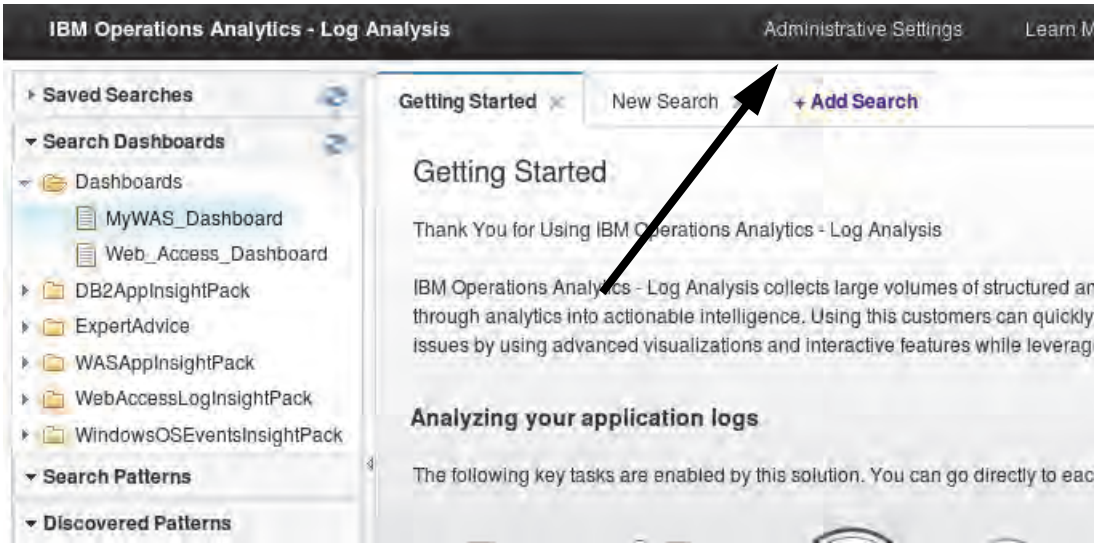
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 3 Deleting historical data

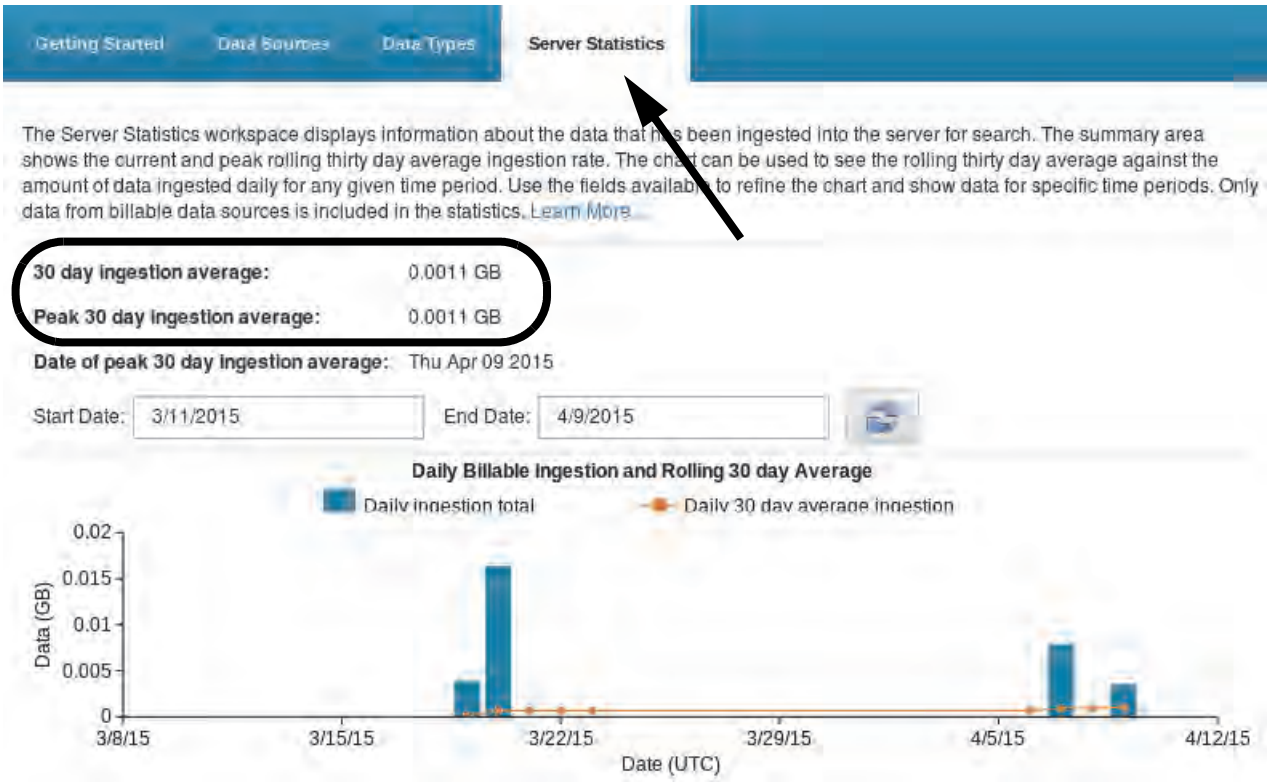
In this exercise, you view reports about the volume of log data that IBM Operations Analytics Log Analysis processes. You also delete historical data from the system.

1. Use the Server Statistics page to see how much data IBM Operations Analytics Log Analysis has processed.
   a. Return to the user interface. Click **Administrative Settings**. The administration user interface opens in a new Firefox tab.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Click the **Server Statistics** tab in the administration user interface. This page shows the volume of data that is processed with other product usage measurements. Notice the amount of data that is processed.



2. You can use the export_statistics utility to show the volume of data that is processed. Run the following commands to show the volume of data that was processed by data source. Notice the name of each data source and the name of the collection.

```
cd /opt/IBM/LogAnalysis/utilities
./export_statistics -u unityadmin -p unityadmin -t daily
```

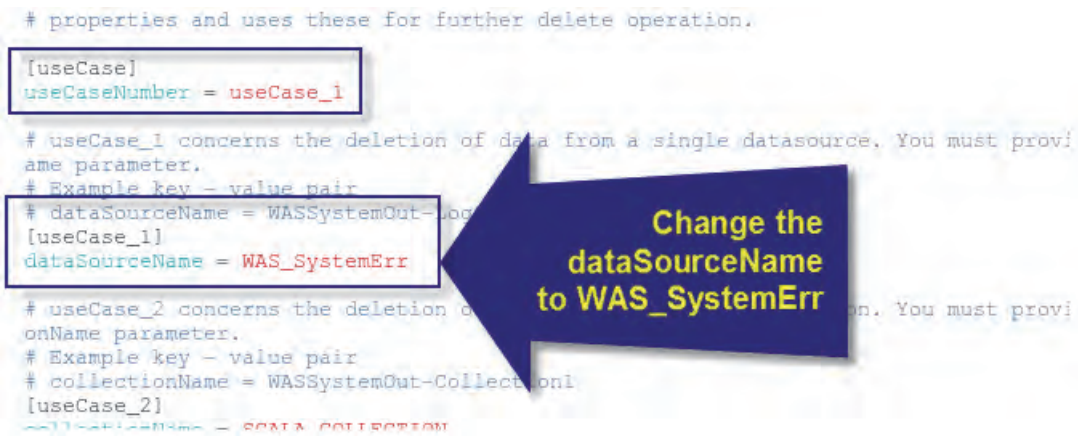
```
Data Source      |          Collection          |     Date     |  Ingested Bytes
|  Billable  |                    Log Path                    |      Hostname
-----------------------+-----------------------------+--------------+---------
---------+------------+-------------------------------------------------+------
--------------
WAS_SystemErr       |  WAS_SystemErr            |  2015-04-07  |      533498
|    True    |  /software/log_samples/WAS_logs/SystemErr.log   |
host2.tivoli.edu
  WAS_SystemOut       |  WAS_SystemOut            |  2015-04-07  |    1051931
|    True    |  /software/log_samples/WAS_logs/SystemOut.log   |
host2.tivoli.edu
  Web_Server          |  Web_Server               |  2015-04-07  |    4749248
|    True    |  /software/log_samples/IHS_logs/IHS-access.log  |
host2.tivoli.edu
```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

3. You use a command-line tool to delete data from the system. Use this tool to remove data from the WebSphere SystemErr data source that you previously created.
   a. You must configure the tool to delete only the data you define. Open the `delete.properties` file in a text editor to configure the tool. This example uses `vi`.

      ```
      cd /opt/IBM/LogAnalysis/utilities/deleteUtility
      vi delete.properties
      ```

   b. Make one change to this file. Change the value of the **dataSourceName** property to **WAS_SystemErr**. Notice the use case number close to the top of the file. Make the `delete.properties` file look like the following example.



   c. Save and exit the file after you finish editing it.

   d. Run the following command to delete data from the WAS_SystemErr data source.

      ```
      /usr/bin/python2.6 deleteUtility.py unityadmin
      ```

   e. Look at the log file that shows what data you deleted. The bottom of the log shows the records that were deleted. Use the following command to view the log.

      ```
      tail -20 /opt/IBM/LogAnalysis/logs/DeleteApplication.log
      ...
      04/09/15 13:43:41:339 UTC [main] INFO  - DeleteManager : Datasource retrieved
      :WAS_SystemErr
      04/09/15 13:43:41:601 UTC [main] INFO  - SolrDeleteManager : Solr collection
      UnityCollection_07_04_2015_00_00_00_UTC, delete query:
      +(_datasource:"WAS_SystemErr")
      04/09/15 13:43:42:167 UTC [main] INFO  - SolrDeleteManager : Solr collection
      UnityCollection_09_04_2015_00_00_00_UTC, delete query:
      +(_datasource:"WAS_SystemErr")
      04/09/15 13:43:42:192 UTC [main] INFO  - CommonUtil : 1 Trying to suspend
      thread execution for 1000 miliseconds.
      04/09/15 13:43:43:229 UTC [main] INFO  - CommonUtil : 1 Successfully executed
      POST request.
      ```

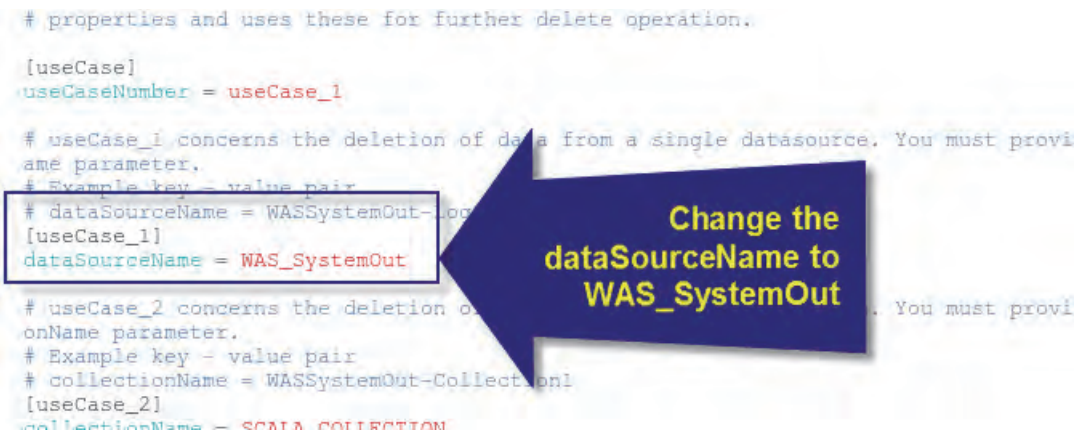

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
04/09/15 13:43:43:229 UTC [main] INFO  - DeleteManager : Total number of
records deleted:  All records deleted
04/09/15 13:43:43:229 UTC [main] INFO  - DeleteManager : Total number of
records :  All records deleted
```

4. Use the tool again to remove data from the WebSphere SystemOut data source that you created.
   a. Open the `delete.properties` file again a text editor. This example uses `vi`.

      ```
      vi delete.properties
      ```

   b. Change the value of the **dataSourceName** property to **WAS_SystemOut**. Make the `delete.properties` file look like the following example.



   c. Save and exit the file after you finish editing it.

   d. Run the following command to delete data from the WAS_SystemOut data source.

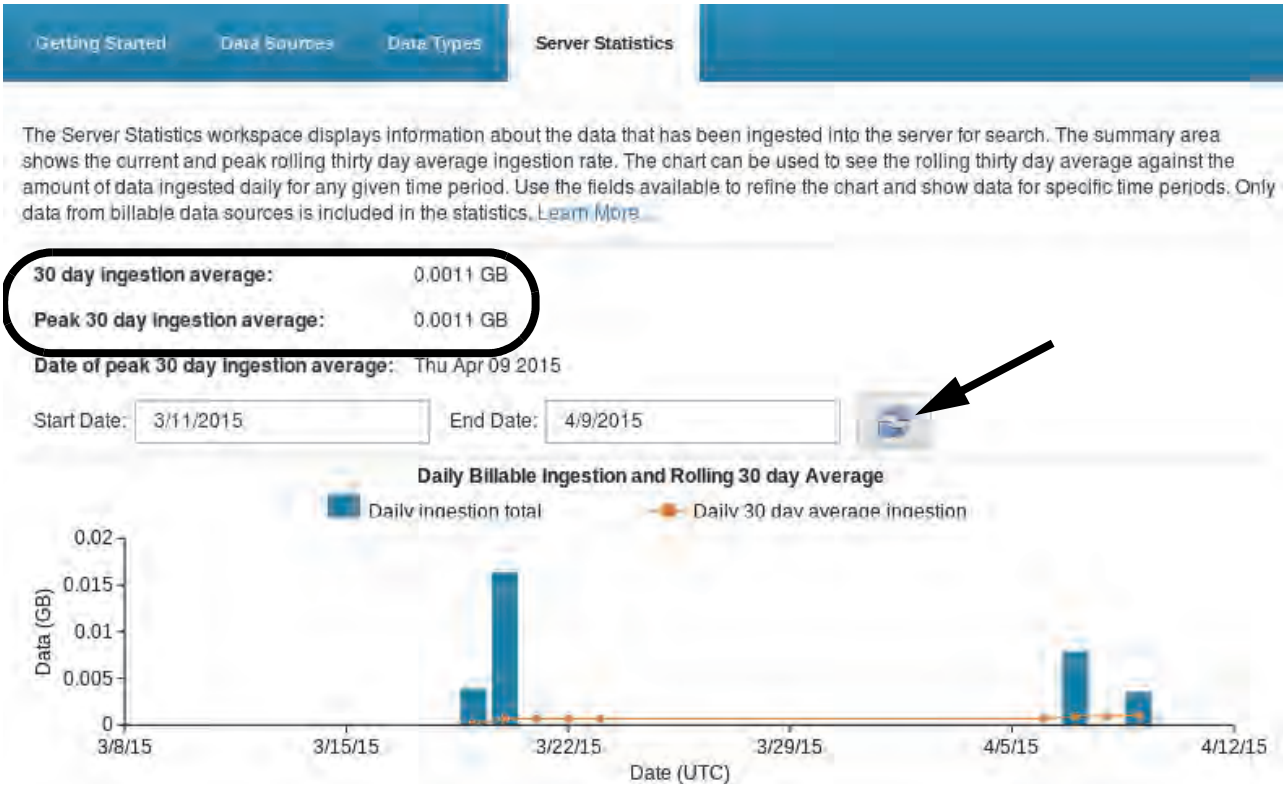
      ```
      /usr/bin/python2.6 deleteUtility.py unityadmin
      ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Look at the log file that shows what data you deleted. The bottom of the log shows the number of records that are deleted. Use the following command to view the log.

```
tail -20 /opt/IBM/LogAnalysis/logs/DeleteApplication.log
...
04/09/15 13:52:07:377 UTC [main] INFO  - DeleteManager : Datasource retrieved
:WAS_SystemOut
04/09/15 13:52:07:597 UTC [main] INFO  - SolrDeleteManager : Solr collection
UnityCollection_07_04_2015_00_00_00_UTC, delete query:
+(_datasource:"WAS_SystemOut")
04/09/15 13:52:08:046 UTC [main] INFO  - SolrDeleteManager : Solr collection
UnityCollection_09_04_2015_00_00_00_UTC, delete query:
+(_datasource:"WAS_SystemOut")
04/09/15 13:52:08:072 UTC [main] INFO  - CommonUtil : 1 Trying to suspend
thread execution for 1000 miliseconds.
04/09/15 13:52:09:096 UTC [main] INFO  - CommonUtil : 1 Successfully executed
POST request.
04/09/15 13:52:09:096 UTC [main] INFO  - DeleteManager : Total number of
records deleted:  All records deleted
04/09/15 13:52:09:097 UTC [main] INFO  - DeleteManager : Total number of
records :  All records deleted
```

5. Return to the **Server Statistics** page in the administration user interface. Click the **Refresh** button. Notice that the measurements of how much data is processed do not change, even after you delete historical data.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Note: The product usage measurements that you see with the export_statistics tool are like the measurements on this page. They do not change even after you delete data.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

2 Common configuration tasks exercises

Exercise 1 Using the Generic Annotation Insight Pack

In this exercise, you use the Generic Annotation Insight Pack to analyze an OMNIbus ObjectServer log file.

1. Open the ObjectServer log file sample. Notice the format of the time stamp.
   a. Run the following command to open the ObjectServer log file sample.

      ```
      more /home/netcool/NYC_AGG_P.log
      ```

   b. Look at the format of the time stamp in this log. The format is **yyyy-MM-dd'T'HH:mm:ss**.

      ```
      2015-04-08T14:07:05: Warning: W-STO-103-001: Truncating column SiteState
      2015-04-08T14:07:05: Warning: W-STO-103-001: Truncating column SiteState
      2015-04-08T14:07:05: Warning: W-STO-103-001: Truncating column SiteState
      ```

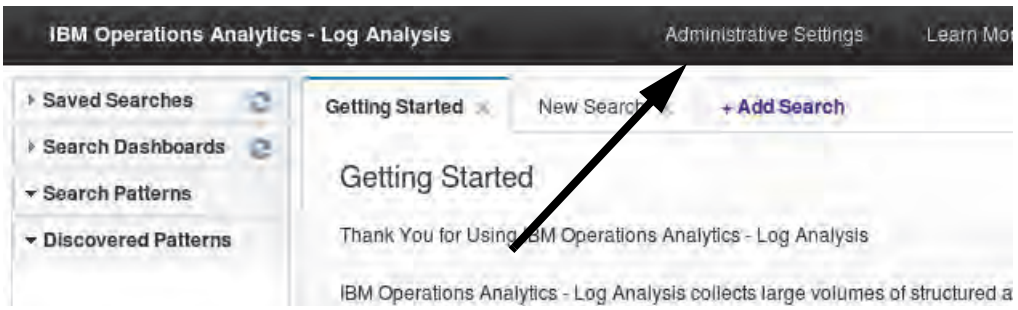
2. Open the administration user interface.
   a. Double-click the **Firefox** icon on the desktop.

   b. Browse to the following address.

      ```
      https://host2.tivoli.edu:9987/Unity
      ```

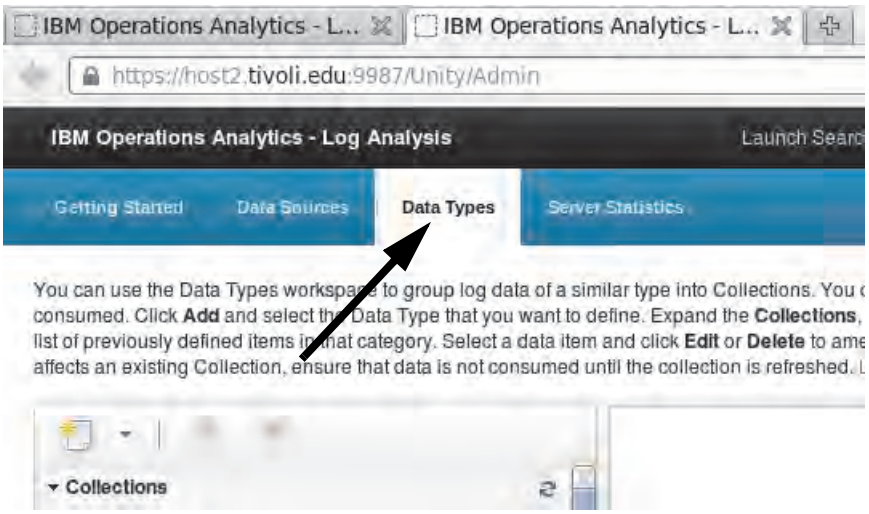
   c. Log in to the user interface with the user name **unityadmin** and the password **unityadmin**.

   d. Click **Administrative Settings**. The administration user interface opens in a new Firefox tab.

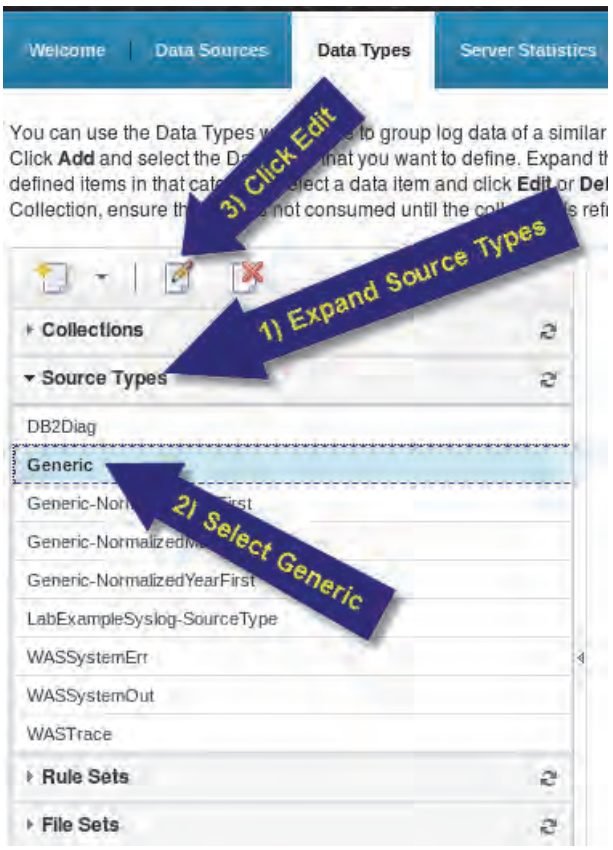


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

3. Open the **Generic** source type in the administration user interface. Copy the index configuration from the **Generic** source type.
   a. Click the **Data Types** tab in the administration user interface. The administration user interface is in the second Firefox tab.

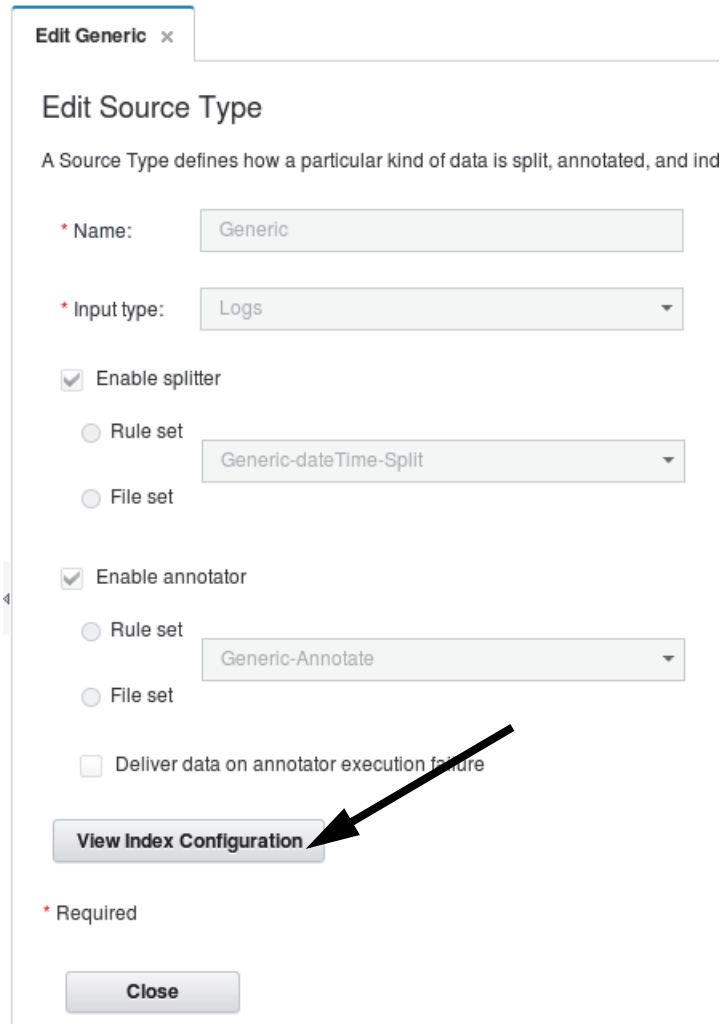


   b. Expand **Source Types**. Select the **Generic** source type and click **Edit**.



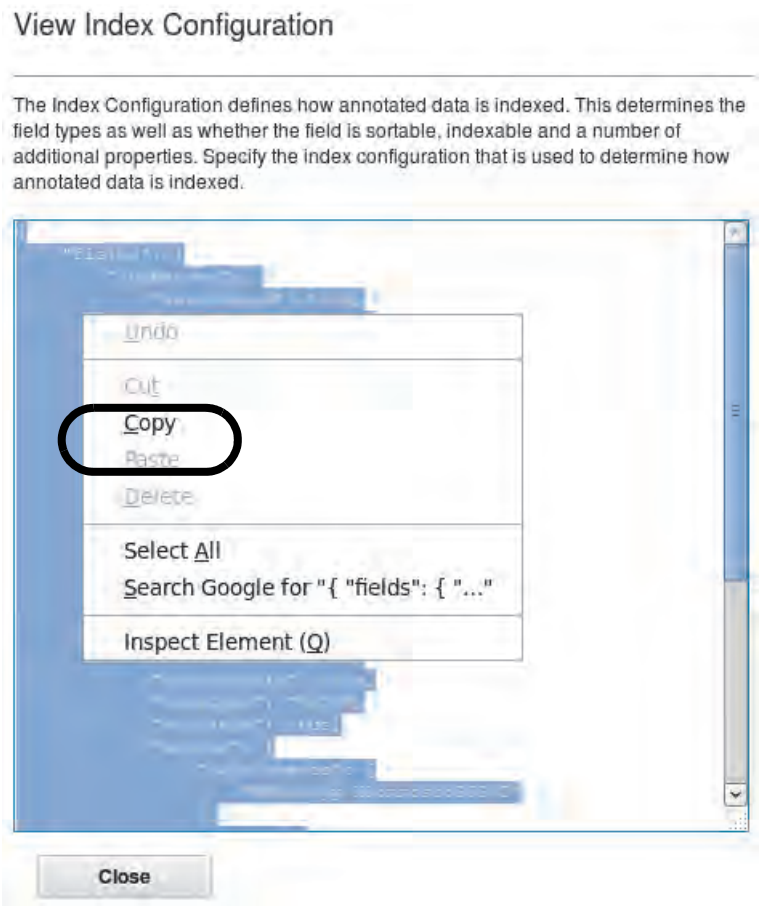
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Click **View Index Configuration**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Copy all of the text in the index configuration. Close it when you finish.



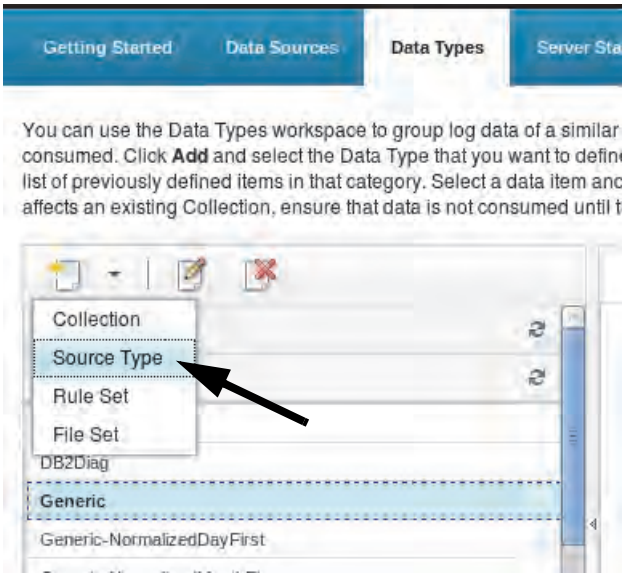
4. Create a source type name **Generic-ObjectServer-ST**. Use the values in the following table.

Field	Value
Name	Generic-ObjectServer-ST
Enable splitter	Select this option
Rule set	Generic-dateTime-Split
Enable annotator	Select this option
Rule set	Generic-Annotate
Deliver data on annotator execution failure	Leave this option clear
Edit Index Configuration	Enter the index configuration that you copied in a preceding step. Change the **dateFormats** field to "**yyyy-MM-dd'T'HH:mm:ss**"

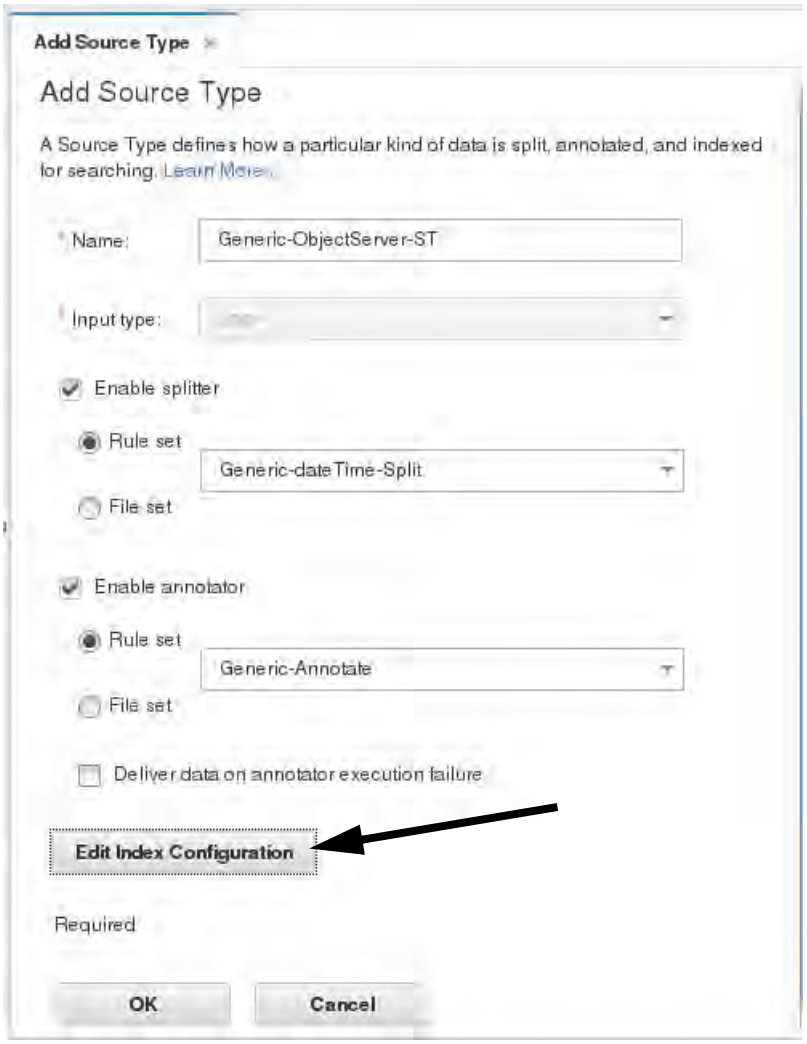
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

a. Click **Add > Source Type**.



b. Enter the values from the preceding table. Click **Edit Index Configuration**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

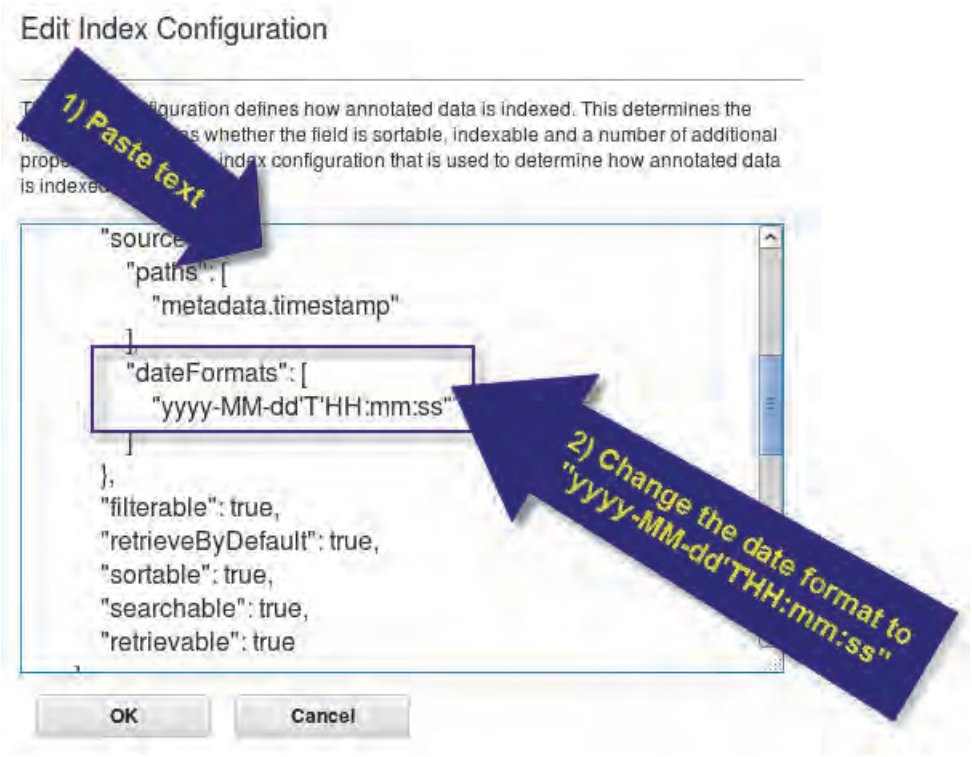
c. Change the **dateFormats** field to match the format of the OMNIbus log file.

   i. Remove all of the text from the index configuration.

   ii. Paste the index configuration that you copied from the **Generic** source type.

   iii. Change the **dateFormats** field as follows, including the quotation marks:
   "yyyy-MM-dd'T'HH:mm:ss"

   iv. Click **OK**.



d. Click **OK** to save the source type. Click **OK** again to confirm.

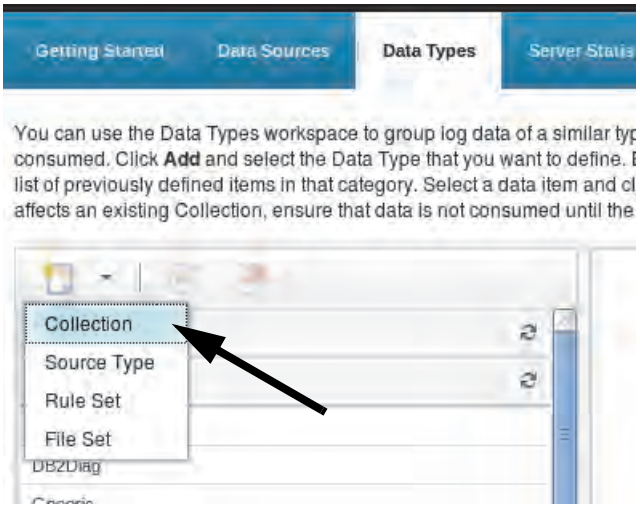
5. Create a collection named **Generic-ObjectServer-C**. Use the values in the following table.

Field	Value
Name	Generic-ObjectServer-C
Source Type	Generic-ObjectServer-ST

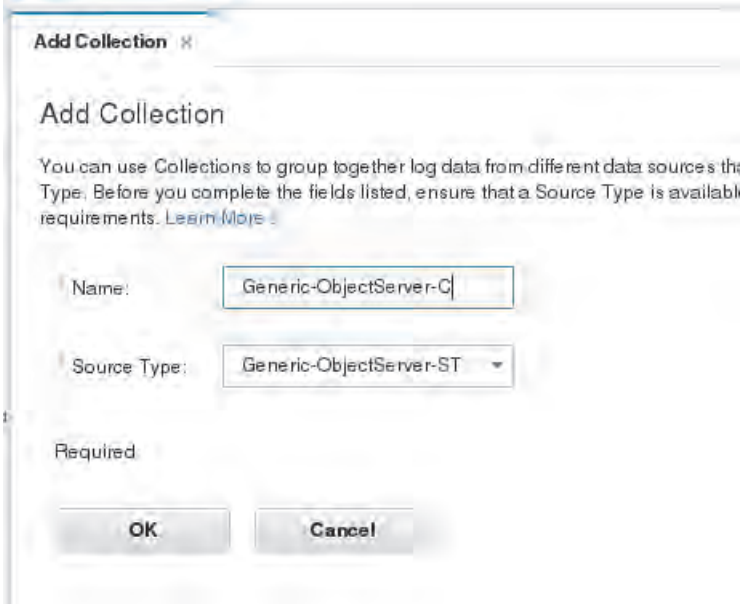
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

a. Click **Add > Collection**.



b. Enter the values from the preceding table. Click **OK**. Click **OK** to confirm.



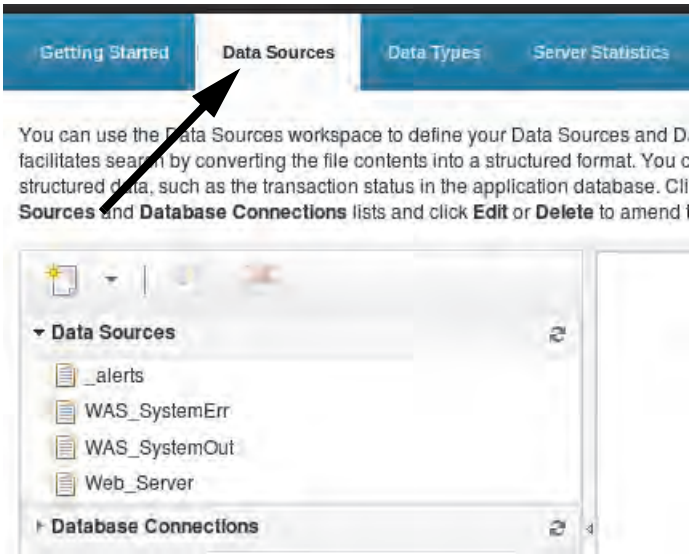
6. Create a data source named ObjectServer-Log. Use the values in the following table to complete the data source wizard.

Field	Value
Location	Select Custom
Host name	host2
File Path	`/opt/IBM/LogAnalysis/logsources/GAInsightPack/NYC_AGG_P.log`
Type	Generic-ObjectServer-ST
Collection	Generic-ObjectServer-C
Name	ObjectServer-Log

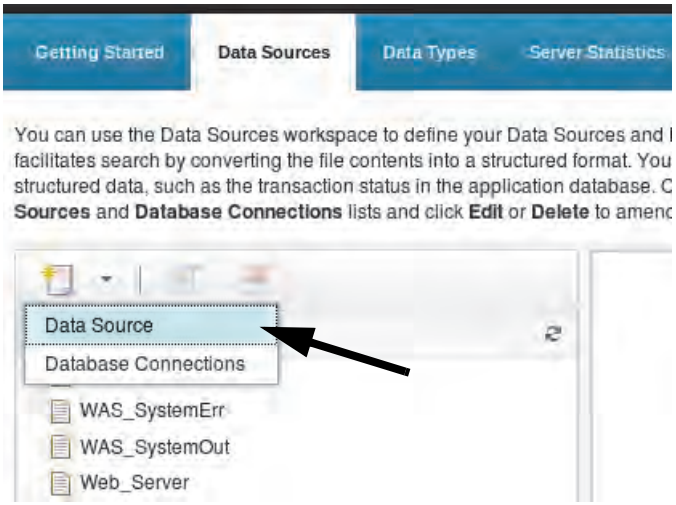
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Field	Value
Description	This source uses ObjectServer logs
Group	Leave this field blank

a. Click the **Data Sources** tab in the administration user interface. The administration user interface is in the second Firefox tab.



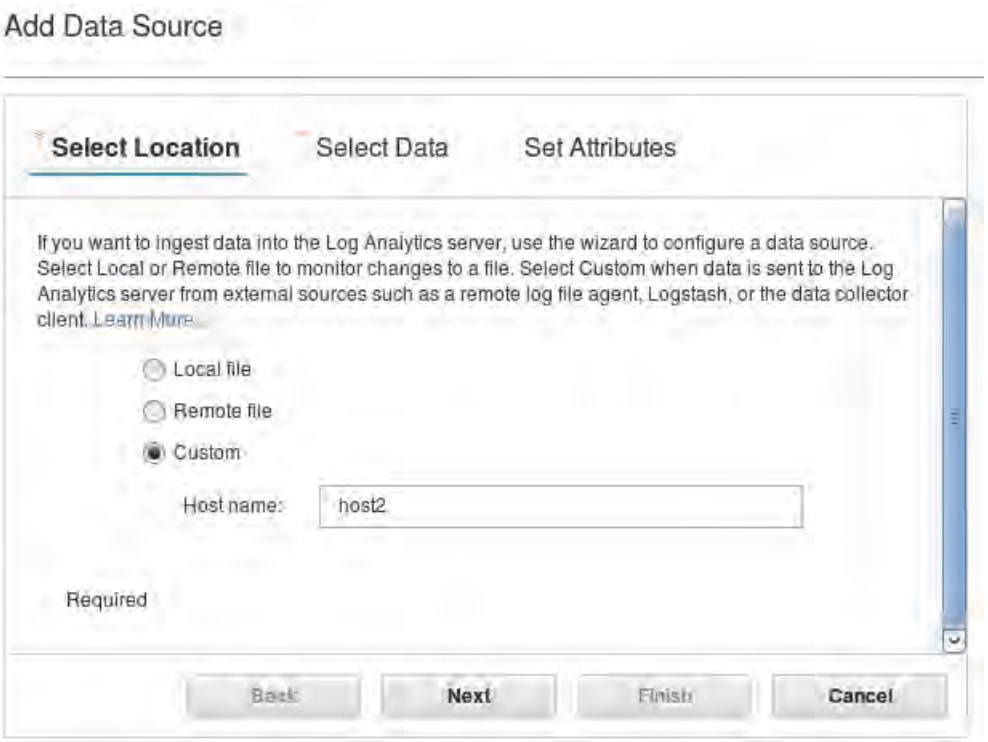
b. Click **Add > Data Source**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

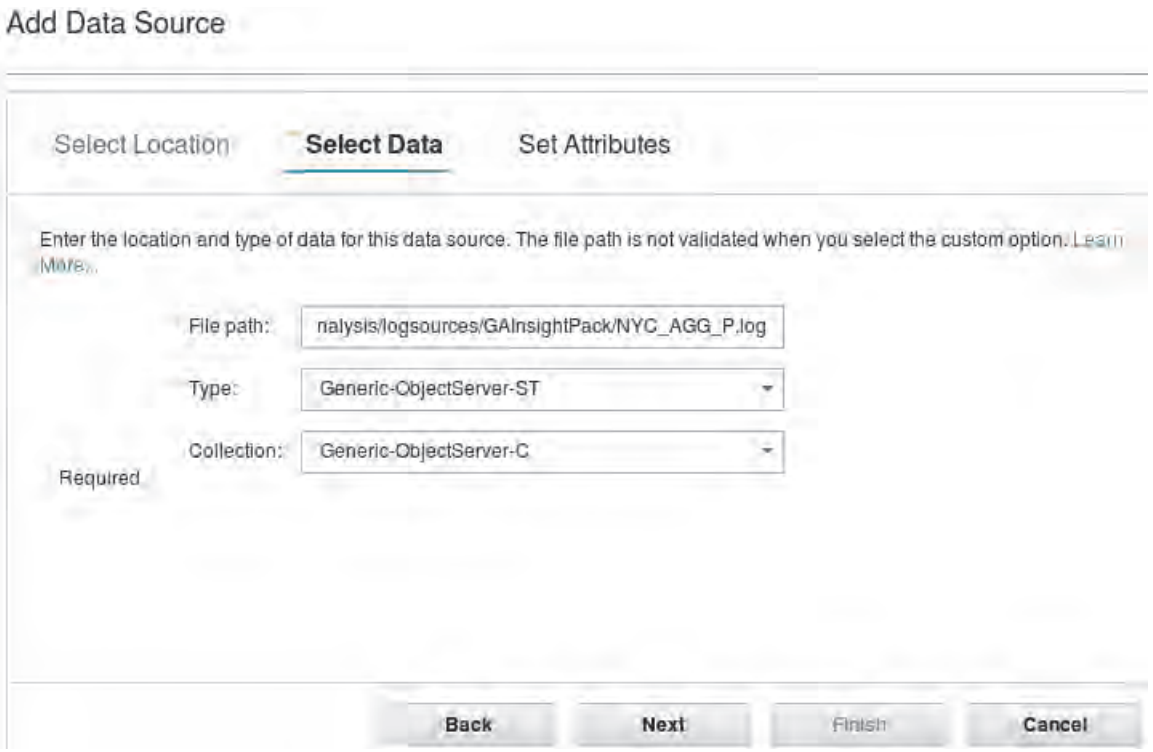
c. Select **Custom**. Enter **host2** as the **Host name** and click **Next**.



d. Enter `/opt/IBM/LogAnalysis/logsources/GAInsightPack/NYC_AGG_P.log` as the file path.

e. Select **Generic-ObjectServer-ST** as the **Type.**

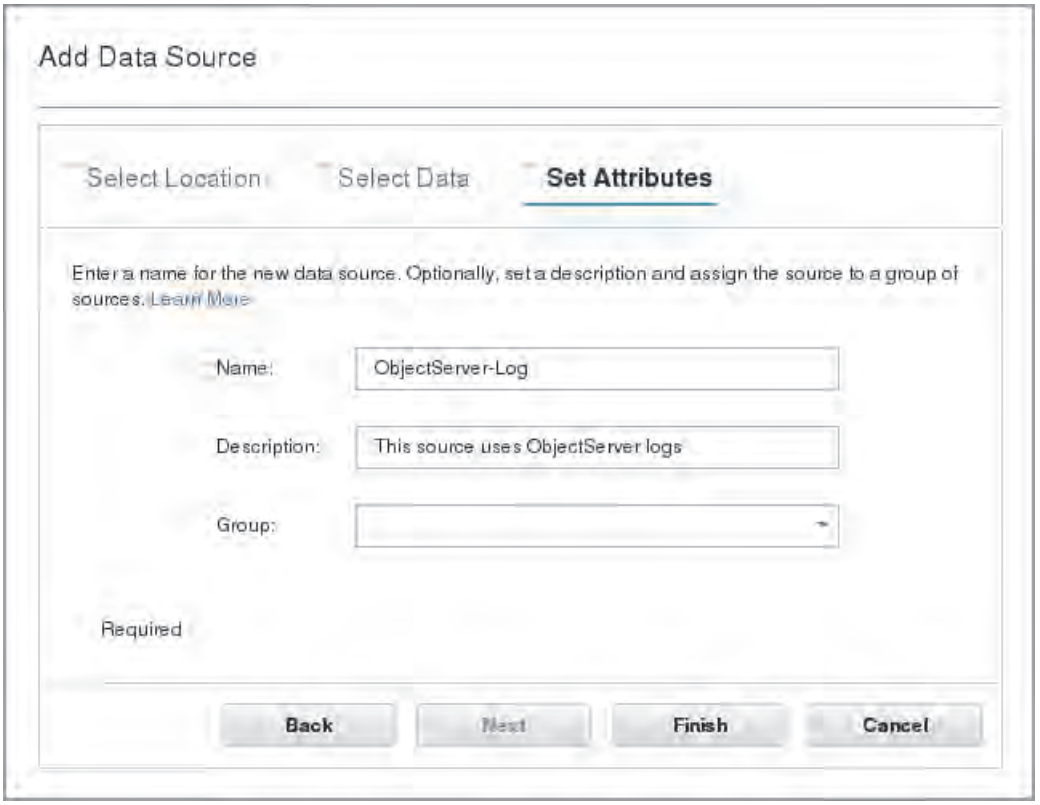
f. Select **Generic-ObjectServer-C** as the **Collection** and click **Next**.



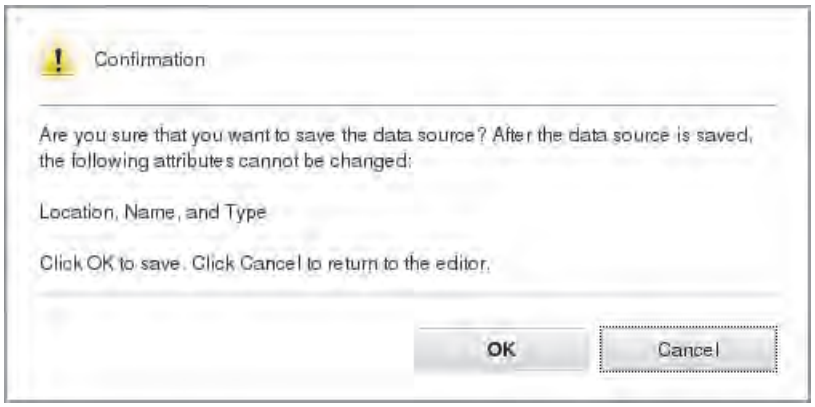
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

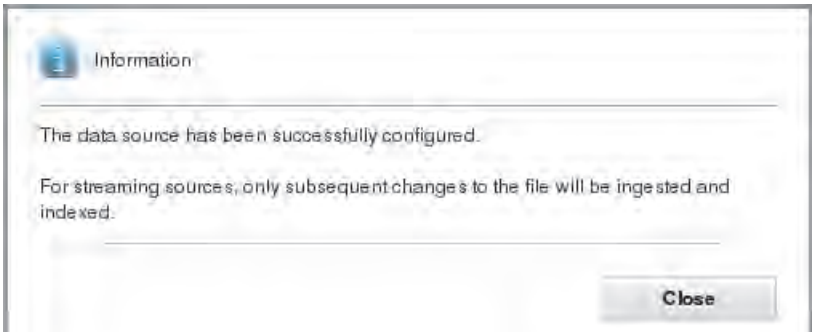
g. Enter **ObjectServer-Log** as the **Name** of the data source.

h. Enter the **Description** from the preceding table and click **Finish**.



i. Click **OK** and **Close** in the confirmation windows.





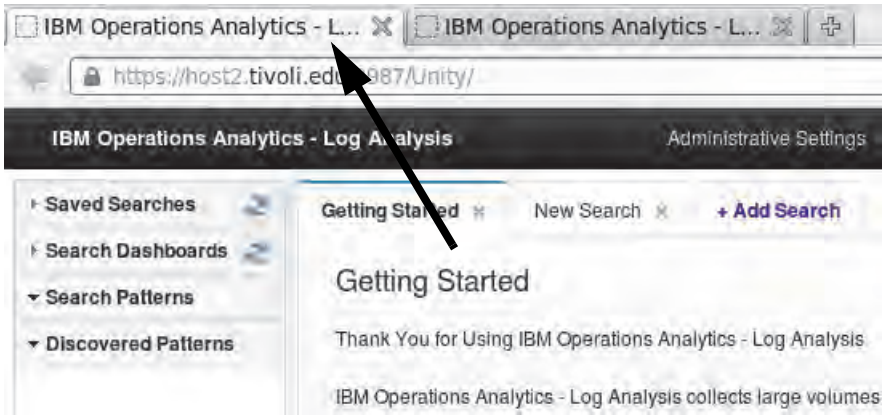
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

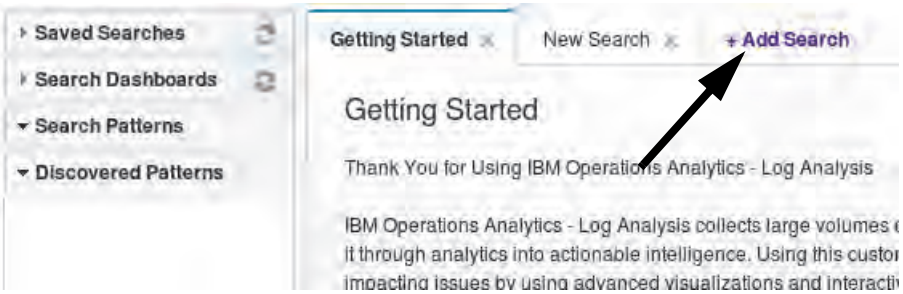
7. Run the following command to manually add some messages to the bottom of the `NYC_AGG_P.log` file. Enter the entire command on one line.

   ```
   cat /home/netcool/NYC_AGG_P.log >>
   /opt/IBM/LogAnalysis/logsources/GAInsightPack/NYC_AGG_P.log
   ```

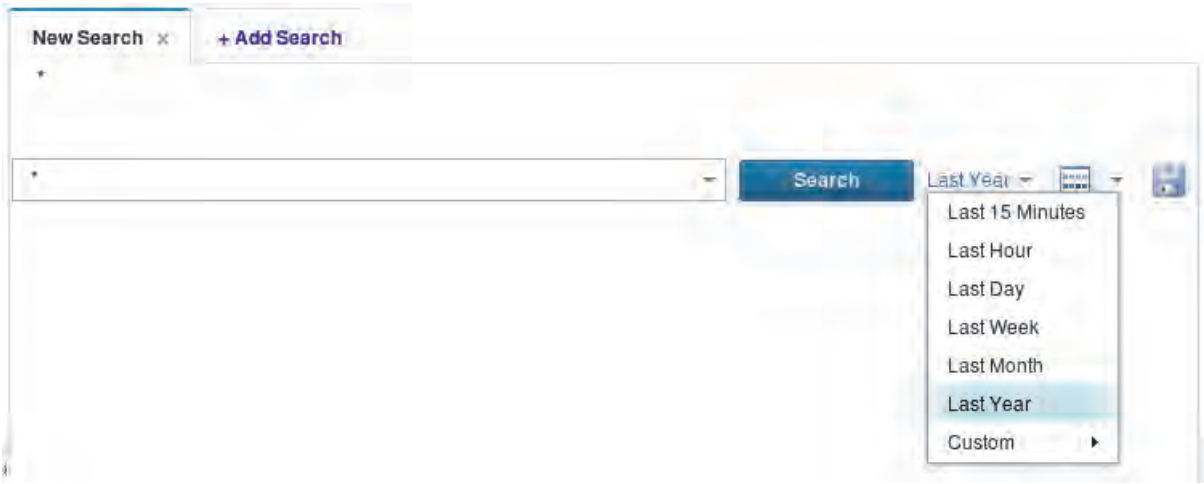
8. Return to the user interface by clicking the first Firefox tab.



9. Search through the new log and create a saved search based on this log source.
   a. Click **Add Search**.

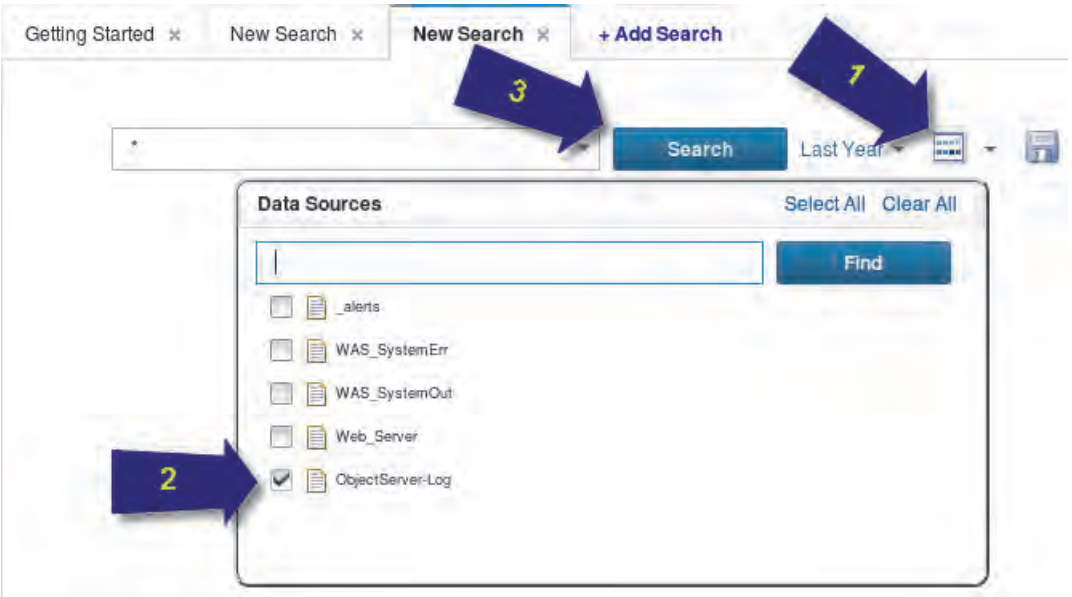


   b. Select **Last Year** as the time filter.

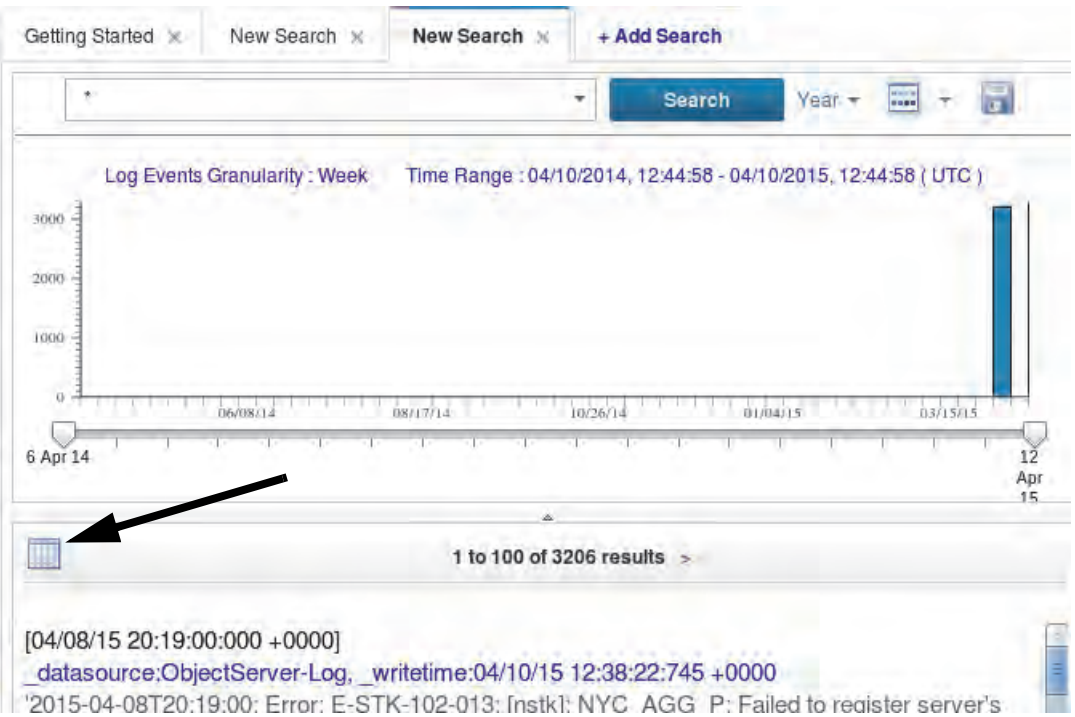


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Select only **ObjectServer-Log** as the log source.

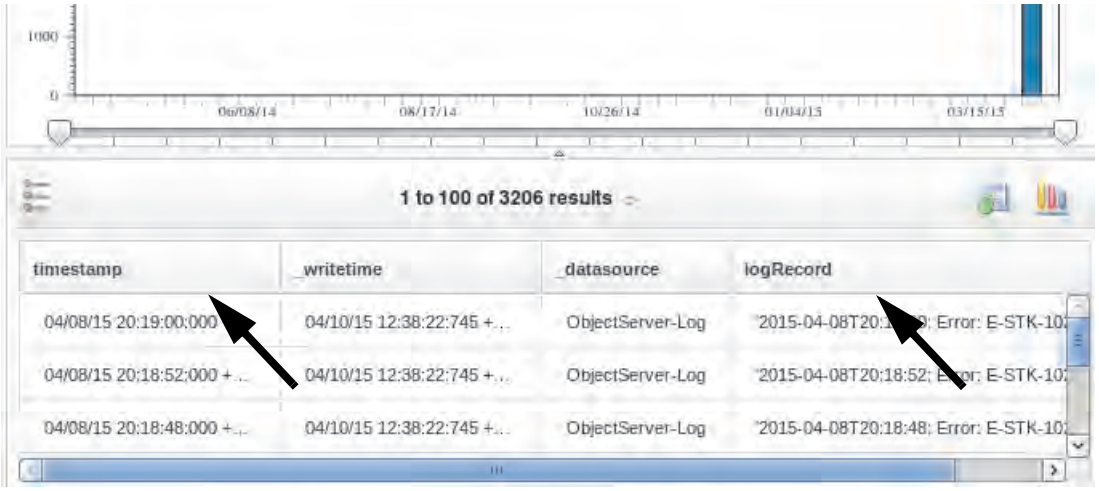


d. Click **Search**. Log events load in to the user interface. Switch to grid view.



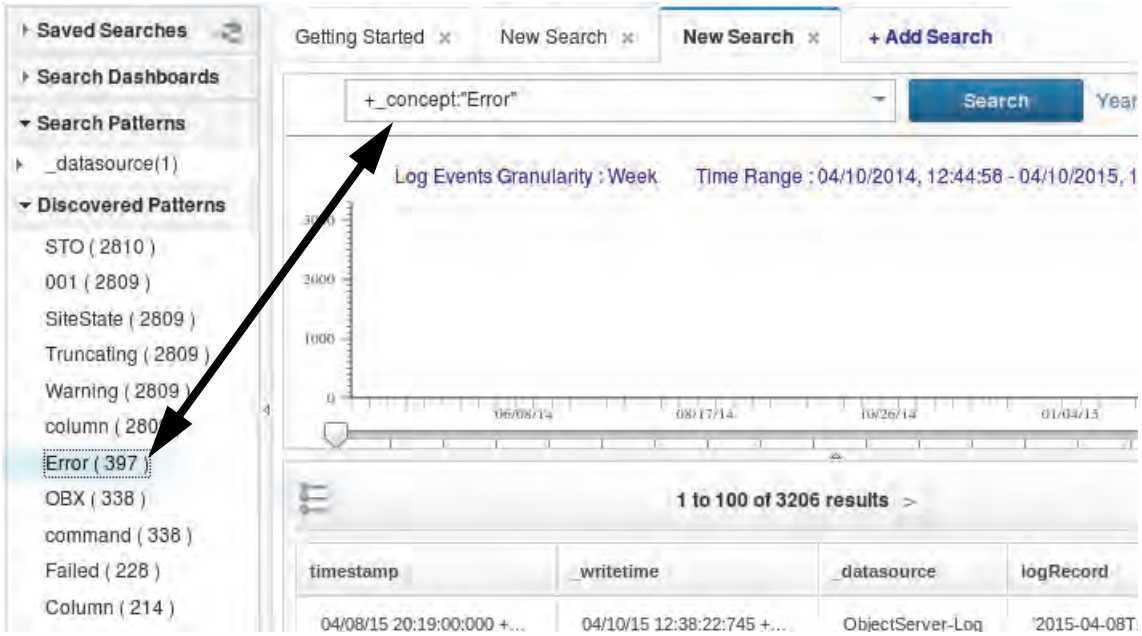
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Scroll from left to right and notice the columns with log data in them.



f. Look at the **Discovered Patterns** area on the left of the user interface. This area lists text strings that IBM Operations Analytics Log Analysis found recurring in the log file. You can use these patterns to filter log events.

g. Click **Error** in the Discovered Patterns, and click **Search**. The log file is filtered to show messages that contain the word **Error**.



h. Take some time to search through the OMNIbus log with the IBM Operations Analytics Log Analysis user interface.

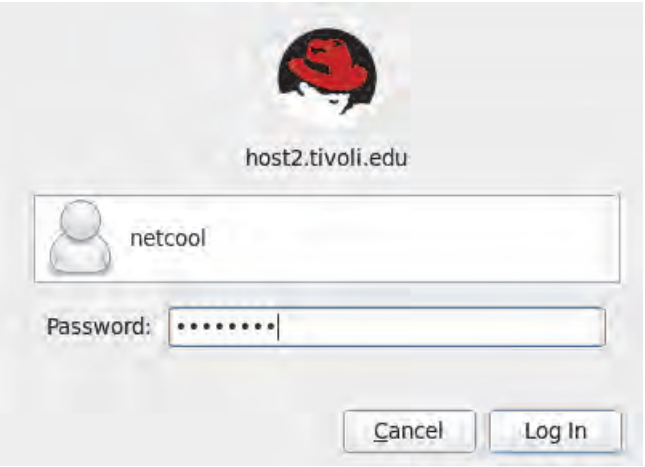
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 2 Using the DSV toolkit

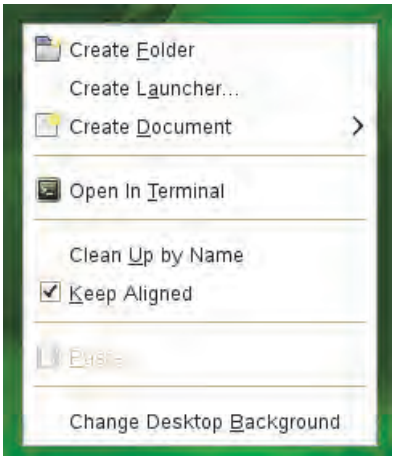
In this exercise, you use the DSV toolkit to create an Insight Pack. The log file that you build the pack for is generated by the UNIX Sar utility.

Creating the Insight Pack

1. Log in to the host2 virtual machine (host2.tivoli.edu) with the user name **netcool** and the password **object00**, if you are not already logged in.



2. Right-click the desktop and select **Open In Terminal**.



3. Use the following command to verify that you are logged in to the correct host.

```
hostname
host2.tivoli.edu
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

4. Open a sample of the log file and notice the following details about the format of the log messages. Run the following command to view a sample of the log file.
   - The log file uses a comma as the delimiting character.
   - There are nine fields, or columns, in this log.
   - The first field in this log file is a time stamp, and the format is dd-MMM-yyyy HH:mm:ss.
   - The fields in the log file contain mostly numeric values

   ```
   more /home/netcool/sar_memory/fragments/mem.log

   09-Apr-2015  02:48:05,962588,2159140,69.16,253748,813288,2096472,0,0.00
   09-Apr-2015  02:48:17,961292,2160436,69.21,253748,813340,2096472,0,0.00
   09-Apr-2015  02:48:30,962068,2159660,69.18,253748,813340,2096472,0,0.00
   09-Apr-2015  02:48:42,962068,2159660,69.18,253748,813340,2096472,0,0.00
   09-Apr-2015 02:48:54,961680,2160048,69.19,253748,813332,2096472,0,0.00
   ```

5. Run the following commands to create a new directory for your initial DSV properties file.

   ```
   mkdir /opt/IBM/LogAnalysis/unity_content/DSVToolkit_v1.1.0.3/sarMem
   cd /opt/IBM/LogAnalysis/unity_content/DSVToolkit_v1.1.0.3
   ```

6. Use the `primeProps.py` tool to generate a generic properties file for your log. Run the following command. Enter the entire command on one line.

   ```
   /usr/bin/python2.6 primeProps.py
   /opt/IBM/LogAnalysis/unity_content/DSVToolkit_v1.1.0.3/sarMem/
   sarMemProperties.properties 9
   ```

7. Edit the `sarMemProperties.properties` file that you generated. This file is a list of 10 different fields: one field for the overall log record and nine fields for each of the fields in the log file.
   a. Open the `sarMemProperties.properties` file with a text editor. This example uses `vi`.

      ```
      vi sarMem/sarMemProperties.properties
      ```

   b. Change the value of **scalaHome** to **/opt/IBM/LogAnalysis**.

   c. Change the **aqlModuleName** to **sarmemDSV9Column**.

   d. Change the name of field1 to **timestamp**. Change the **dataType** to **DATE**. Add a **dateFormat** line to the bottom of the field1 paragraph with the time stamp format you saw in the log file sample. Make field1 look like the following example.

      ```
      [field1_indexConfig]
      name: timestamp
      dataType: DATE
      retrievable: true
      retrieveByDefault: true
      sortable: true
      filterable: true
      searchable: true
      dateFormat: dd-MMM-yyyy HH:mm:ss
      ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Change fields 2 - 9 so that their names are `kbMemoryFree, kbMemoryUsed, memoryUsed, kbBuffers, kbCached, kbSwapFree, kbSwapUsed, swapUsed`.

f. Change fields 2,3,5,6,7 and 8 so that the dataType is `LONG`.

g. Change fields 4 and 9 so that the dataType is `DOUBLE`.

h. Edit fields 2 - 9 to match the following properties:

   retrievable: **true**

   retrieveByDefault: **true**

   sortable: **true**

   filterable: **false**

   searchable: **true**

i. Verify that your `sarMemProperties.properties` file looks exactly like the following example. When you finish, save and exit the file.

```
[SCALA_server]
scalaHome: /opt/IBM/LogAnalysis

[DSV_file]
delimiter: ,
totalColumns: 9
aqlModuleName: sarmemDSV9Column
version: 1.0.0.0

[field0_indexConfig]
name: logRecord
dataType: TEXT
retrievable: true
retrieveByDefault: true
sortable: false
filterable: false
searchable: true
path_1: content.text
combine: FIRST

[field1_indexConfig]
name: timestamp
dataType: DATE
retrievable: true
retrieveByDefault: true
sortable: true
filterable: true
searchable: true
dateFormat: dd-MMM-yyyy HH:mm:ss

[field2_indexConfig]
```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
name: kbMemoryFree
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field3_indexConfig]
name: kbMemoryUsed
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field4_indexConfig]
name: memoryUsed
dataType: DOUBLE
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field5_indexConfig]
name: kbBuffers
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field6_indexConfig]
name: kbCached
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field7_indexConfig]
name: kbSwapFree
dataType: LONG
retrievable: true
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field8_indexConfig]
name: kbSwapUsed
dataType: LONG
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true

[field9_indexConfig]
name: swapUsed
dataType: DOUBLE
retrievable: true
retrieveByDefault: true
sortable: true
filterable: false
searchable: true
```

8. Create the insight pack with the `dsvGen.py` tool. When you run this tool, it generates an Insight Pack based on the configuration you added in the properties file.
   a. Verify that you are in the `dsvGen.py` tool directory.

      ```
      cd /opt/IBM/LogAnalysis/unity_content/DSVToolkit_v1.1.0.3/
      ```

   b. Run the following command to create the Insight Pack. Enter the command on a single line.

      ```
      /usr/bin/python2.6 dsvGen.py sarMem/sarMemProperties.properties  -o -d -u
      unityadmin -p unityadmin
      ```

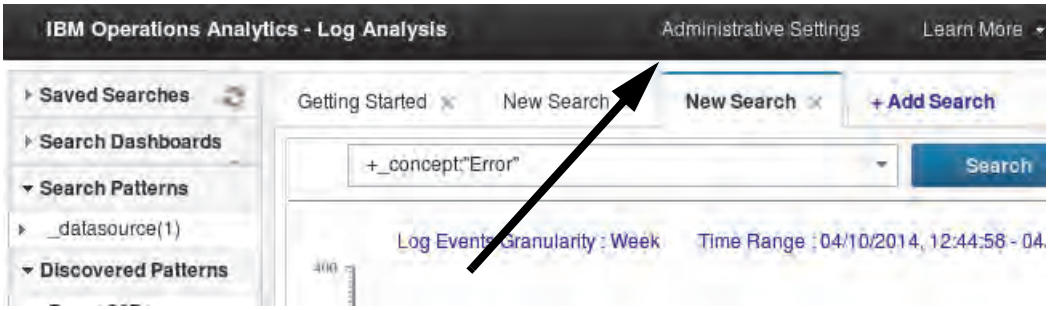
   c. Enter **y** when you are prompted to restart the log file agent.

      ```
      Deploying/undeploying Log File Adapter configuration files requires the LFA
      to to stopped before and restarted after. Do you want to continue (y/n)?
      y
      ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Testing the Insight Pack

9. Open the administration user interface. Click **Administrative Settings**. The administration user interface opens in a new Firefox tab.

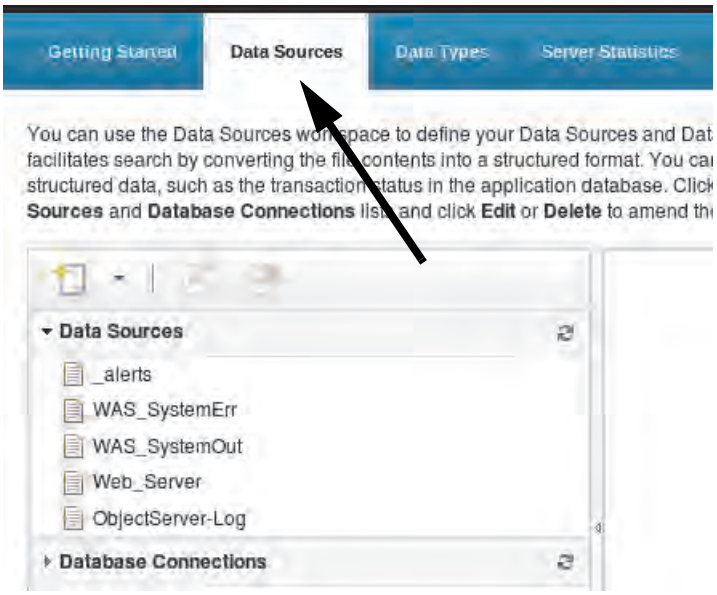


10. Create a data source named **Sar_Memory**. Use the values in the following table to complete the data source wizard.

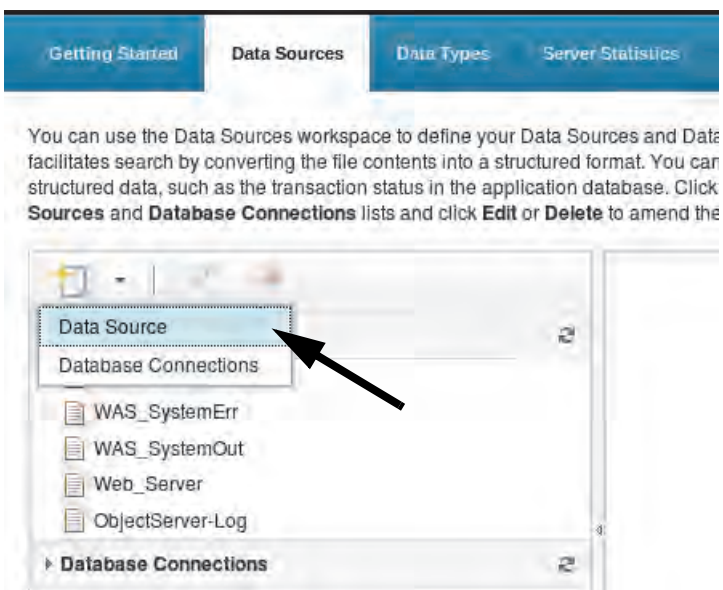
Field	Value
Location	Select Custom
Host name	host2
File Path	`/opt/IBM/LogAnalysis/logsources/sarmemDSV9ColumnInsightPack/mem.log`
Type	sarmemDSV9Column
Collection	sarmemDSV9Column-Collection
Name	Sar_Memory
Description	This source uses sysstat measurements
Group	Leave this field blank

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

a. Click the **Data Sources** tab in the administration user interface. The administration user interface is in the second Firefox tab.



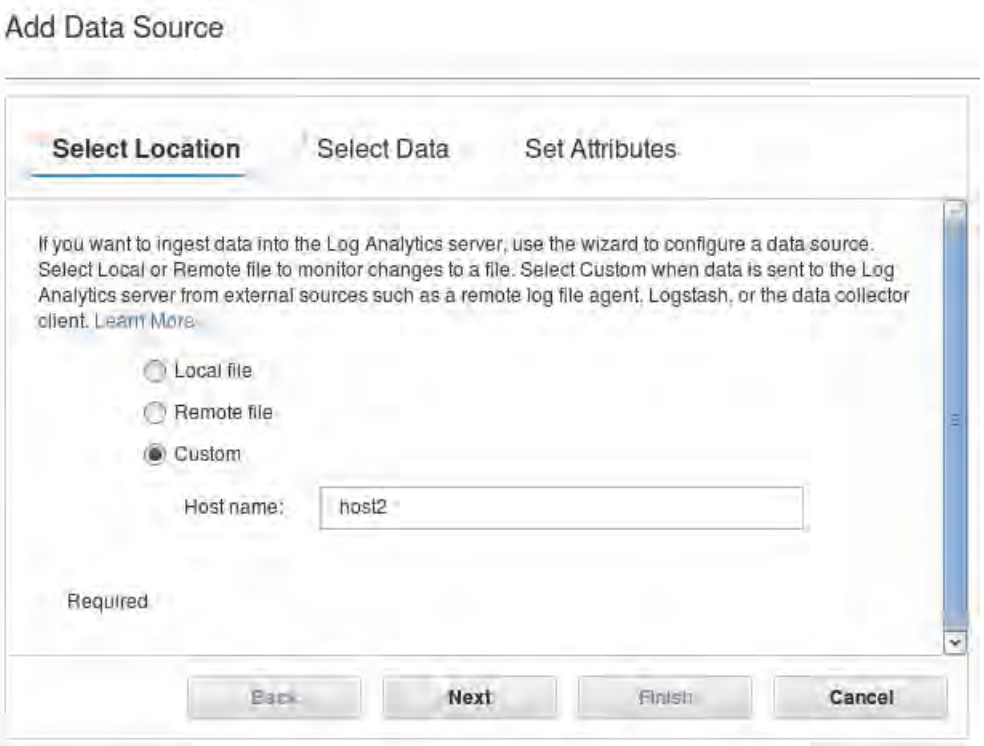
b. Click **Add > Data Source**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Select **Custom**. Enter **host2** as the **Host name** and click **Next**.



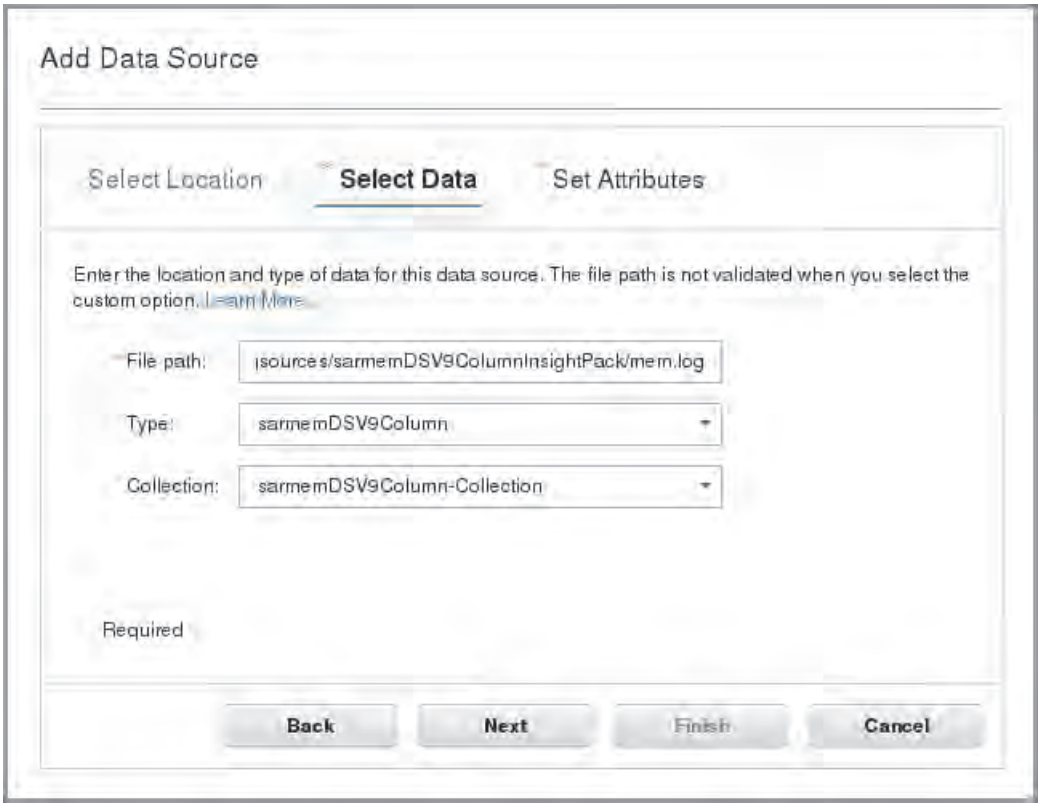
d. Enter `/opt/IBM/LogAnalysis/logsources/sarmemDSV9ColumnInsightPack/mem.log` as the file path.

Important: Ensure that you enter the path correctly.

e. Select **sarmemDSV9Column** as the **Type**.

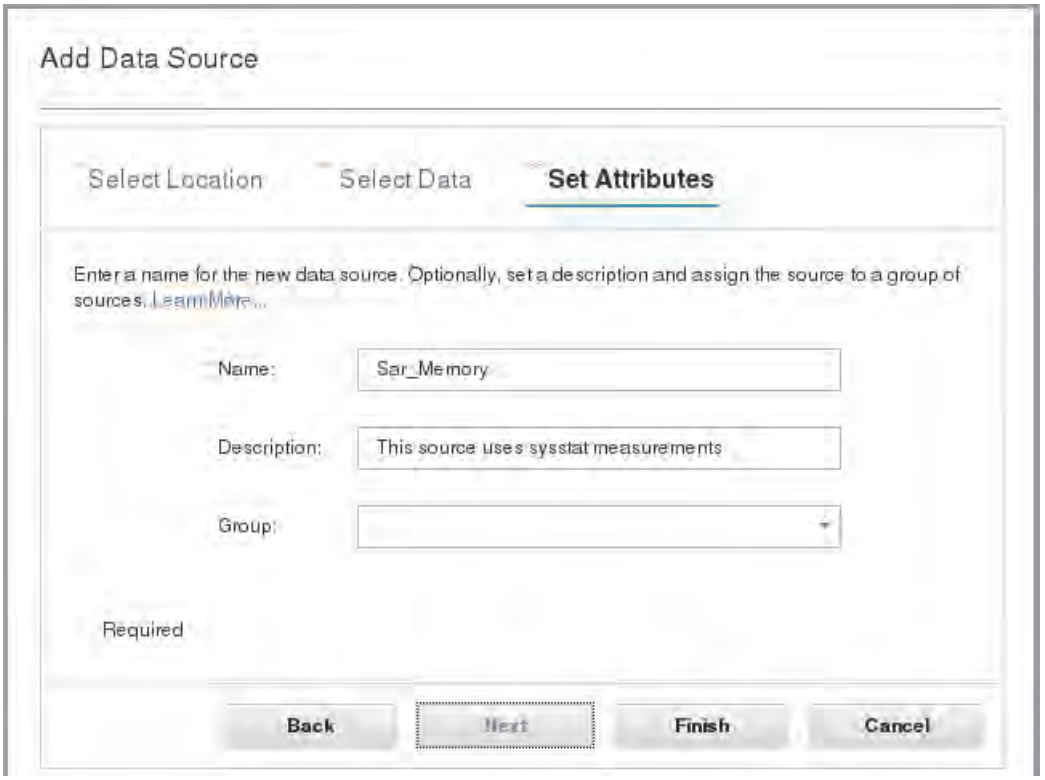
© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

f. Select **sarmemDSV9Column-Collection** as the **Collection** and click **Next**.



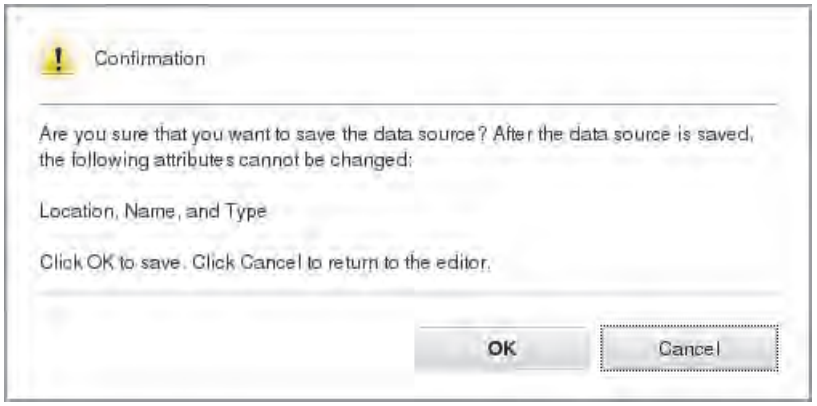
g. Enter `Sar_Memory` as the **Name** of the data source.

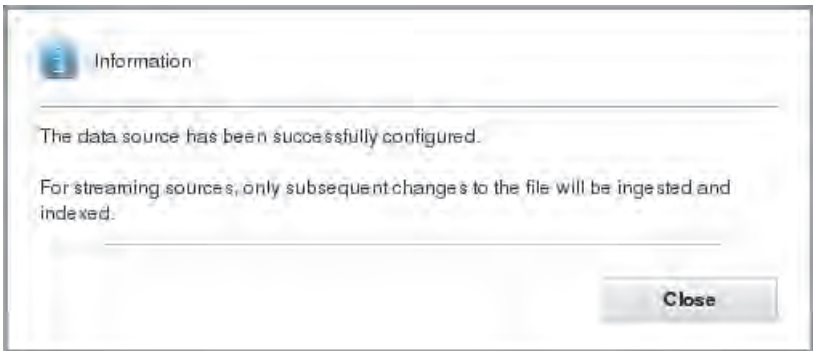
h. Enter the **Description** from the preceding table and click **Finish**.



Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

i. Click **OK** and **Close** in the confirmation windows.



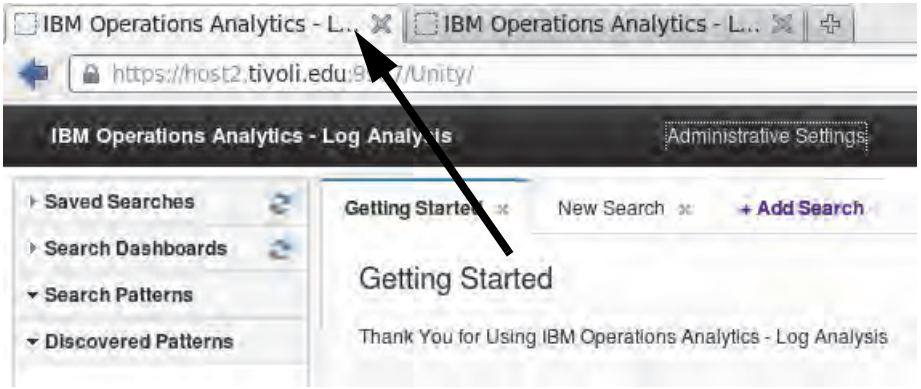


The sar memory log file for this lab is generated by a script.

11. Return to the terminal window. Run the following command to generate events in the `mem.log` file.

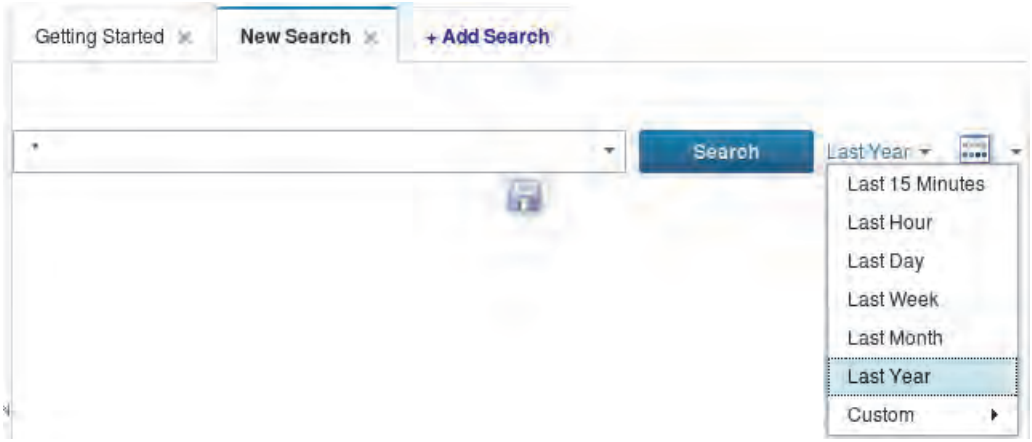
    `/home/netcool/sar_memory/fragments/Generate_sarMemory.sh`

12. Return to the search interface by clicking the first Firefox tab.

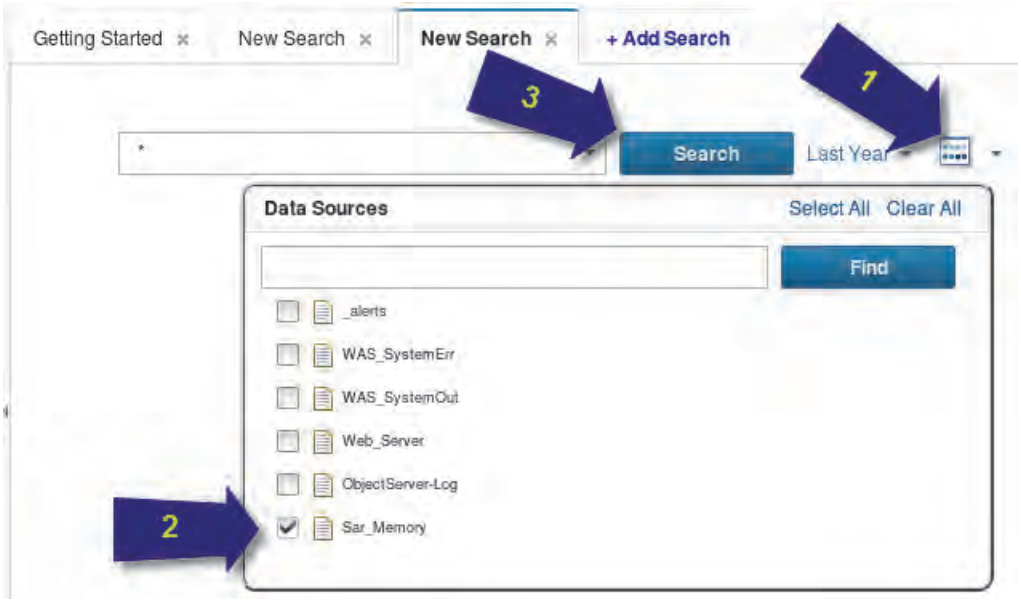


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

13. Search through the new log and verify that the log file was processed successfully.
    a. Click the **Add Search** tab. Select **Last Year** as the time filter.



    b. Select only **Sar_Memory** as the data source. Click **Search**.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Log events load in to the user interface. Click the **Grid View** button.

d. Scroll left and right to view the columns. Verify that each of the fields you configured for the log file are now columns in the user interface. Users can now search through this log, create charts and dashboards, and so on.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

3 Troubleshooting exercises

There are no student exercises for this unit.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

4 Alerts exercises

In this exercise, you configure the product to generate alerts from conditions in log files.

Exercise 1 Creating alert actions

In this exercise, you create two alert actions. One action adds an entry to a log file and the other action sends an email notification.

Index alert action

When a condition is detected in a log file, the product automatically indexes the occurrence of the alert. Users can query the indexed alerts in the search interface. This action is enabled by default.

1. Look at the index alert action with the `alerts.sh` utility.
   a. Change to the alerts subdirectory:

      ```
      cd /opt/IBM/LogAnalysis/utilities/alerts
      ```

   b. Run the following command to show all alert actions.

      ```
      ./alerts.sh -getAlertAction
      ```

   The index alert action is enabled by default. You use this action in alert conditions later in this exercise.

   ```
   Name: index
   Label: Index
   Description: Alert action implementation that indexes triggered alerts
   Template: index
   Enabled: true
   ```

Log alert action

2. Create an alert action that adds a message to a log file.
   a. Verify that you are in the alerts subdirectory.

      ```
      cd /opt/IBM/LogAnalysis/utilities/alerts
      ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Make a copy of the `logAlertAction.json` file. Name the copy `LAB_logAlertAction.json`.

```
cp logAlertAction.json LAB_logAlertAction.json
```

c. Open the `LAB_logAlertAction.json` file in a text editor. Edit the following three fields in the file. Make the `LAB_logAlertAction.json` file match the following example.

```
vi LAB_logAlertAction.json

{
  "name": "LAB-log-action",
  "description": "This action adds a message to a log file",
  "alertActionTemplateName": "log",
  "parameterValues": {
    "filePath": "/tmp/LAB_alert.log"
  }
}
```

d. Save and close the file when you are done.

3. Use the `alerts.sh` utility to create the new alert action.

a. Run the following command to create the alert action.

```
./alerts.sh -createAlertAction LAB_logAlertAction.json
```

b. Run the following command to verify that the alert action was created.

```
./alerts.sh -getAlertAction
...
Name: LAB-log-action
Description: This action adds a message to a log file
Template: log
Parameter Values:
    filePath: /tmp/LAB_alert.log
Enabled: true
```

Email alert action

4. Create an alert action that sends an email to the **netcool** user.

a. Make a copy of the `emailAlertAction.json` file. Name the copy `LAB_emailAlertAction.json`.

```
cp emailAlertAction.json LAB_emailAlertAction.json
```

b. Open the `LAB_emailAlertAction.json` file in a text editor. Edit the following six fields in the file. Make the `LAB_emailAlertAction.json` file match the following example.

```
vi LAB_emailAlertAction.json

{
  "name": "LAB-email-action",
  "description": "This action sends an e-mail to netcool",
```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
  "alertActionTemplateName": "email",
  "parameterValues": {
    "smtpMailServer": "localhost",
    "secure": false,
    "from": "from@ibm.com",
    "to": ["netcool"],
    "cc": [],
    "bcc": [],
    "subjectPrefix": "An alert from a log record requires your attention",
    "header": "Dear User,",
    "footer": "*** This is a system generated e-mail, please do not reply to
this e-mail ***\n",
    "attachLogRecordAnnotations": true,
  }
}
```

c. Save and close the file when you are done.

5. Use the `alerts.sh` utility to create the new alert action.

   a. Run the following command to create the alert action.

```
./alerts.sh -createAlertAction LAB_emailAlertAction.json
```

   b. Run the following command to verify that the alert action was created.

```
./alerts.sh -getAlertAction
...
Name: LAB-email-action
Description: This action sends an e-mail to netcool
Template: email
Parameter Values:
    to: [netcool]
    footer: *** This is a system generated e-mail, please do not reply to
this e-mail ***

    attachLogRecordAnnotations: true
    secure: false
    bcc: []
    subjectPrefix: An alert from a log record requires your attention
    from: from@ibm.com
    header: Dear User,
    cc: []
    smtpMailServer: localhost
Enabled: true
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 2 Creating base conditions

In this exercise, you create base conditions. These conditions use queries to detect text patterns in data sources.

WebSphere SystemOut log base condition

1. Create a base condition that queries the WAS_SystemOut data source and uses all of the actions you configured in the preceding exercise. Query for the text `java.sql.SQLException` in the WebSphere SystemOut log.
   a. Verify that you are in the alerts subdirectory.

      ```
      cd /opt/IBM/LogAnalysis/utilities/alerts
      ```

   b. Make a copy of the `queryBaseCondition.json` file. Name the copy `WASOUT_queryBaseCondition.json`.

      ```
      cp queryBaseCondition.json WASOUT_queryBaseCondition.json
      ```

   c. Open the `WASOUT_queryBaseCondition.json` file in a text editor. Edit the following five fields in the file. Make the `WASOUT_queryBaseCondition.json` file match the following example.

      ```
      vi WASOUT_queryBaseCondition.json
      ```

      ```
      {
        "name": "WASOUT-base-condition",
        "description": "This condition detects java sql exceptions",
        "baseConditionTemplateName": "query",
        "datasourceName": "WAS_SystemOut",
        "parameterValues": { "query" :
      "+javaException:java.sql.SQLException"},
        "actions": ["index","LAB-log-action","LAB-email-action"]
      }
      ```

   d. Save and close the file when you are done.

2. Use the `alerts.sh` utility to create the new condition.
   a. Run the following command to create the condition.

      ```
      ./alerts.sh -createBaseCondition WASOUT_queryBaseCondition.json
      ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Run the following command to verify that the condition was created.

```
./alerts.sh -getBaseCondition
...
Name: WASOUT-base-condition
Description: This condition detects java sql exceptions
Template: query
Datasource: WAS_SystemOut
Parameter Values:
  query: +javaException:java.sql.SQLException
Actions: [LAB-email-action, LAB-log-action, index]
Enabled: true
```

WebSphere SystemErr log base condition

3. Create a base condition that queries the WAS_SystemErr data source and uses all of the actions that you configured earlier. Query for the text `java.sql.SQLException` in the WebSphere SystemErr log. This condition is identical to the `WASOUT_queryBaseCondition.json` you just created, except that it uses a different data source (WAS_SystemErr).

   a. Verify that you are in the alerts subdirectory.

   ```
   cd /opt/IBM/LogAnalysis/utilities/alerts
   ```

   b. Make a copy of the `WASOUT_queryBaseCondition.json` file. Name the copy `WASERR_queryBaseCondition.json`.

   ```
   cp WASOUT_queryBaseCondition.json WASERR_queryBaseCondition.json
   ```

   c. Open the `WASERR_queryBaseCondition.json` file in a text editor. Edit the following two fields in the file. Make the `WASERR_queryBaseCondition.json` file match the following example.

   ```
   vi WASERR_queryBaseCondition.json

   {
     "name": "WASERR-base-condition",
     "description": "This condition detects java sql exceptions",
     "baseConditionTemplateName": "query",
     "datasourceName": "WAS_SystemErr",
     "parameterValues": { "query" : "+javaException:java.sql.SQLException"},
     "actions": ["index","LAB-log-action","LAB-email-action"]
   }
   ```

   d. Save and close the file when you are done.

4. Use the `alerts.sh` utility to create the new condition.

   a. Run the following command to create the condition.

   ```
   ./alerts.sh -createBaseCondition WASERR_queryBaseCondition.json
   ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Run the following command to verify that the condition was created.

```
./alerts.sh -getBaseCondition
...
Name: WASERR-base-condition
Description: This condition detects java sql exceptions
Template: query
Datasource: WAS_SystemErr
Parameter Values:
  query: +javaException:java.sql.SQLException
Actions: [LAB-email-action, LAB-log-action, index]
Enabled: true
```

Web access log base condition

5. Create a base condition that queries the Web_Server data source and uses all of the actions you configured earlier. Query for server response times that are over 30,000 microseconds.

   a. Verify that you are in the alerts subdirectory.

   ```
   cd /opt/IBM/LogAnalysis/utilities/alerts
   ```

   b. Make a copy of the `queryBaseCondition.json` file. Name the copy `WEB_queryBaseCondition.json`.

   ```
   cp queryBaseCondition.json WEB_queryBaseCondition.json
   ```

   c. Open the `WEB_queryBaseCondition.json` file in a text editor. Edit the following five fields in the file. Make the `WEB_queryBaseCondition.json` file match the following example.

   ```
   vi WEB_queryBaseCondition.json

   {
     "name": "WEB-base-condition",
     "description": "This condition detects high response times",
     "baseConditionTemplateName": "query",
     "datasourceName": "Web_Server",
     "parameterValues": { "query" : "+responseTime:[30000 TO *]"},
     "actions": ["index","LAB-log-action","LAB-email-action"]
   }
   ```

   d. Save and close the file when you are done.

6. Use the `alerts.sh` utility to create the new condition.

   a. Run the following command to create the condition.

   ```
   ./alerts.sh -createBaseCondition WEB_queryBaseCondition.json
   ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Run the following command to verify that the condition was created.

```
./alerts.sh -getBaseCondition
...
Name: WEB-base-condition
Description: This condition detects high response times
Template: query
Datasource: Web_Server
Parameter Values:
  query: +responseTime:[30000 TO *]
Actions: [LAB-email-action, LAB-log-action, index]
Enabled: true
```

Exercise 3 Testing base conditions

In this exercise, you test the alert actions and conditions you created in a preceding exercise.

1. Run the following commands to add more messages to the WAS and web server log files.

```
/software/log_samples/scripts/WAS_Logs.sh
/software/log_samples/scripts/Web_Logs.sh
```

2. Open the `/tmp/LAB_alert.log` file. Notice the alerts in this log file that were triggered by the WAS and the Web_Server conditions.

```
more /tmp/LAB_alert.log

{"conditionName":"WASOUT-base-condition","conditionType":"base","datasources":[
"WAS_SystemOut"],"triggeringInput":{"datasourceHostname":["host2.tivoli.edu"],"
threadID":["00000000"],"packageName":["com.ibm.tivoli.ncw.datasource"],"excepti
onClassName":["ConnectionPool"],"severity":["E"],"exceptionMethodName":["create
Connection"],"timestamp":[1426946599768],"_writetime":[1429035550400]
...
{"conditionName":"WASERR-base-condition","conditionType":"base","datasources":[
"WAS_SystemErr"],"triggeringInput":{"datasourceHostname":["host2.tivoli.edu"],"
threadID":["0000000e"],"packageName":["com.ibm.tivoli.ncw.ncosvmm.sql"],"except
ionClassName":["FailBackDataSourceSelector"],"severity":["R"],"exceptionMethodN
ame":["getDataSource"],"timestamp":[1427037406733],"_writetime":[1429035560583]
...
{"conditionName":"WEB-base-condition","conditionType":"base","datasources":["We
b_Server"],"triggeringInput":{"bytes":["3409"],"agent":["curl\/7.21.3
(x86_64-unknown-linux-gnu) libcurl\/7.21.3 OpenSSL\/1.0.0
zlib\/1.2.3"],"timestamp":[1426794280000],"response":["200"],"webServerType":["
Apache\/IHS"],"referrer":["-"],"ident":["-"],"verb":["GET"],"request":["GET
\/daytrader\/app?action=sell&holdingID=5015 HTTP\/1.1"]
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

3. Check the mail for the **netcool** user. Notice the email notifications that were triggered by the WAS and the Web_Server conditions.
   a. Run the following command to check the mail for the **netcool** user.

```
mail

>U  1 from@ibm.com          Tue Apr 14 18:19 251/12689 "An alert from a log
record requires your attention  [Alert condition WASOUT-base-condition
trigger"
 U  2 from@ibm.com          Tue Apr 14 18:19 253/12699 "An alert from a log
record requires your attention  [Alert condition WASOUT-base-condition
trigger"
 U  3 from@ibm.com          Tue Apr 14 18:19 234/12740 "An alert from a log
record requires your attention  [Alert condition WASERR-base-condition
trigger"
 U  4 from@ibm.com          Tue Apr 14 18:19 234/12741 "An alert from a log
record requires your attention  [Alert condition WASERR-base-condition
trigger"
 U  5 from@ibm.com          Tue Apr 14 18:19 234/12739 "An alert from a log
record requires your attention  [Alert condition WASERR-base-condition
trigger"
 U  6 from@ibm.com          Tue Apr 14 18:20  76/2163  "An alert from a log
record requires your attention  [Alert condition WEB-base-condition
triggered]"
 U  7 from@ibm.com          Tue Apr 14 18:20  76/2192  "An alert from a log
record requires your attention  [Alert condition WEB-base-condition
triggered]"
 U  8 from@ibm.com          Tue Apr 14 18:20  76/2599  "An alert from a log
record requires your attention  [Alert condition WEB-base-condition
triggered]"
...
```

   b. Run a command like the following example to delete all mail messages.

```
& del 1-12
```

   c. Quit the mail program.

```
& quit
```

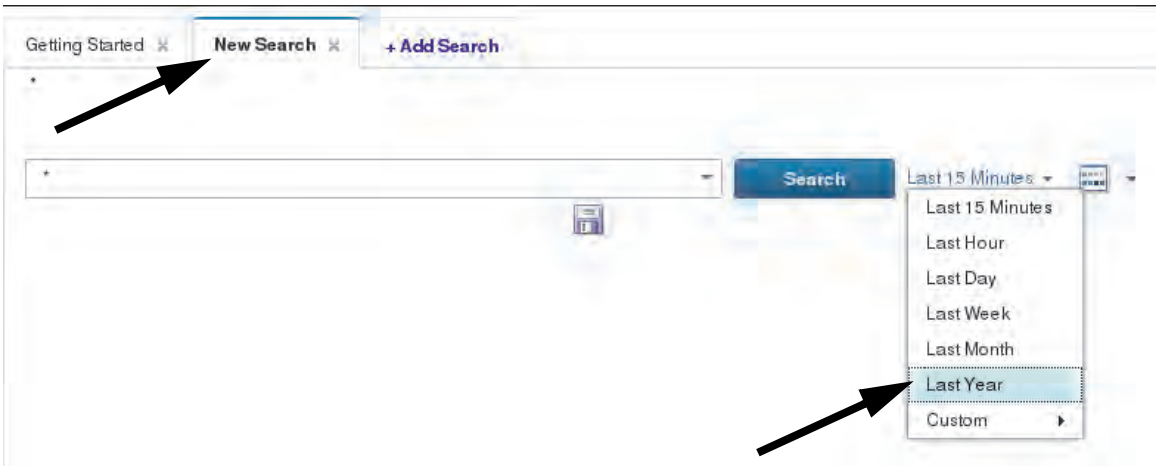
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

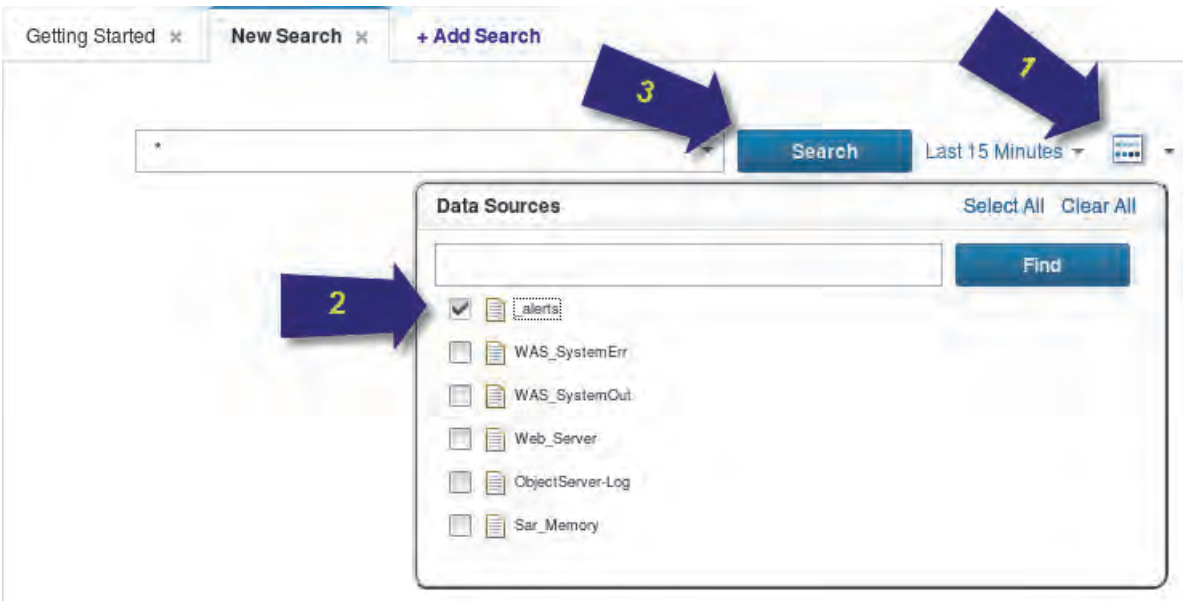
4. Open a Firefox browser and search for the log alerts.
   a. Open a Firefox browser and browse to the following address. Log in with the user name **unityadmin** and the password **unityadmin**.

      `https://host2.tivoli.edu:9987/Unity`

   b. Click the **New Search** tab. Select **Last Year** as the time filter.

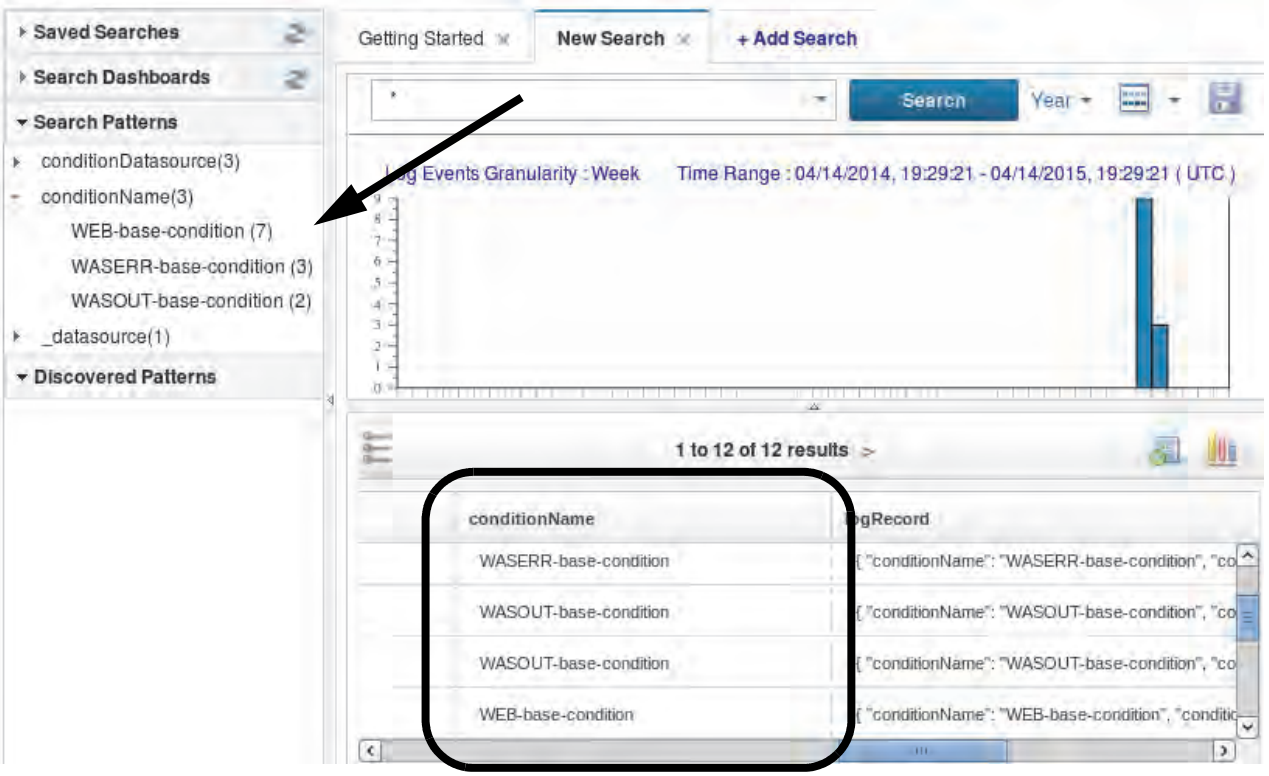


   c. Select only **_alerts** as the log source. Click **Search**.



   Indexed alerts load in to the user interface. Notice the alerts that were triggered by the WAS and the Web_Server conditions.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.



Exercise 4 Creating composite conditions

In this exercise, you create composite conditions. These conditions accept input from base conditions.

WebSphere multi-condition-window composite condition

1. Create a composite condition that triggers an alert when the text `java.sql.SQLException` occurs in the WAS_SystemOut ***and*** the WAS_SystemErr data sources within a 90-second window. Use the two WAS base conditions that you created in a preceding exercise. Use all of the actions that you configured earlier.
   a. Verify that you are in the alerts subdirectory.

      ```
      cd /opt/IBM/LogAnalysis/utilities/alerts
      ```

   b. Make a copy of the `multiConditionWindow.json` file. Name the copy `WAS_multiConditionWindow.json`.

      ```
      cp multiConditionWindow.json WAS_multiConditionWindow.json
      ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Open the `WAS_multiConditionWindow.json` file in a text editor. Edit the following five fields in the file. Make the `WAS_multiConditionWindow.json` file match the following example.

```
vi WAS_multiConditionWindow.json

{
  "name": "WAS-multi-condition",
  "description": "This condition detects java sql exceptions in two WAS logs",
  "compositeConditionTemplateName": "multi-condition-window",
  "inputConditions": ["WASOUT-base-condition", "WASERR-base-condition"],
  "parameterValues": { "windowDuration" : "90s"},
  "actions": ["index","LAB-log-action","LAB-email-action"]
}
```

d. Save and close the file when you are done.

2. Use the `alerts.sh` utility to create the new condition.

a. Run the following command to create the condition.

```
./alerts.sh -createCompositeCondition WAS_multiConditionWindow.json
```

b. Run the following command to verify that the condition was created.

```
./alerts.sh -getCompositeCondition
...
Name: WAS-multi-condition
  Description: This condition detects java sql exceptions in two WAS logs
  Template: multi-condition-window
  Parameter Values:
    windowDuration: 90s
Actions: [LAB-email-action, LAB-log-action, index]
Input conditions: [WASERR-base-condition, WASOUT-base-condition]
  Enabled: true
```

Web access single-condition-count composite condition

1. Create a composite condition that triggers an alert when the value of responseTime is over 30,000 five times within a 20-minute window. Use the WEB-base-condition that you created in a preceding exercise. Use all of the actions that you configured earlier.

a. Verify that you are in the alerts subdirectory.

```
cd /opt/IBM/LogAnalysis/utilities/alerts
```

b. Make a copy of the `singleConditionCount.json` file. Name the copy `WEB_singleConditionCount.json`.

```
cp singleConditionCount.json WEB_singleConditionCount.json
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Open the `WEB_singleConditionCount.json` file in a text editor. Edit the following five fields in the file. Make the `WEB_singleConditionCount.json` file match the following example.

```
vi WEB_singleConditionCount.json

{
  "name": "WEB-window-count-condition",
  "description": "This condition detects when 5 response times over 30K
occur within 20 minutes",
  "compositeConditionTemplateName": "single-condition-count",
  "inputConditions": ["WEB-base-condition"],
  "parameterValues": { "windowDuration" : "20m", "threshold": 5},
  "actions": ["index","LAB-log-action","LAB-email-action"]
}
```

d. Save and close the file when you are done.

2. Use the `alerts.sh` utility to create the new condition.

a. Run the following command to create the condition.

```
./alerts.sh -createCompositeCondition WEB_singleConditionCount.json
```

b. Run the following command to verify that the condition was created.

```
./alerts.sh -getCompositeCondition
...
Name: WEB-window-count-condition
  Description: This condition detects when 5 response times over 30K occur
within 20 minutes
  Template: single-condition-count
  Parameter Values:
    windowDuration: 20m
    threshold: 5
Actions: [LAB-email-action, LAB-log-action, index]
Input conditions: [WEB-base-condition]
  Enabled: true
```

Exercise 5 Testing composite conditions

In this exercise, you test the composite conditions that you created in the preceding exercise.

1. Run the following commands to add more messages to the WAS and web server log files.

```
/software/log_samples/scripts/WAS_Logs.sh
/software/log_samples/scripts/Web_Logs.sh
```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

2. Open the `/tmp/LAB_alert.log` file. Notice the alerts in this log file that were triggered by the composite conditions.

   ```
   more /tmp/LAB_alert.log
   ```

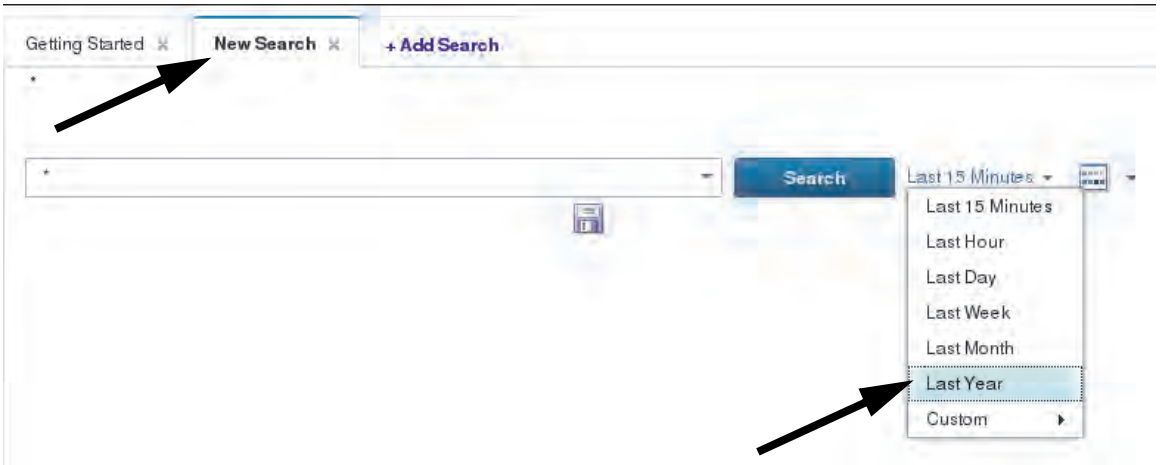
   ```
   ...
   {"conditionName":"WAS-multi-condition","conditionType":"composite","datasources":["WAS_SystemErr","WAS_SystemOut"],"timestamp":1427037406612,"date":"2015-03-22T15:16:46.612Z","alertDetails":{"intervalSeconds":0,"maxDate":"2015-03-22T15:16:46.841Z","minDate":"2015-03-22T15:16:46.612Z","minTimestamp":1427037406612,"maxTimestamp":1427037406841}}
   ...
   {"conditionName":"WEB-window-count-condition","conditionType":"composite","datasources":["Web_Server"],"timestamp":1426795356000,"date":"2015-03-19T20:02:36.000Z","alertDetails":{"minTimestamp":1426794823000,"minDate":"2015-03-19T19:53:43.000Z","maxTimestamp":1426795875000,"maxDate":"2015-03-19T20:11:15.000Z","intervalSeconds":1052,"count":5}}
   ...
   ```

3. Open a Firefox browser if one is not already open. Search for the alerts that were triggered by the composite conditions.

   a. Open a Firefox browser and browse to the following address. Log in with the user name **unityadmin** and the password **unityadmin**.

      `https://host2.tivoli.edu:9987/Unity`

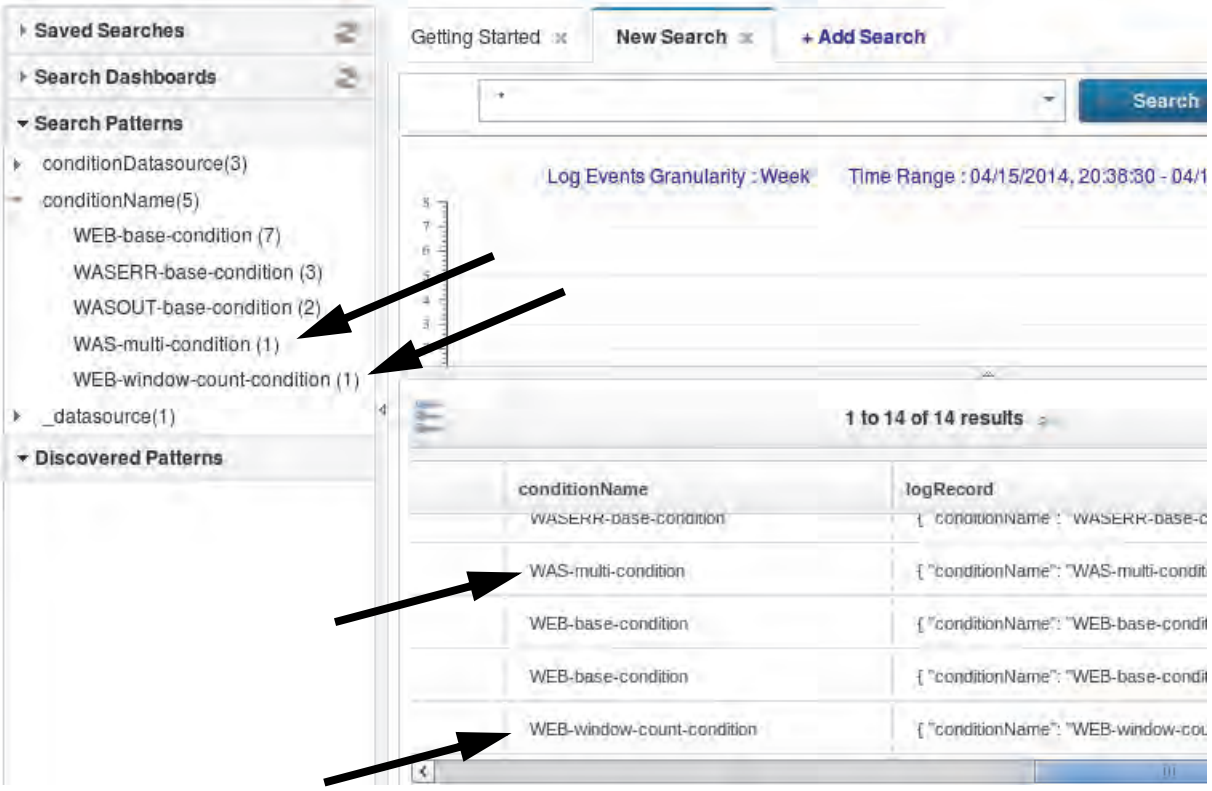
   b. Click the **New Search** tab. Select **Last Year** as the time filter.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Select only **_alerts** as the log source. Click **Search**.

Alerts that have been indexed load in to the user interface. Notice the alerts that were triggered by the composite conditions.



Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

5 Hadoop Distributed File System (HDFS) integration exercises

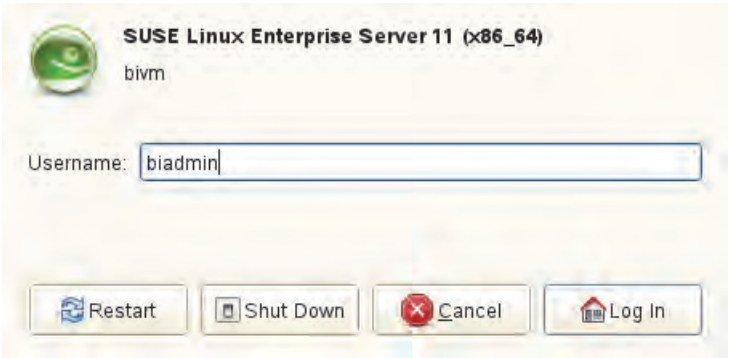
In these exercises, you configure IBM Operations Analytics Log Analysis to use Hadoop Distributed File System (HDFS) for long-term data storage.

Exercise 1 Configuring passwordless SSH

The integration of Log Analysis and HDFS requires passwordless SSH authentication between hosts for the user that owns Log analysis. You must set up passwordless SSH in a full mesh configuration for all hosts in the data node cluster, including authentication for the hosts connecting to themselves.

You use two hosts in your lab environment. The host named host2.tivoli.edu runs the Log Analysis software. The host named bivm.ibm.com runs IBM InfoSphere BigInsights version 3.0.0.1, which includes HDFS and map-reduce.

1. Start the virtual machine named bivm.ibm.com. Log in to the bivm.ibm.com host with the user name **biadmin** and the password **object00**.



© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

2. Create a user on bivm.ibm.com that matches the **netcool** user on host2.tivoli.edu.
   a. Open a terminal window on the bivm.ibm.com host.
   b. Run the following command to verify that you are working on the correct host.

      ```
      hostname
      bivm
      ```

   c. Switch to the **root** user. The password is **object00**.

      ```
      su - root
      Password: object00
      ```

   d. Run the following commands to create the **netcool** user and the **ncoadmin** group.

      ```
      groupadd -g 502 ncoadmin
      useradd -g 502 -u 501 -m -d /home/netcool -k /etc/skel -s /bin/bash netcool
      ```

   e. Set **object00** as the password for the **netcool** user. Ignore the warning about the bad password.

      ```
      passwd netcool

      Changing password for netcool.
      New Password: object00
      Bad password: it is based on a dictionary word
      Reenter New Password: object00
      Password changed.
      ```

3. Configure passwordless SSH authentication from host2.tivoli.edu to bivm.ibm.com.
   a. Switch to the host2.tivoli.edu host and open a terminal window as the **netcool** user.
   b. Run the following command to verify that you are working on the correct host.

      ```
      hostname
      host2.tivoli.edu
      ```

   c. Change to the /home/netcool directory.

      ```
      cd /home/netcool
      ```

   d. Run the following command to generate a pair of public keys. Press Enter to accept all of the default values.

      ```
      ssh-keygen -t rsa

      Generating public/private rsa key pair.
      Enter file in which to save the key (/home/netcool/.ssh/id_rsa):
      Enter passphrase (empty for no passphrase):
      Enter same passphrase again:
      Your identification has been saved in /home/netcool/.ssh/id_rsa.
      Your public key has been saved in /home/netcool/.ssh/id_rsa.pub.
      The key fingerprint is:
      ```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
aa:c1:3d:69:ff:bb:05:ac:f2:8a:1c:1b:36:68:80:eb netcool@host2.tivoli.edu
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|.        .       |
|o       S o      |
| o o . o . .     |
|. o B B .   .    |
|.. o X =   .     |
| E  = ..o.+o     |
+-----------------+
```

e. Run the following command to create an .ssh subdirectory for netcool on the bivm.ibm.com host. Enter **yes** when you are prompted to continue. Enter **object00** as the password.

```
ssh netcool@bivm.ibm.com mkdir -p .ssh

The authenticity of host 'bivm.ibm.com (192.168.100.166)' can't be
established.
RSA key fingerprint is eb:35:c3:3d:bb:27:4e:0d:fe:24:fe:19:e2:ed:36:80.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'bivm.ibm.com,192.168.100.166' (RSA) to the list
of known hosts.
Password: object00
```

f. Copy the new public key (`id_rsa.pub`) to a file named authorized_keys on bivm.ibm.com. Enter **object00** as the password.

```
cat .ssh/id_rsa.pub | ssh netcool@bivm.ibm.com 'cat >> .ssh/authorized_keys'
Password: object00
```

g. Run the following command to set permissions for the .ssh subdirectory and authorized_keys file on bivm.ibm.com.

```
ssh netcool@bivm.ibm.com "chmod 700 .ssh; chmod 640 .ssh/authorized_keys"
```

h. Test the configuration by connecting to bivm.ibm.com as the **netcool** user. Run the following command and verify that you are not prompted for a password.

```
[netcool@host2 ~]$ ssh bivm.ibm.com
netcool@bivm:~>
```

i. Type `exit` to close the SSH session to bivm.ibm.com.

```
exit

logout
Connection to bivm.ibm.com closed.
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

4. Configure passwordless SSH authentication from bivm.ibm.com to itself (bivm.ibm.com).
   a. Switch to the bivm.ibm.com host and open a terminal window as the **netcool** user.

      ```
      su - netcool
      Password: object00
      ```

   b. Run the following command to verify that you are working on the correct host.

      ```
      hostname
      bivm
      ```

   c. Change to the `/home/netcool` directory.

      ```
      cd /home/netcool
      ```

   d. Run the following command to generate a pair of public keys. Press Enter to accept all of the default values.

      ```
      ssh-keygen -t rsa

      Generating public/private rsa key pair.
      Enter file in which to save the key (/home/netcool/.ssh/id_rsa):
      Enter passphrase (empty for no passphrase):
      Enter same passphrase again:
      Your identification has been saved in /home/netcool/.ssh/id_rsa.
      Your public key has been saved in /home/netcool/.ssh/id_rsa.pub.
      The key fingerprint is:
      86:36:e7:5b:8f:0a:cf:f0:0b:b8:b6:01:bc:14:37:67 netcool@bivm
      The key's randomart image is:
      +--[ RSA 2048]----+
      |                 |
      |                 |
      |  . o E          |
      | . o + .         |
      |  +   + S        |
      | . o o =         |
      |  . o + . .      |
      |    .o B o o     |
      |   .o.  Bo. .    |
      +-----------------+
      ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Add the new public key (`id_rsa.pub`) to the file named `authorized_keys` on bivm.ibm.com. Enter **yes** when you are prompted to continue. Enter **object00** as the password.

```
cat .ssh/id_rsa.pub | ssh netcool@bivm.ibm.com 'cat >> .ssh/authorized_keys'

The authenticity of host 'bivm.ibm.com (192.168.100.166)' can't be
established.
RSA key fingerprint is eb:35:c3:3d:bb:27:4e:0d:fe:24:fe:19:e2:ed:36:80.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'bivm.ibm.com,192.168.100.166' (RSA) to the list
of known hosts.
Password: object00
```

f. Test the configuration by connecting to bivm.ibm.com as the **netcool** user. Run the following command and verify that you are not prompted for a password.

```
netcool@bivm:~> ssh bivm.ibm.com
Last login: Fri Apr 24 14:30:53 2015 from host2.tivoli.edu
netcool@bivm:~>
```

g. Type `exit` to close the SSH session to bivm.ibm.com.

```
exit

logout
Connection to bivm.ibm.com closed.
```

5. Configure passwordless SSH authentication from bivm.ibm.com to host2.tivoli.edu.

a. Open a terminal window as the **netcool** user, if you have not already done so.

b. Run the following command to verify that you are working on the correct host.

```
hostname
bivm
```

c. Change to the *`/home/netcool`* directory.

```
cd /home/netcool
```

d. Add the public key on bivm.ibm.com (`id_rsa.pub`) to the file named `authorized_keys` on host2.tivoli.edu. Enter **yes** when you are prompted to continue. Enter **object00** as the password.

```
cat .ssh/id_rsa.pub | ssh netcool@host2.tivoli.edu 'cat >>
.ssh/authorized_keys'

The authenticity of host 'host2.tivoli.edu (192.168.100.161)' can't be
established.
RSA key fingerprint is 1c:2c:83:be:ca:fd:a4:86:14:29:16:2f:76:65:af:55.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'host2.tivoli.edu,192.168.100.161' (RSA) to the
list of known hosts.
netcool@host2.tivoli.edu's password: object00
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Test the configuration by connecting to host2.tivoli.edu as the **netcool** user. Run the following command and verify that you are not prompted for a password.

```
netcool@bivm:~> ssh host2.tivoli.edu

Last login: Thu Mar 19 13:49:39 2015 from 192.168.100.1
[netcool@host2 ~]$
```

f. Type `exit` to close the SSH session to host2.tivoli.edu.

```
exit

logout
Connection to host2.tivoli.edu closed.
```

Exercise 2 Configuring BigInsights and Hadoop

1. Copy the .jar files that Hadoop requires from host2.tivoli.edu to bivm.ibm.com.

   a. Switch to the bivm.ibm.com host and open a terminal window as the **netcool** user, if you have not already done so.

   ```
   su - netcool
   Password: object00
   ```

   b. Run the following command to verify that you are working on the correct host.

   ```
   hostname
   bivm
   ```

   c. Change to the /home/netcool directory.

   ```
   cd /home/netcool
   ```

   d. Run the following commands to create directories to save the .jar files.

   ```
   mkdir LA_SERVICE_HOME
   mkdir SEARCH_JARS_TEMP
   ```

   e. Change to the following directory:

   ```
   cd /home/netcool/LA_SERVICE_HOME/
   ```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

f. Use FTP to connect to host2.tivoli.edu. Log in with the user name **netcool** and the password **object00**.

```
ftp host2.tivoli.edu

Connected to host2.tivoli.edu.
220 (vsFTPd 2.2.2)
Name (host2.tivoli.edu:biadmin): netcool
331 Please specify the password.
Password: object00
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

g. Run the following command to change to the directory where the .jar files are saved.

```
cd /opt/IBM/LogAnalysis/utilities/hadoop/
```

h. Run the following command to copy the file named `service.zip`.

```
get service.zip
```

i. Run the following command to change your local directory.

```
lcd /home/netcool/SEARCH_JARS_TEMP
```

j. Run the following command to copy the file named `search.zip`.

```
get search.zip
```

k. Close the FTP session.

```
quit
```

2. Decompress the `service.zip` file and start the Log Analysis - BigInsights ingestion service.

a. Change to the directory where you saved the `service.zip` file.

```
cd /home/netcool/LA_SERVICE_HOME
```

b. Decompress the `service.zip` file.

```
unzip service.zip
```

c. Start the Hadoop service.

```
bin/server.sh clusterStart

Starting server on [bivm.ibm.com] ... starting rpc server at port 9003.
Server started. Appending logs to file
/home/netcool/LA_SERVICE_HOME/logs/rpcServer.out
```

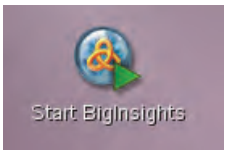
d. Check the status of the service.

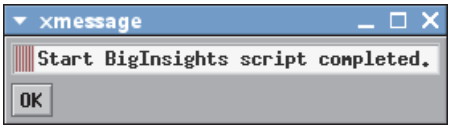
```
bin/server.sh clusterStatus

Getting status for [bivm.ibm.com] ... Server running with process id=9479.
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

3. Start IBM InfoSphere BigInsights. Verify that BigInsights and all of its applications are available.
   a. Double-click the Start BigInsights icon on the biadmin desktop. Wait for BigInsights and all of its applications to start.

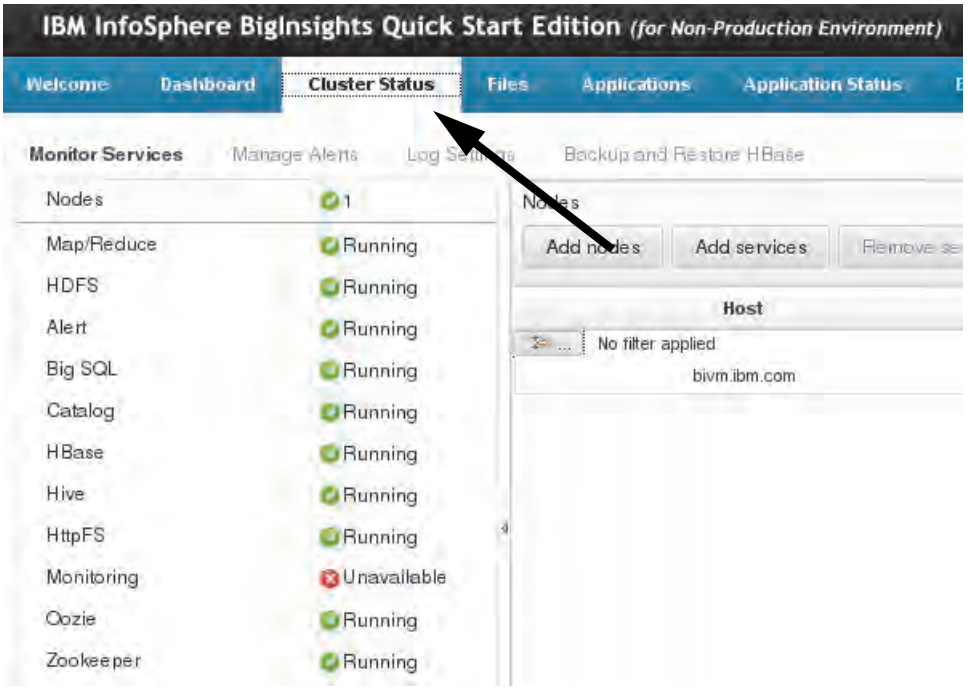




   b. Double-click the Web console shortcut on the biadmin desktop. Log in with the user name **biadmin** and the password **object00**.

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

c. Click the **Cluster Status** tab. Verify that all nodes are running.



Note: You can ignore the unavailable Monitoring node.

4. Create directories for Log Analysis data on the HDFS data node as the **biadmin** user.

   a. Open a new terminal window and switch to the biadmin user. The password is **object00**.

   ```
   su - biadmin
   Password: object00
   ```

   b. Run the following command to verify that you are working on the correct host.

   ```
   hostname
   bivm
   ```

   c. Run the following commands to create the required directories.

   ```
   hadoop fs -mkdir /la-hadoop-tier
   hadoop fs -mkdir /la-hadoop-tier/data
   hadoop fs -mkdir /la-hadoop-tier/jars
   hadoop fs -mkdir /la-hadoop-tier/output
   ```

   d. Run the following command to change the owner of these directories to **netcool**.

   ```
   hadoop fs -chown -R netcool:ncoadmin /la-hadoop-tier
   ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Run the following commands to verify that the directories were created and that **netcool** owns them.

```
hadoop fs -ls /

drwxrwxr-x   - hdfs    biadmin          0 2014-09-18 23:55 /biginsights
drwxr-xr-x   - hdfs    biadmin          0 2014-09-18 23:32 /hadoop
drwxr-xr-x   - hbase   biadmin          0 2015-04-24 15:37 /hbase
drwxr-xr-x   - netcool ncoadmin         0 2015-04-24 16:20 /la-hadoop-tier
drwxrwxrwt   - hdfs    biadmin          0 2014-09-19 00:34 /tmp
drwxrwxrwx   - hdfs    biadmin          0 2014-09-25 20:11 /user

hadoop fs -ls /la-hadoop-tier

drwxr-xr-x   - netcool ncoadmin         0 2015-04-24 16:20
/la-hadoop-tier/data
drwxr-xr-x   - netcool ncoadmin         0 2015-04-24 16:20
/la-hadoop-tier/jars
drwxr-xr-x   - netcool ncoadmin         0 2015-04-24 16:20
/la-hadoop-tier/output
```

5. As the **netcool** user, copy the service .jar files to the new `/la-hadoop-tier/jars` directory.

   a. Open a terminal window and switch to the **netcool** user if you do not already have one open.

   ```
   su - netcool
   Password: object00
   ```

   b. Run the following command to verify that you are working on the correct host.

   ```
   hostname
   bivm
   ```

   c. Run the following command to copy the service .jar files to the correct directory.

   ```
   hadoop fs -copyFromLocal /home/netcool/LA_SERVICE_HOME/lib/*.jar
   /la-hadoop-tier/jars/
   ```

6. As the **netcool** user, copy the search .jar files to the new `/la-hadoop-tier/jars` directory.

   a. Run the following commands to decompress the search .jar files.

   ```
   cd /home/netcool/SEARCH_JARS_TEMP

   unzip search.zip
   ```

   b. Run the following command to copy the search .jar files to the correct directory.

   ```
   hadoop fs -copyFromLocal /home/netcool/SEARCH_JARS_TEMP/*.jar
   /la-hadoop-tier/jars/
   ```

Note: You can ignore the `File exists` messages.

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

7. Verify that all of the .jar files were copied to the `/la-hadoop-tier/jars` directory.

```
hadoop fs -ls /la-hadoop-tier/jars
```

Exercise 3 Configuring Log Analysis

1. Edit the `unitysetup.properties` file on the Log Analysis server to enable the Hadoop integration.
   a. Switch to the host2.tivoli.edu host and open a terminal window as the **netcool** user.
   b. Run the following command to verify that you are working on the correct host.

```
hostname
host2.tivoli.edu
```

   c. Open the `unitysetup.properties` file with a text editor.

```
vi
/opt/IBM/LogAnalysis/wlp/usr/servers/Unity/apps/Unity.war/WEB-INF/unitysetup
.properties
```

   d. Find the **INDEX_IMPLEMENTATION** property. Change the value to **SOLR,HADOOP**.

```
...
#Number of charts allowed in dynamic dashboards
DASHBOARD_CHARTS_LIMIT=8

#Underlying search index implementation
INDEX_IMPLEMENTATION=SOLR,HADOOP

#Setting range on minute to calculate Granularity (in minutes)
GRANULARITY_MINUTE_LOWER_LIMIT=15
GRANULARITY_MINUTE_UPPER_LIMIT=60

#Wait time for get search result call (in ms)
...
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

e. Find the HADOOP_TIER_HDFS_BASE_DIR and HADOOP_TIER_JOB_TRACKER_URI properties. Change the value of these properties to match the following example.

```
...
#Maximum no. of charts allowed to auto refresh across dashboards
MAX_AUTO_REFRESH_CHARTS=20

#Hadoop-tier properties
#Enable HADOOP_TIER by adding HADOOP to INDEX_IMPLEMENTATION property ->
INDEX_IMPLEMENTATION=SOLR,HADOOP
HADOOP_TIER_HDFS_BASE_DIR=hdfs://bivm.ibm.com:9000/la-hadoop-tier
HADOOP_TIER_HDFS_ADMIN_USER=hdfs
HADOOP_TIER_JOB_TRACKER_URI=bivm.ibm.com:9001
HADOOP_TIER_SERVER_PORT=9003
...
```

f. Save and close the file when you are finished.

2. Copy the `core-site.xml` and `hdfs-site.xml` configuration files from the bivm.ibm.com host to the host2.tivoli.edu host.

   a. Change to the directory where Log Analysis expects to see the `core-site.xml` and `hdfs-site.xml` files.

   ```
   cd
   /opt/IBM/LogAnalysis/wlp/usr/servers/Unity/apps/Unity.war/WEB-INF/classes/
   ```

   b. Run the following commands to copy the files from bivm.ibm.com and save them locally.

   ```
   scp netcool@bivm.ibm.com:/opt/ibm/biginsights/hadoop-conf/core-site.xml .
   scp netcool@bivm.ibm.com:/opt/ibm/biginsights/hadoop-conf/hdfs-site.xml .
   ```

   c. Verify that the files were correctly copied.

   ```
   ls -l
   -rw-r--r-- 1 netcool ncoadmin 3416 Apr 24 20:47 core-site.xml
   -rw-r--r-- 1 netcool ncoadmin 3906 Apr 24 20:47 hdfs-site.xml
   -rw-r--r-- 1 netcool ncoadmin 3520 Mar 19 18:35 log4j.properties
   ```

3. Stop Log Analysis.

   ```
   /opt/IBM/LogAnalysis/utilities/unity.sh -stop
   ```

4. Start Log Analysis.

   ```
   /opt/IBM/LogAnalysis/utilities/unity.sh -start
   ```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise 4 Verifying the integration

After you enable the integration, Log Analysis stores log data to both Solr and HDFS. In this exercise, you verify that Log Analysis is writing data to the HDFS system.

Important: Run all of the steps in this exercise on the host2.tivoli.edu virtual machine.

1. Run the following commands to create more log messages for Log Analysis to process.

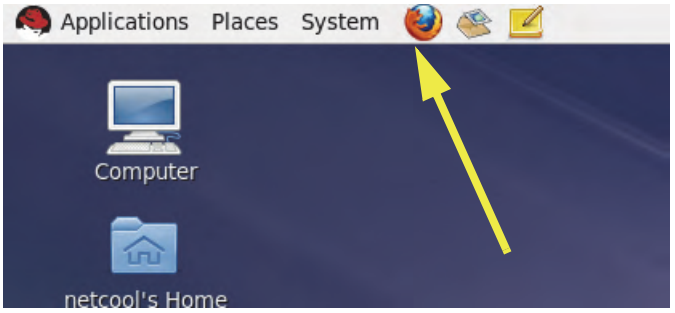
   ```
   /software/log_samples/scripts/WAS_Logs.sh
   /software/log_samples/scripts/Web_Logs.sh
   ```

2. Open the `/opt/IBM/LogAnalysis/logs/Hadooptier.log` file. Look for messages like the following example. These messages verify that Log Analysis is communicating with the new BigInsights ingestion service.

   ```
   04/27/15 13:36:55:437 UTC [Thread-46] INFO
   com.ibm.tivoli.unity.hadoop.ingestion.client.ServiceNode - Retrieved batches
   status for service node [192.168.100.166:9003]
   04/27/15 13:37:00:438 UTC [Thread-46] INFO
   com.ibm.tivoli.unity.hadoop.ingestion.client.ServiceNode - Retrieving batches
   status from service node [192.168.100.166:9003]
   04/27/15 13:37:00:439 UTC [Thread-46] INFO
   com.ibm.tivoli.unity.hadoop.ingestion.client.ServiceNode - Received updates for
   [3] batches from service node [192.168.100.166:9003]. [0] batches finished with
   errors.
   ```

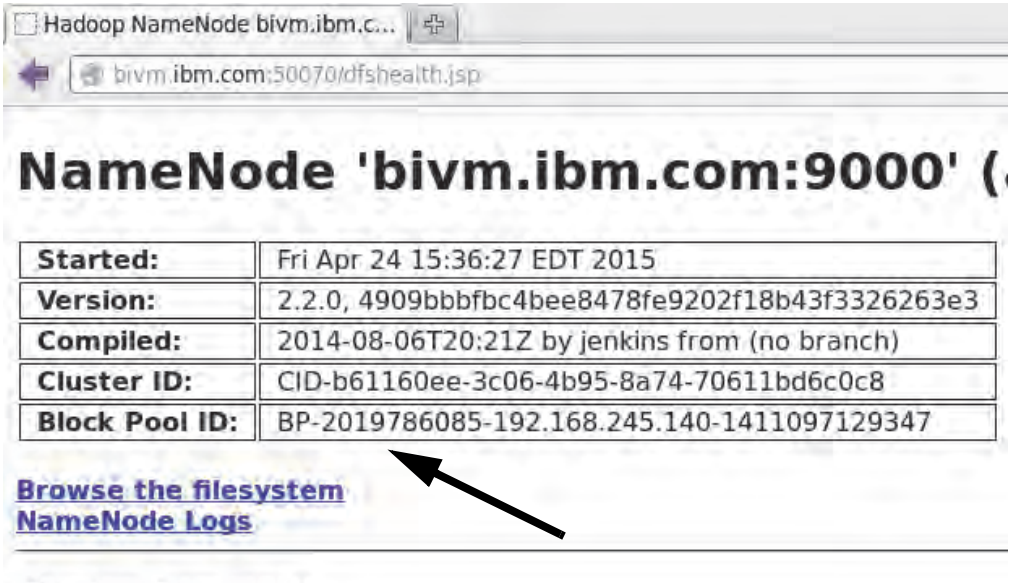
3. Use a browser to view the HDFS file system and verify that log data is present.

   a. Double-click the **Firefox** icon on the desktop.

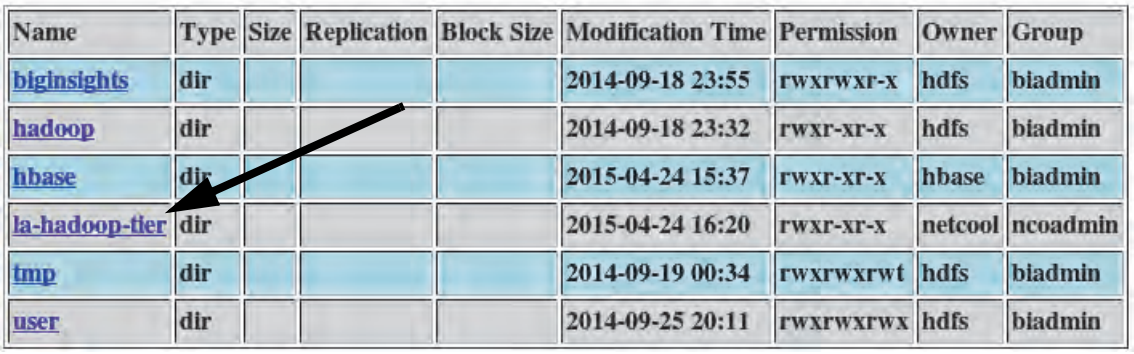


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Browse to the address `http://bivm.ibm.com:50070`. Click **Browse the filesystem**.

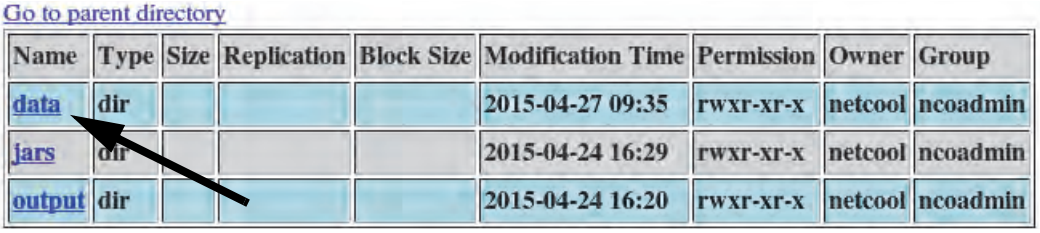


c. Click **la-hadoop-tier**.



Name	Type	Size	Replication	Block Size	Modification Time	Permission	Owner	Group
biginsights	dir				2014-09-18 23:55	rwxrwxr-x	hdfs	biadmin
hadoop	dir				2014-09-18 23:32	rwxr-xr-x	hdfs	biadmin
hbase	dir				2015-04-24 15:37	rwxr-xr-x	hbase	biadmin
la-hadoop-tier	dir				2015-04-24 16:20	rwxr-xr-x	netcool	ncoadmin
tmp	dir				2014-09-19 00:34	rwxrwxrwt	hdfs	biadmin
user	dir				2014-09-25 20:11	rwxrwxrwx	hdfs	biadmin

d. Click **data**.



Go to parent directory

Name	Type	Size	Replication	Block Size	Modification Time	Permission	Owner	Group
data	dir				2015-04-27 09:35	rwxr-xr-x	netcool	ncoadmin
jars	dir				2015-04-24 16:29	rwxr-xr-x	netcool	ncoadmin
output	dir				2015-04-24 16:20	rwxr-xr-x	netcool	ncoadmin

e. Click **UnityCollection_*<date>*_UTC**.

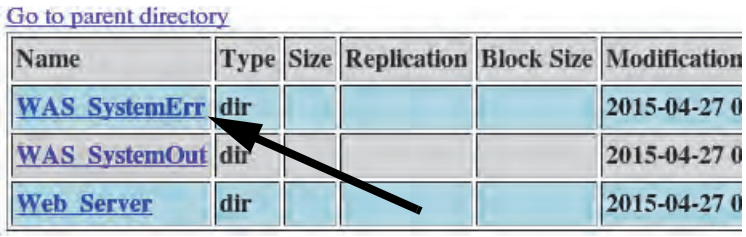
Go to parent directory

Name	Type	Size	Replication	Block Size	Mod
.tmp	dir				2015
UnityCollection_27_04_2015_00_00_00_UTC	dir				2015

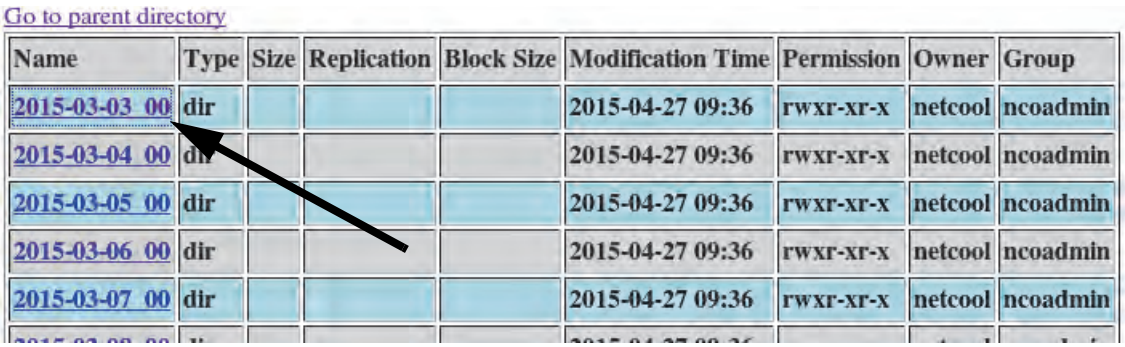
© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

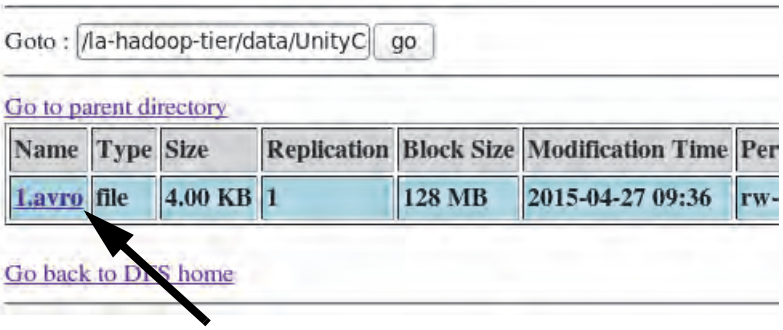
f. Notice the subdirectories that are named like the Log Analysis data sources. Click one of the subdirectories.



g. Click one of the date directories.



Notice the .avro file or files. These files contain log data in compressed binary format.



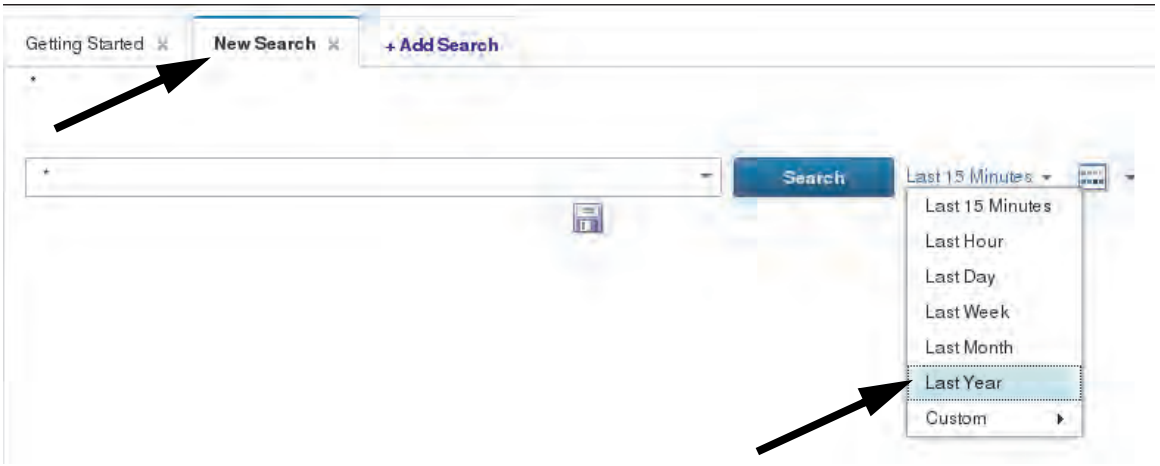
4. Open a Firefox browser and search for the log messages. Search through one of the data sources you saw in the HDFS directory structure, such as WAS_SystemErr.

   a. Open a Firefox browser and browse to the following address. Log in with the user name **unityadmin** and the password **unityadmin**.

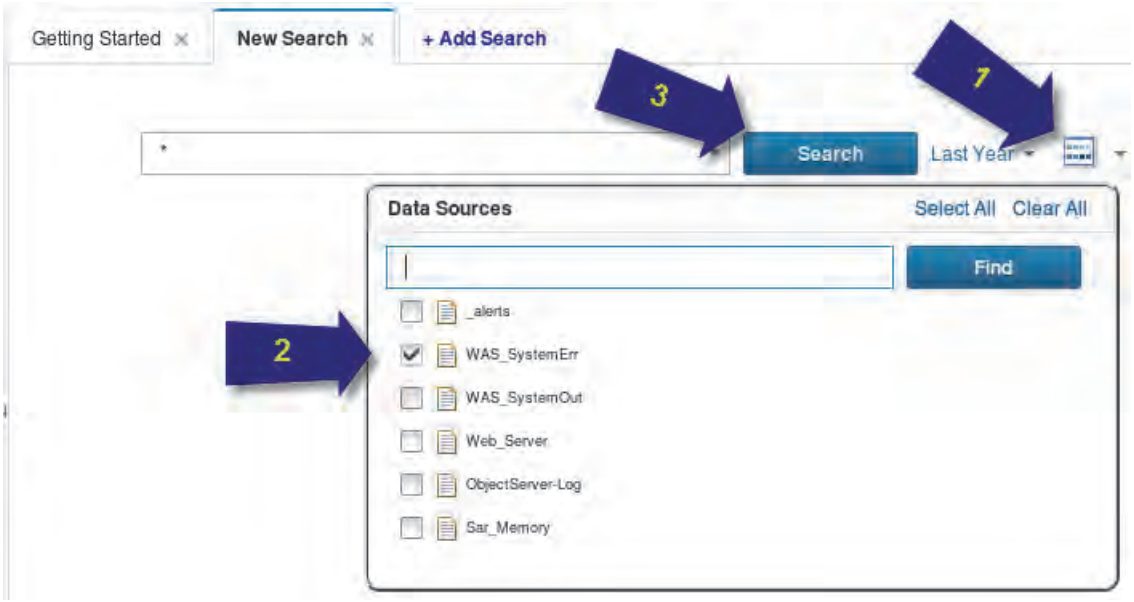
   `https://host2.tivoli.edu:9987/Unity`

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Click the **New Search** tab. Select **Last Year** as the time filter.



c. Select only **WAS_SystemErr** as the log source. Click **Search**.



d. Log messages load in to the user interface. Leave the search results open.

5. Open the `/opt/IBM/LogAnalysis/logs/UnityApplication.log` file. Look for messages like the following example. These messages verify that Log Analysis is searching the HDFS node for data. Notice that Log analysis is also searching for data in the Solr file system.

```
04/27/15 14:35:55:733 UTC [Default Executor-thread-15] INFO  -
JAXRSUnitySearchServlet : New search query is being POSTed. Mode=async
04/27/15 14:35:55:749 UTC [Default Executor-thread-15] INFO  - USRHandler :
Collection: WAS_SystemErr, bean:
id=31   name=WAS_SystemErr      sourceType=13   indexingConfig=null
annotator=0
04/27/15 14:35:55:755 UTC [Default Executor-thread-15] INFO  -
InsightPackResourceBundleManager : __ENTRY translatedIndexConfigFields()
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

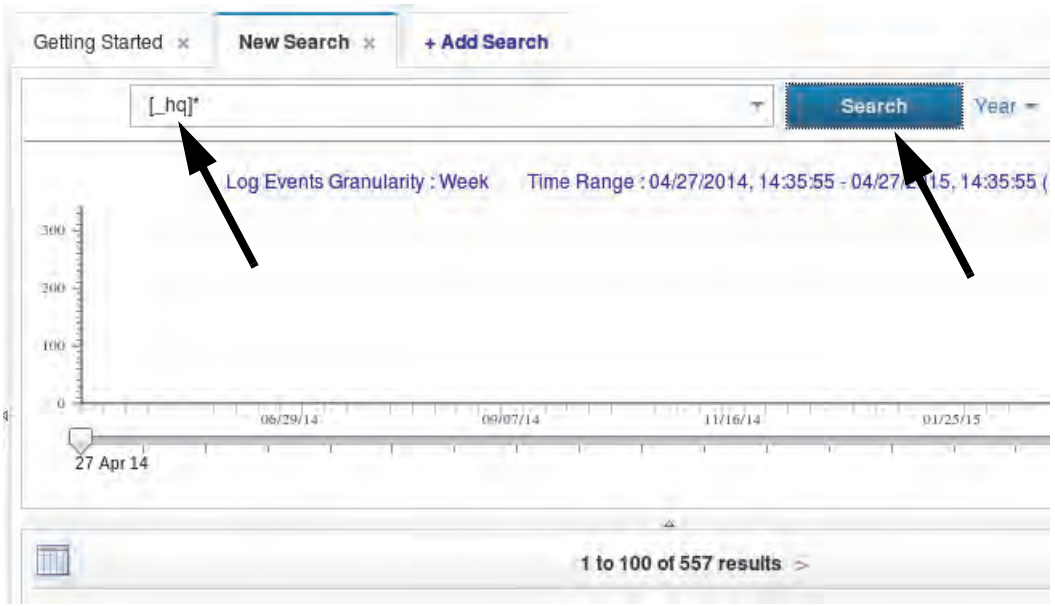
```
04/27/15 14:35:55:756 UTC [Default Executor-thread-15] INFO  -
InsightPackArtifactMapHandler :  Not in the cache! Going to DB for SOURCETYPE id
13
04/27/15 14:35:55:910 UTC [Default Executor-thread-15] INFO  -
InsightPackResourceBundleManager : __EXIT translatedIndexConfigFields()
04/27/15 14:35:55:920 UTC [Default Executor-thread-15] INFO  - UnitySearchQuery
: Disabled highlighting for * query
04/27/15 14:35:55:971 UTC [Default Executor-thread-15] INFO  -
UnitySearchRuntime : Checking for hadoop data in query, time-stamp range =
[1398609355000, 1430145355401]
04/27/15 14:35:55:972 UTC [Default Executor-thread-15] INFO  -
UnitySearchRuntime : Min-colr-tier-timestamp: 1426723200000,
queryReferencesHadoopData: true
04/27/15 14:35:55:972 UTC [Default Executor-thread-15] INFO  -
UnitySearchRuntime : Search Query ID: Query mode: asynchronous
04/27/15 14:35:55:976 UTC [Default Executor-thread-15] INFO  -
UnitySearchRuntime : Submitted Solr search query: 1
04/27/15 14:35:55:976 UTC [Thread-87] INFO  - SearchQueryRunner : Starting query
runner thread for Solr query 1
04/27/15 14:35:55:977 UTC [Thread-87] INFO  - SolrSearchQuery : Solr search
query: *:*
04/27/15 14:35:55:981 UTC [Default Executor-thread-15] INFO  -
UnitySearchRuntime : Submitted Hadoop search query: 1
04/27/15 14:35:55:982 UTC [Thread-88] INFO  - SearchQueryRunner : Starting query
runner thread for hadoop query 1
04/27/15 14:35:55:982 UTC [Thread-88] INFO  - HadoopTierSearchQuery : Retrieving
hadoop-tier partitions: maxWriteTime=1426723200000
04/27/15 14:35:55:989 UTC [Thread-87] INFO  - SolrSearchQuery : Solr filter
query: +(_datasource:"WAS_SystemErr") +timestamp:[2014-04-27T14:35:55.000Z TO
2015-04-27T14:35:55.401Z}
04/27/15 14:35:56:130 UTC [Thread-88] INFO  - HadoopTierSearchQuery : Retrieved
partitions, num = 0
04/27/15 14:35:56:130 UTC [Thread-88] INFO  - HadoopTierSearchQuery : No
hadoop-tier partitions, state = COMPLETE
04/27/15 14:35:56:130 UTC [Thread-88] INFO  - SearchQueryRunner : Completed
executing hadoop-tier queries: 1
04/27/15 14:35:56:130 UTC [Thread-88] INFO  - SearchQueryRunner : Completed
query execution for hadoop-tier query ID 1, status = COMPLETE
04/27/15 14:35:56:196 UTC [Default Executor-thread-16] INFO  - LogSourcesHandler
: 6
04/27/15 14:35:56:976 UTC [Thread-87] INFO  - SolrSearchQuery : Solr Query
1[1/2], search Time: 984
04/27/15 14:35:56:976 UTC [Thread-87] INFO  - SolrSearchQuery : Solr Query 1,
total Results: 557
04/27/15 14:35:56:977 UTC [Thread-87] INFO  - SolrSearchQuery : Solr Query 1,
num Results: 557
04/27/15 14:35:57:019 UTC [Thread-87] INFO  - SolrSearchQuery : Solr search
query: *:*
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
04/27/15 14:35:57:019 UTC [Thread-87] INFO  - SolrSearchQuery : Solr filter
query: +(_datasource:"WAS_SystemErr") +timestamp:[2014-04-27T14:35:55.000Z TO
2015-04-27T14:35:55.401Z}
...
04/27/15 14:35:57:532 UTC [Default Executor-thread-3] INFO  - UnitySearchResult
: COMBINED-STATE: COMPLETE
```

Important: When a user searches for log messages, Log Analysis queries the Solr and Hadoop file systems. The data in both file systems is combined and displayed in the user search results. If there is identical data in both file systems, Log Analysis only shows data from Solr to the user. In this example, only data from Solr is returned to the search results. This is why you see messages like `No hadoop-tier partitions` in the UnityApplication log file.

6. Force the Log Analysis user interface to search for data only in the HDFS node.
   a. Return to the Firefox browser where the Log Analysis user interface is open.
   b. Verify that you are searching the **WAS_SystemErr** data source. Type `[_hq]*` in the search filter field. Click **Search**. Log messages load in to the search results.



7. Open the `/opt/IBM/LogAnalysis/logs/UnityApplication.log` file again. Look for messages like the following example. These messages verify that Log Analysis is retrieving data from the HDFS node.

```
04/27/15 15:11:26:718 UTC [Thread-90] INFO  - HadoopTierSearchQuery : Hadoop
Query 2[1/1], search Time: 35871
04/27/15 15:11:26:718 UTC [Thread-90] INFO  - HadoopTierSearchQuery : Hadoop
Query 2, total Results: 557
04/27/15 15:11:26:718 UTC [Thread-90] INFO  - HadoopTierSearchQuery : Hadoop
Query 2, num Results: 90
```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
04/27/15 15:11:26:718 UTC [Thread-90] INFO  - SearchQueryRunner : Completed
executing hadoop-tier queries: 2
04/27/15 15:11:26:718 UTC [Thread-90] INFO  - SearchQueryRunner : Completed
query execution for hadoop-tier query ID 2, status = COMPLETE
```

Exercise 5 Disabling the HDFS integration

These steps show you how to disable the HDFS integration.

Important: Run all of the steps in this exercise on the **host2.tivoli.edu** virtual machine.

1. Edit the `unitysetup.properties` file on the Log Analysis server to disable the Hadoop integration.
   a. Open a terminal window as the **netcool** user, if you do not already have one open.
   b. Open the `unitysetup.properties` file with a text editor.

      ```
      vi
      /opt/IBM/LogAnalysis/wlp/usr/servers/Unity/apps/Unity.war/WEB-INF/unitysetup
      .properties
      ```

   c. Find the **INDEX_IMPLEMENTATION** property. Change the value to **SOLR**.

      ```
      ...
      #Number of charts allowed in dynamic dashboards
      DASHBOARD_CHARTS_LIMIT=8

      #Underlying search index implementation
      INDEX_IMPLEMENTATION=SOLR

      #Setting range on minute to calculate Granularity (in minutes)
      GRANULARITY_MINUTE_LOWER_LIMIT=15
      GRANULARITY_MINUTE_UPPER_LIMIT=60

      #Wait time for get search result call (in ms)
      ...
      ```

   d. Save and close the file when you are finished.
2. Stop Log Analysis.

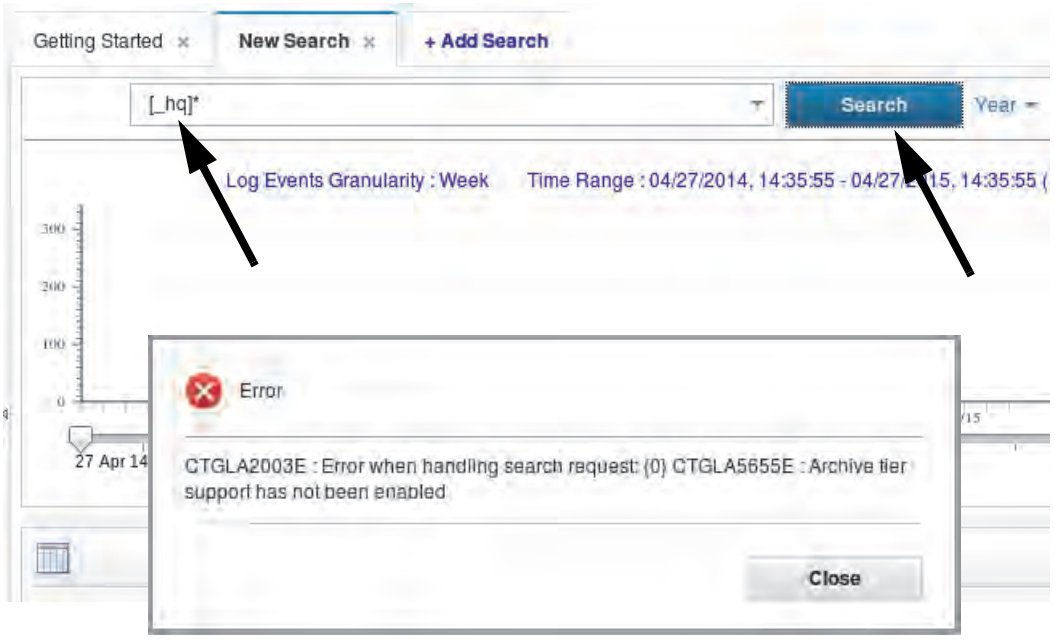
   ```
   /opt/IBM/LogAnalysis/utilities/unity.sh -stop
   ```

3. Start Log Analysis.

   ```
   /opt/IBM/LogAnalysis/utilities/unity.sh -start
   ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

4. Force the Log Analysis user interface to search for data only in the HDFS node again to verify that the HDFS integration has been disabled.
   a. Return to the Firefox browser where the Log Analysis user interface is open.
   b. Verify that you are searching the **WAS_SystemErr** data source. Type `[_hq]*` in the search filter field. Click **Search**. An error message about archive tier support confirms that you have disabled the HFDS integration.



Note: You can find similar error messages in the `UnityApplication.log` file.

5. Shut down the virtual machine named **bivm.ibm.com**.

Important: You do not use the **bivm.ibm.com** virtual machine for any other exercises during this course.

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6 Performance tuning exercises

Exercise 1 Tuning the EIF Receiver

In this exercise, you change the configuration of the EIF (Tivoli® Event Integration Facility) Receiver. You use IBM Operations Analytics Log Analysis log files to confirm the configuration change. This exercise shows you how to meter incoming log messages from streaming log sources.

1. Monitor the IBM Operations Analytics Log Analysis log files to look for messages that are related to data ingestion.
   a. Open a new terminal and tail the `GenericReceiver.log` file.

      ```
      tail -f /opt/IBM/LogAnalysis/logs/GenericReceiver.log
      ```

   b. Open a new terminal and tail the `UnityEifReceiver.log` file.

      ```
      tail -f /opt/IBM/LogAnalysis/logs/UnityEifReceiver.log
      ```

   c. Run the following command to create more log messages in the WAS_SystemOut data source. Watch the UnityEifReceiver.log and GenericReceiver.log log messages. Notice the delay between new messages in UnityEifReceiver.log and new messages in GenericReceiver.log.

      ```
      /software/log_samples/scripts/WAS_Logs.sh
      ```

Note: UnityEifReceiver.log shows messages that are sent from the Log File Agent. GenericReceiver.log shows messages from the Log Analysis common data ingestion interface.

2. Wait about 90 seconds, or until new log messages stop arriving. Press Ctrl+C to stop the tail in both logs. Look for messages in `UnityEifReceiver.log` that show the EIF Receiver posting the JSON payload and the size of the posted data. Notice the number of successes and failures in the post event. Notice the indexed source volume. Messages like this one have a corresponding message in GenericReceiver.log.

   ```
   04/16/15 16:15:30:235 UTC [pool-6-thread-1] INFO  - LogEventPoster : -----------
   Posting Event to UNITY DATA COLLECTOR -
   https://host2.tivoli.edu:9987/Unity/DataCollector
   04/16/15 16:15:30:235 UTC [pool-6-thread-1] INFO  - LogEventPoster : Post
   Queue-Remove Operation:0
   ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
04/16/15 16:15:30:240 UTC [pool-6-thread-1] INFO  - LogEventPoster : Posting
Post Data Json of size:275607
04/16/15 16:15:30:736 UTC [pool-6-thread-1] INFO  - LogEventPoster : Total
Response time taken(sec):0
04/16/15 16:15:30:736 UTC [pool-6-thread-1] INFO  - LogEventPoster : +++++++++
RESPONSE MESSAGE +++++++++
04/16/15 16:15:30:736 UTC [pool-6-thread-1] INFO  - LogEventPoster : OK
04/16/15 16:15:30:736 UTC [pool-6-thread-1] INFO  - LogEventPoster :
{"BATCH_STATUS":{"failures":[],"stream":"_unity_default_stream","writeTime":"20
15-04-16T16:04:04.994+0000","indexedSourceVolume":266774,"indexNumSuccessful":5
57,"indexNumFailures":0,"indexBatchIds":"1429200244994_54,","batchSize":557,"ba
tchId":"1429200930584_58","numSuccessful":557,"numFailures":0},"RESPONSE_MESSAG
E":"INPUT_BATCH_PROCESSED","RESPONSE_CODE":200}
```

3. Look for messages in `GenericReceiver.log` that show the generic receiver processing messages that were sent from the EIF receiver.

```
04/16/15 16:15:35:275 UTC [Default Executor-thread-8] INFO  -
UnityFlowController :  Batch Status for -> WAS_SystemErr , Size: 557 , Num
successful: 557 , Num failures: 0 , Indexed Source volume: 0
04/16/15 16:15:35:275 UTC [Default Executor-thread-8] INFO  -
DataCollectorRestServlet : Batch of Size 557 processed and encountered 0
failures
04/16/15 16:15:35:056 UTC [Thread-60] INFO  - IndexStatusChecker : Updating
statistics for data source [WAS_SystemErr], stream [_unity_default_stream],
ingested bytes [266774], write date [Wed Thu 16 16:15:35 UTC 2015].
```

4. In a separate terminal, stop IBM Operations Analytics Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -stop
```

5. Edit the EIF receiver configuration. Change the following properties. The properties are at the bottom of the file.
   - logsource.buffer.wait.timeout=2
   - logsource.max.buffer.size=1024

   a. Open the EIF receiver configuration file.

   ```
   vi  /opt/IBM/LogAnalysis/UnityEIFReceiver/config/unity.conf
   ```

   b. Change the following two properties to match the following example.

   ```
   #Timeout in Seconds
   logsource.buffer.wait.timeout=2
   #Buffer Size in Bytes
   logsource.max.buffer.size=1024
   ```

   c. Save and close the file when you are done.

Important: These settings are not appropriate for a production system. The settings in this example are set intentionally low.

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6. Back up and remove the `UnityEifReceiver.log` and `GenericReceiver.log` files. Removing these log files make it easier to find new log messages.

```
cd /opt/IBM/LogAnalysis/logs/
mv GenericReceiver.log GenericReceiver.log.old
mv UnityEifReceiver.log UnityEifReceiver.log.old
```

7. Start IBM Operations Analytics Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -start
```

8. Wait for all of the log analysis components to start. Resume the tail of the `UnityEifReceiver.log` and `GenericReceiver.log` files.
   a. Find the two terminals that you opened for viewing these log files in a preceding step.
   b. Resume the tail of the log files. Run these commands in two different terminal windows.

```
tail -f /opt/IBM/LogAnalysis/logs/GenericReceiver.log
tail -f /opt/IBM/LogAnalysis/logs/UnityEifReceiver.log
```

Hint: When you view these log files, it might be easier to stop and start the tail on the UnityEifReceiver.log and GenericReceiver.log files to search for specific messages. You can start the tail with the two preceding commands. You can stop the tail with Ctrl+C.

9. Look at the first messages in UnityEifReceiver.log after it starts. Notice the updated properties in the log file. The full path to this log file is `/opt/IBM/LogAnalysis/logs/UnityEifReceiver.log`.

```
Unity Data Collector
KEYSTORE=/opt/IBM/LogAnalysis/wlp/usr/servers/Unity/keystore/unity.ks
Unity Data Collector LOGSOURCE TIMEOUT=2
Unity Data Collector LOGSOURCE BUFFER SIZE=1024
Unity Data Collector MAX EV SERVICE JSON QUEUE SIZE=80000
Unity Data Collector MAX EV POSTER QUEUE SIZE=500
```

10. Run the following command to create more log messages in the WAS_SystemOut data source.

```
/software/log_samples/scripts/WAS_Logs.sh
```

11. Wait approximately 60 seconds. Watch the `UnityEifReceiver.log` and `GenericReceiver.log` log messages. Notice that the delay between new messages in `UnityEifReceiver.log` and new messages in GenericReceiver.log is less than before the configuration change.

12. Look for messages in `UnityEifReceiver.log` that show the EIF Receiver posting the JSON payload.

```
04/16/15 17:02:37:820 UTC [pool-6-thread-1] INFO  - LogEventPoster : Posting
Post Data Json of size:1151
..
04/16/15 17:02:37:853 UTC [pool-6-thread-1] INFO  - LogEventPoster : Posting
Post Data Json of size:1165
```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
...
04/16/15 17:02:37:925 UTC [pool-6-thread-1] INFO  - LogEventPoster : Posting
Post Data Json of size:897
```

Important: The size of the posted data is much smaller than before you made the configuration change. The EIF receiver is posting data to the generic receiver more frequently now, but the size of each post is smaller.

13. Look for messages in GenericReceiver.log about the size of each batch of messages. This is the number of log messages in each batch. The full path to this log file is `/opt/IBM/LogAnalysis/logs/GenericReceiver.log`.

```
04/16/15 17:02:37:818 UTC [Default Executor-thread-8] INFO  -
DataCollectorRestServlet : Batch of Size 5 processed and encountered 0 failures
...
04/16/15 17:02:37:851 UTC [Default Executor-thread-5] INFO  -
DataCollectorRestServlet : Batch of Size 6 processed and encountered 0 failures
...
04/16/15 17:02:37:924 UTC [Default Executor-thread-3] INFO  -
DataCollectorRestServlet : Batch of Size 4 processed and encountered 0 failures
```

Important: Notice that the number of messages in each batch are much lower after you made the configuration change. The numbers changed because the message buffer of the EIR receiver is smaller. The EIF receiver now sends a batch of messages to the generic receiver when the EIF receiver buffer reaches 1024 bytes.

14. If you are tailing the log files, press Ctrl+C to stop the tail in both logs.

Exercise 2 Solr administration

In this exercise, you view details about the Solr file system.

1. Look at the file system where Solr is indexing log data.
   a. Change to the following directory:

      ```
      cd /opt/IBM/LogAnalysis/solr-4.7.1/scala_instance1/solr
      ```

   b. List the contents of the directory. There is one subdirectory for each shard and each day of log data.

      ```
      ls -l
      total 84
      ```


Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

```
drwxr-xr-x 2 netcool ncoadmin 4096 Feb 19  2014 bin
-rw-r--r-- 1 netcool ncoadmin 2473 Feb 19  2014 README.txt
-rw-r--r-- 1 netcool ncoadmin 1715 Feb 19  2014 solr.xml
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 15 19:06
UnityCollection_15_04_2015_00_00_00_UTC_shard1_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 15 19:06
UnityCollection_15_04_2015_00_00_00_UTC_shard2_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 16 16:03
UnityCollection_16_04_2015_00_00_00_UTC_shard1_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 16 16:03
UnityCollection_16_04_2015_00_00_00_UTC_shard2_replica1
```

Note: In this example, two shards are configured. There is log data from two different days: April 15 and April 16. The number of days in your environment might be different from this example.

2. Look at the indexed log files in the Solr file system.
   a. Change to one of the **UnityCollection_<date>_UTC_shard2_replica1** directories. Your directory names have a more recent date.

      ```
      cd UnityCollection_15_04_2015_00_00_00_UTC_shard2_replica1
      ```

   b. List the contents of the **data/index** subdirectory.

      ```
      ls -l data/index/
      ...
      -rw-r--r-- 1 netcool ncoadmin  172827 Apr 15 19:46 _r.fdt
      -rw-r--r-- 1 netcool ncoadmin     232 Apr 15 19:46 _r.fdx
      -rw-r--r-- 1 netcool ncoadmin    4332 Apr 15 19:46 _r.fnm
      -rw-r--r-- 1 netcool ncoadmin   92942 Apr 15 19:46 _r_Lucene41_0.doc
      -rw-r--r-- 1 netcool ncoadmin   93939 Apr 15 19:46 _r_Lucene41_0.pos
      -rw-r--r-- 1 netcool ncoadmin  138017 Apr 15 19:46 _r_Lucene41_0.tim
      -rw-r--r-- 1 netcool ncoadmin    2488 Apr 15 19:46 _r_Lucene41_0.tip
      -rw-r--r-- 1 netcool ncoadmin   29210 Apr 15 19:46 _r_Lucene45_0.dvd
      -rw-r--r-- 1 netcool ncoadmin    1238 Apr 15 19:46 _r_Lucene45_0.dvm
      -rw-r--r-- 1 netcool ncoadmin   10106 Apr 15 19:46 _r.nvd
      -rw-r--r-- 1 netcool ncoadmin      79 Apr 15 19:46 _r.nvm
      -rw-r--r-- 1 netcool ncoadmin     381 Apr 15 19:46 _r.si
      ...
      ```

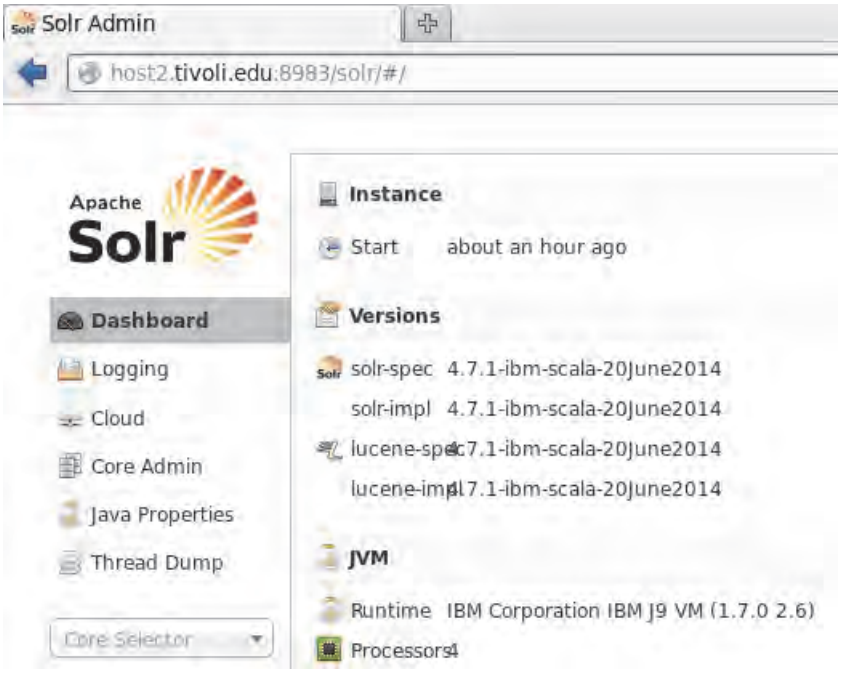
Note: The files in the **data/index** subdirectory are the raw and annotated log messages that IBM Operations Analytics Log Analysis has processed. These files are in compressed binary format.

3. Use the Solr administration interface to look at the Solr file system and indexed data.
   a. Open a Firefox browser. Enter the following URL:

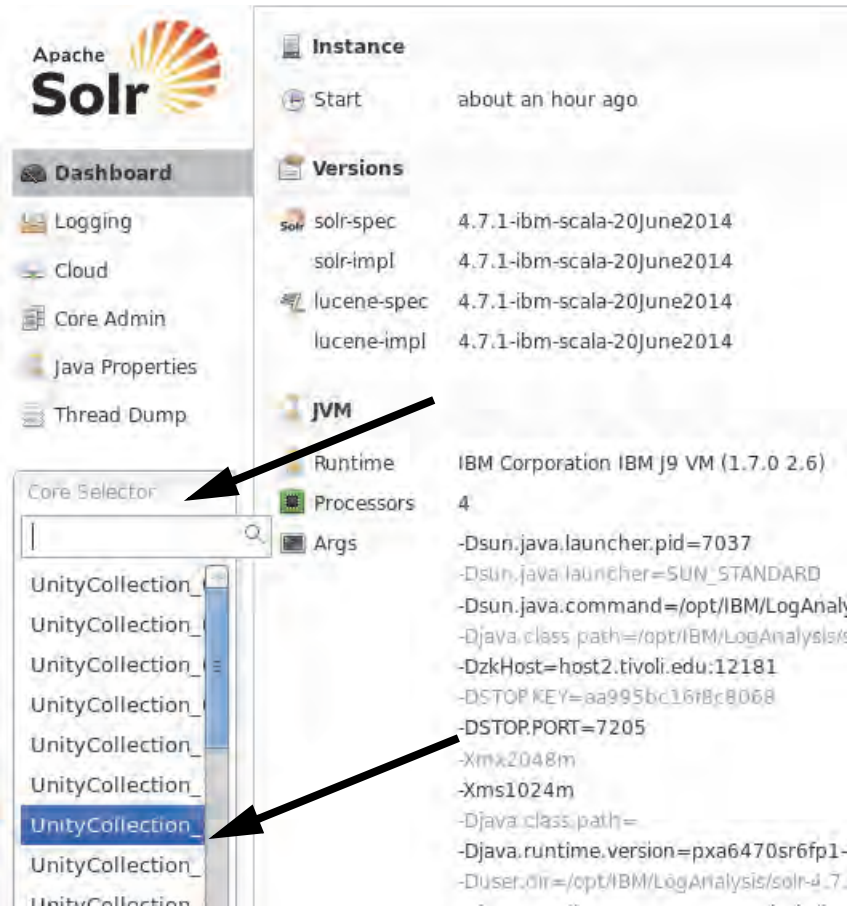
      http://host2.tivoli.edu:8983/solr

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. Press F11 or click **View > Full Screen** in Firefox to view the entire Solr administration interface.



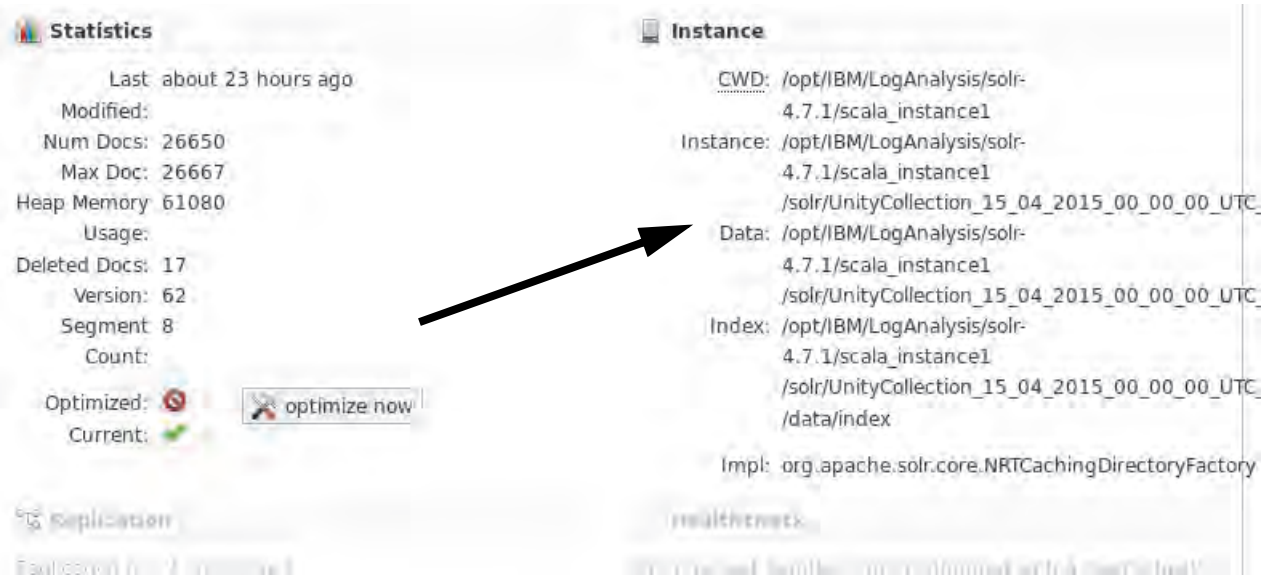
c. Click **Core Selector**, and select one of the shards in your system.



© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Look at the directory structure in the **Instance** summary. This structure matches the file system that you saw in a preceding step.

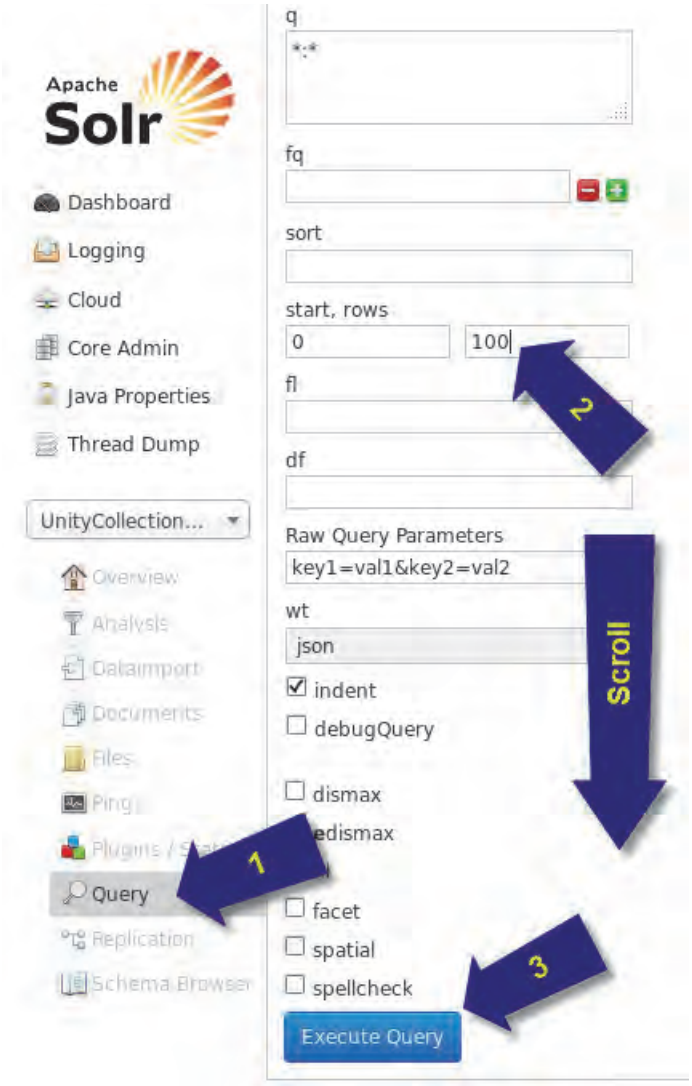


e. Click **Query** in the navigation menu on the left.

f. Enter **100** in the rows field.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

g. Click **Execute Query**. You might have to scroll down to see the Execute Query button.



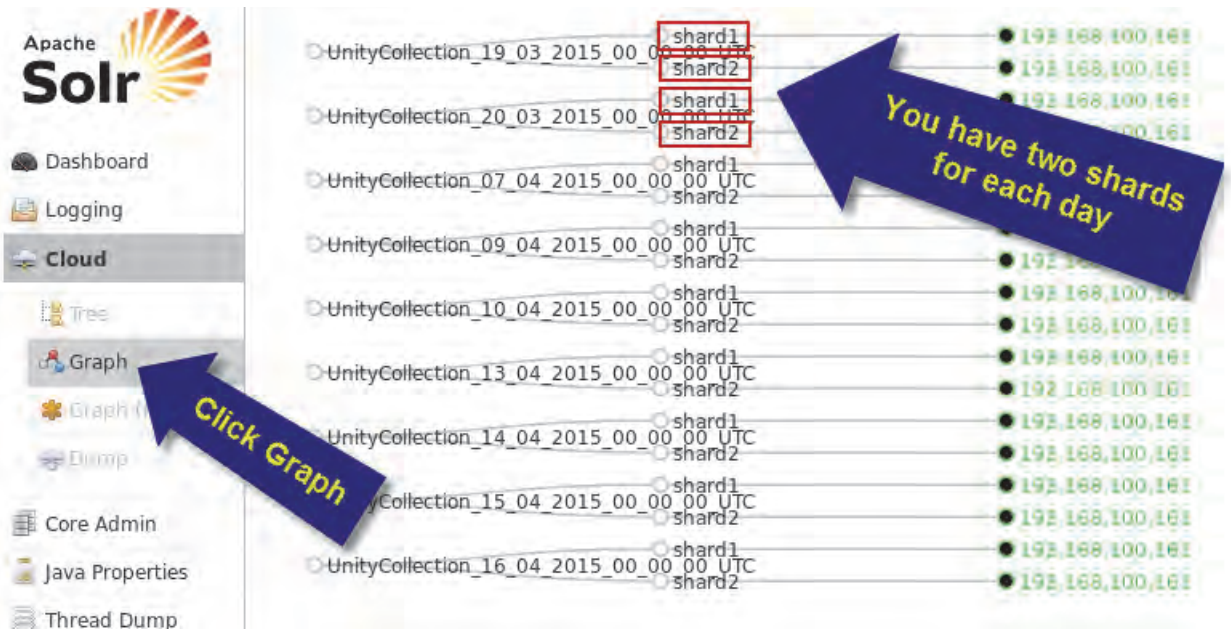
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

h. Scroll down through the search results.


```
{
  "id": "1429124789503_1429124789506_15_75",
  "message_ti": [
    "The com.ibm.tivoli.reporting.ejb.TivoliReportingEJBRemote interface, which is specified fo
  ],
  "datasourceHostname_tf": [
    "host2.tivoli.edu"
  ],
  "timestamp": "2015-03-11T13:32:32.342",
  "threadID_ti": [
    "0000000b"
  ],
  "_writetime": "2015-04-15T13:06:29.5062",
  "_datasource": "WAS_SystemOut",
  "shortname_s": [
    "EJBInjectionB"
  ],
  "severity_ts": "W",
  "msgclassifier_tf": [
    "CWNEN0033W"
  ],
  "logRecord": [
    "[03/11/15 13:32:32:340 UTC] 0000000b EJBInjectionB W   CWNEN0033W: The com.ibm.tivoli.repo
  ],
  "_version_": 1498545955493904400
},
```


Note: This query is showing the last 100 annotated messages that were saved in this shard.

i. Look at a graphical representation of the shards. Click **Cloud > Graph**. Your system is saving data across two shards.



j. Close Firefox.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

4. Edit the Solr configuration to save data over more shards.
   a. Open the **unitysetup.properties** file with a text editor.

```
vi
/opt/IBM/LogAnalysis/wlp/usr/servers/Unity/apps/Unity.war/WEB-INF/
unitysetup.pr operties
```

   b. Find the following two properties.
      - INDEX_NUM_SHARDS
      - COLLECTION_ASYNC_WINDOW

```
#velocity specific properties
# Boolean flag specifying synchronous (true) or asynchronous (false) indexing
asyncIndexing=true

INDEX_NUM_SHARDS=2

# Async time window for creating new time based collection. This value should
NOT be modified by the user
# It can be only an Integer value in hours or days ( < 365 ). If in hours it
has to be a factor of 24 greater than or equal to 6.
# It is specified as nh (n hours) or nd (n days); units being h (hour), or d
(day)
COLLECTION_ASYNC_WINDOW = 1d
##################################################################
```

Note: The number of shards is set to two. The collection window is one day. This is why you have two subdirectories (shards) for each day of data.

   c. Change the **INDEX_NUM_SHARDS** property to **8**.

```
# Boolean flag specifying synchronous (true) or asynchronous (false) indexing
asyncIndexing=true

INDEX_NUM_SHARDS=8

# Async time window for creating new time based collection. This value should
NOT be modified by the user
```

   d. Save and close the file.
   e. Stop IBM Operations Analytics Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -stop
```

   f. Start IBM Operations Analytics Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -start
```

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Important: The new shard configuration takes effect at the start of the next collection window. Remember that the collection window is one day (**`COLLECTION_ASYNC_WINDOW = 1d`**). This setting means that you see the new shard directories at the start of the next day.

Optional steps: Verifying the Solr configuration change

Hint: If you do not want to wait a full day, run the following steps to change the system time to the next day.

5. Change to the root user and change the system clock to the next day.
   a. Open a new terminal window. Run the following command to switch to the **root** user. The password is **object00**.

      ```
      su -
      Password: object00
      ```

   b. Run the following command to view the current system date.

      ```
      date
      Thu Apr 16 19:45:07 UTC 2015
      ```

   c. Run a command like the following example to set the system date to the next day. You must change the date string in the command. Enter the date of the next day.

      ```
      date +%Y%m%d -s "20150417"
      ```

   d. Run the `date` command again to confirm that the system clock was changed.

      ```
      date
      Fri Apr 17 00:00:08 UTC 2015
      ```

   e. Close the terminal window. Complete the rest of the steps in this exercise as the **netcool** user.

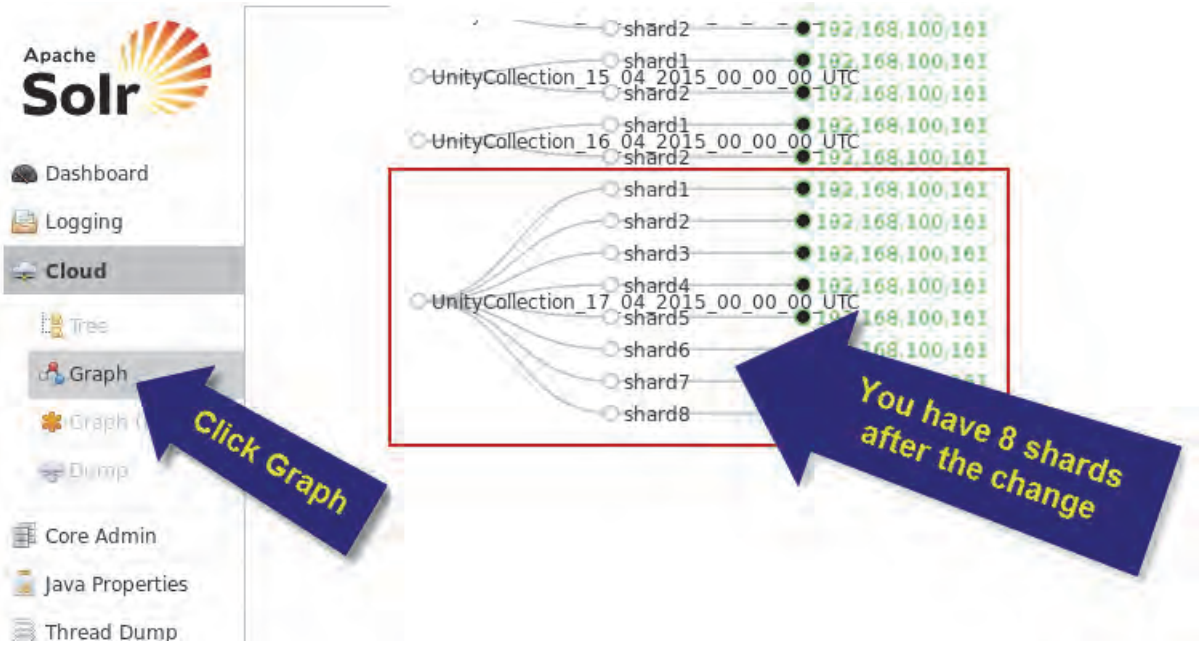
Note: The next steps are optional. These steps show you how to verify the change to the shard configuration. Follow these steps only if you have waited a day after you changed the **INDEX_NUM_SHARDS** property to **8**. You can also use these steps if you changed the system clock to the next day.

6. Run the following command as the **netcool** user to create more log messages in the WAS_SystemOut data source.

   ```
   /software/log_samples/scripts/WAS_Logs.sh
   ```


© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

7. Return to the Solr administration interface to look at the Solr file system and indexed data.
   a. Open a Firefox browser. Enter the following URL:
      http://host2.tivoli.edu:8983/solr
   b. Click **Cloud > Graph**.



   Notice that after the change, and after data was ingested in a new collection window (the day after the change), there are eight shards instead of two.

8. Look at the Solr directory structure that was created to support the new shards.
   a. Change to the following directory:
      `cd /opt/IBM/LogAnalysis/solr-4.7.1/scala_instance1/solr`

© Copyright IBM Corp. 2016

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

b. List the contents of the directory. There is one subdirectory for each shard and each day of log data.

```
ls -l
...
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard1_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard2_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard3_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard4_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard5_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard6_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard7_replica1
drwxr-xr-x 3 netcool ncoadmin 4096 Apr 17 00:01
UnityCollection_17_04_2015_00_00_00_UTC_shard8_replica1

...
```

Note: Notice that you have eight subdirectories (one for each shard) for the current day collection window.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

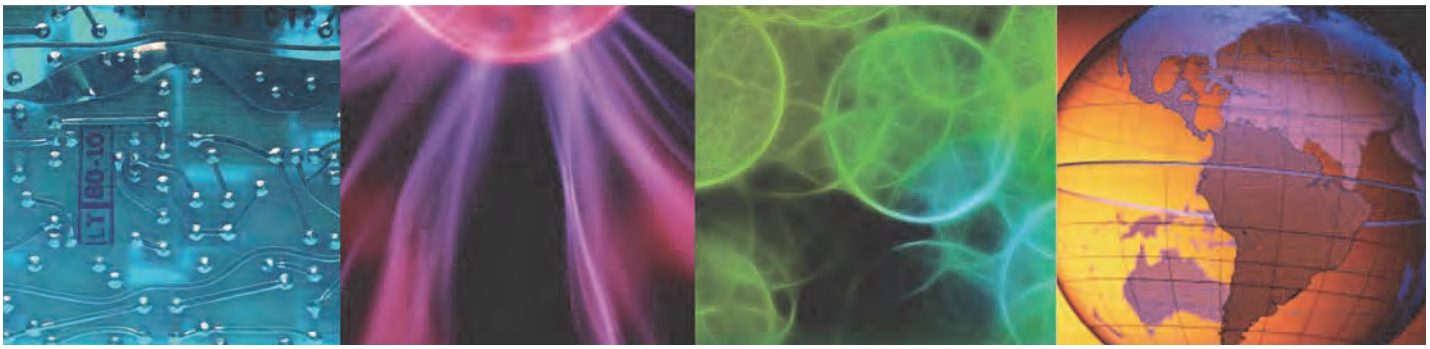
7 Backing up and restoring IBM Operations Analytics Log Analysis exercises

There are no student exercises for this unit.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

© Copyright IBM Corp. 2016
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

TN630G 1.0



ibm.com/training

Authorized IBM Training