EventTracker
Logging in Depth

Enable Auditing in Open LDAP on Linux Server

EventTracker v7.x

Publication Date: Apr 15, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This document describes how to enable auditing for Open LDAP (Lightweight Directory Access Protocol) installed in Linux and forward logs to EventTracker v7.x.

Target Audience

EventTracker users who wish to monitor Open LDAP changes in Linux server.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later, Open LDAP 2.4 or later and rsyslog 5.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

About LDAP

LDAP stands for Lightweight Directory Access Protocol. As the name suggests, it is a lightweight client-server protocol for accessing directory services, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection oriented transfer services.

A directory is similar to a database, but tends to contain more descriptive, attribute-based information. The information in a directory is generally read much more often than it is written. Directories are tuned to give quick-response to high-volume lookup or search operations. They may have the ability to replicate information widely in order to increase availability and reliability, while reducing response time. When directory information is replicated, temporary inconsistencies between the replicas may be OK, as long as they get in sync eventually.

LDAP Logging

The Logging overlay can be used to record all changes on a given backend database and send to EventTracker as syslog.

Enable LDAP Logging

1. Open and edit **rsyslog.conf file** in VI editor.
2. Add the following line to **/etc/rsyslog.conf**

   local4.* /var/log/ldap.log
3. Create empty log file

   touch /var/log/ldap.log
4. Set appropriate permission

   chown ldap:ldap /var/log/ldap.log
5. To rotate log file weekly, add empty file lgap to directory **/etc/logrotate.d**

   touch /etc/logrotate.d/ldap

6. Add appropriate rules for rotation

   ```
   vi /etc/logrotate.d/ldap
   # Logrotate file for LDAP
   # Logrotate file for LDAP
   /var/log/ldap {
   missingok
   compress
   notifempty
   weekly
   rotate 5
   postrotate
   /sbin/service ldap reload
   endscript
   }
   ```

7. Press **Esc** key and enter **:wq** to save the file.

8. Restart rsyslog and LDAP daemons.

   ```
   /etc/init.d/rsyslog restart
   /etc/init.d/ldap restart
   ```

Configure rsyslog to send logs to EventTracker or Remote Host

1. Open and edit **rsyslog.conf** in VI editor.

2. Add the following details at the end of **rsyslog.conf** file, in **cd /etc/rsyslog.conf**.

   ```
   *.*    @@IP Address of remote host:514
   ```

3. Press **Esc** key and enter **:wq** to save the file.

4. Restart the rsyslog service.

   ```
   # service rsyslog restart
   ```

EventTracker Knowledge Pack (KP)

Once LDAP auditing is enabled and Ldap logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v7 to support LDAP monitoring:

Categories:-

- **LDAP: Directory object added:** This category based report provides information related to objects added to LDAP.
- **LDAP: Directory object deleted:** This category based report provides information related to deleted objects from LDAP.
- **LDAP: Directory object modified**: This category based report provides information related to modified objects in LDAP.

Alerts:-

- **LDAP: Object deleted:** This alert is generated when any object is deleted from LDAP.

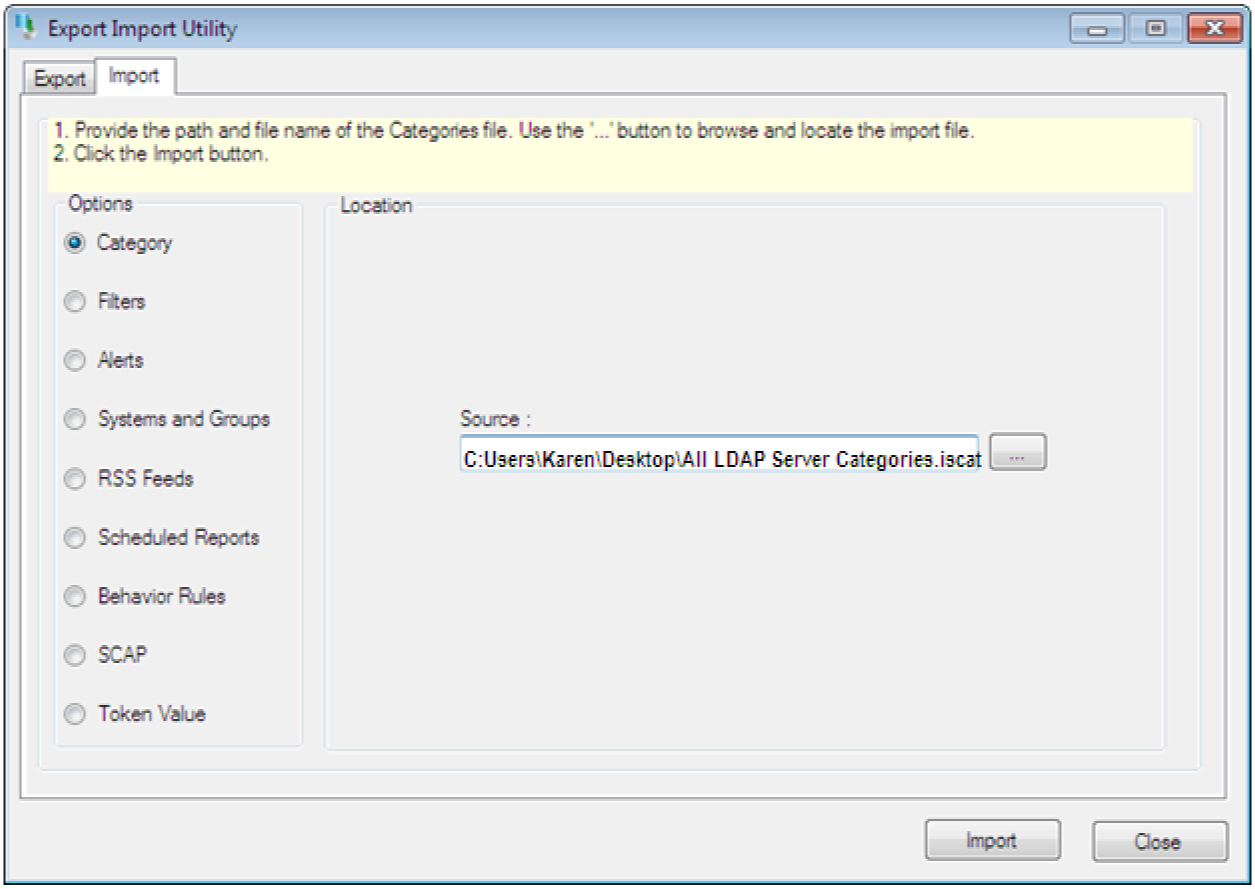
Import LDAP KP to EventTracker

1. Launch EventTracker Control Panel.
2. Double click on the **Export/Import Utility**.
3. Click the **Import** tab.

   Details to import Category/Alert as given below.

To import Category

1. Click **Category** option, and then click the **browse** button.
2. Locate **All LDAP Server Categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category

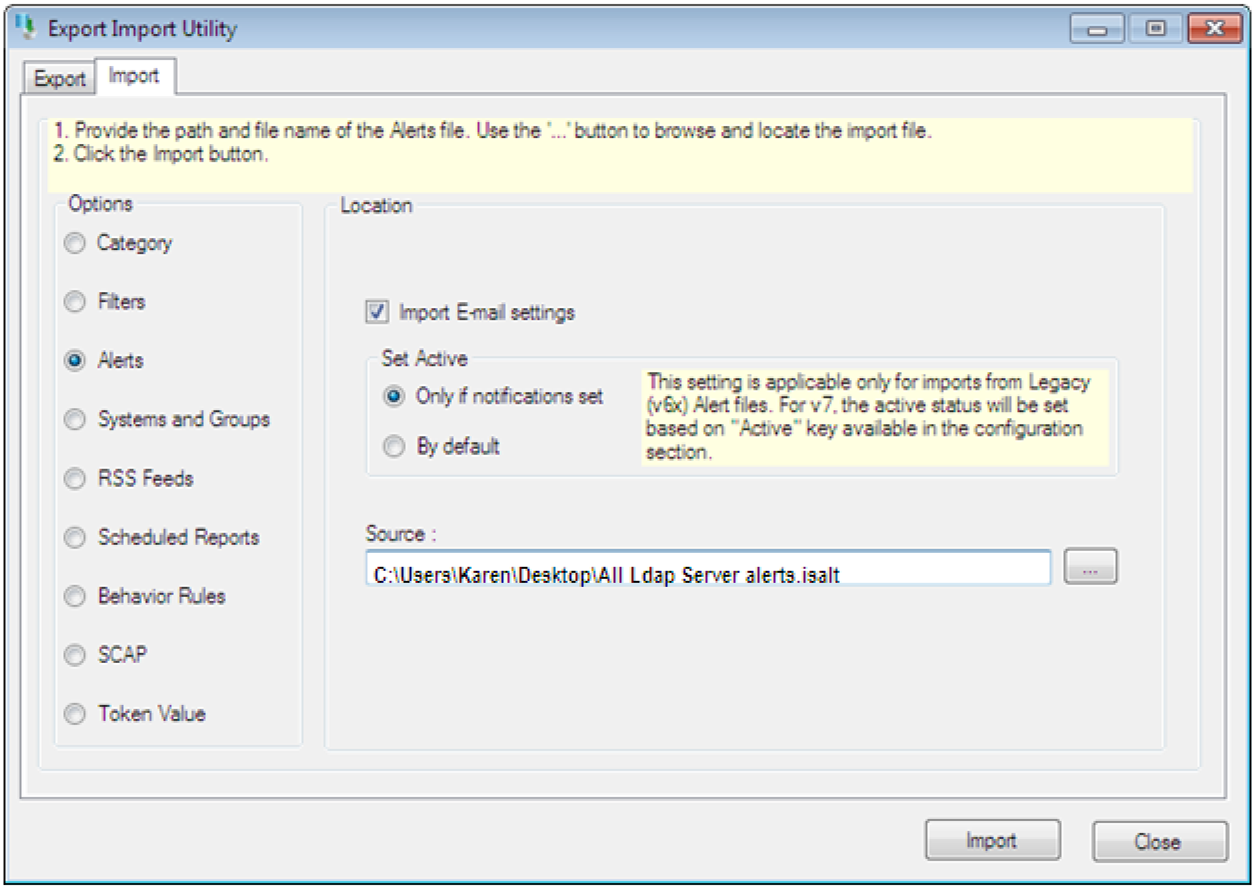
Source : C:\Users\Karen\Desktop\All LDAP Server Categories.iscat

Figure 1

4. Click the **OK** button, and then click **Close** button.

To import Alerts

1. Click **Alert** option, and then click the **browse** button.
2. Locate **All Ldap Server alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

☑ Import E-mail settings

● Only if notifications set
○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : C:\Users\Karen\Desktop\All Ldap Server alerts.isalt

Figure 2

4. Click **OK**, and then click **Close** button.

Verify imported Categories and Alerts in EventTracker

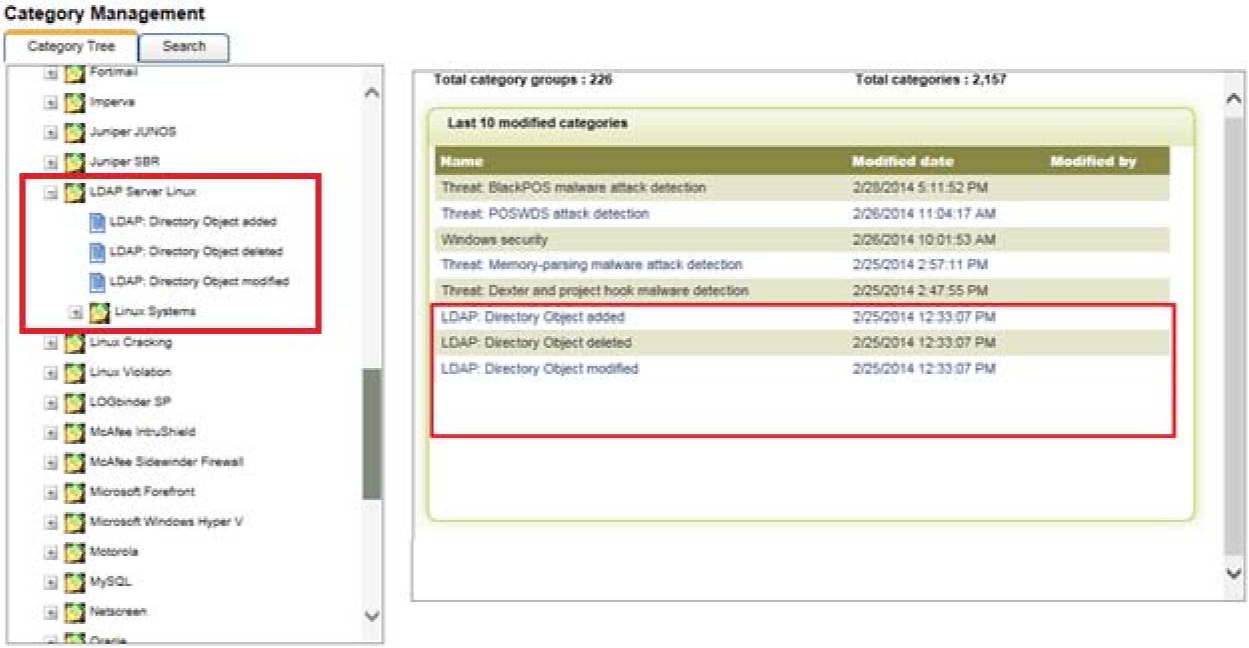
Verify Categories

1. Logon to EventTracker Enterprise.

2. To verify the categories, select the **Admin** menu, and then select **Category**.

3. In **Category Tree**, expand **LDAP Server Linux** node.

   The imported categories are displayed.



Total category groups : 226   Total categories : 2,157

Last 10 modified categories

Name	Modified date	Modified by
Threat: BlackPOS malware attack detection	2/28/2014 5:11:52 PM	
Threat: POSWDS attack detection	2/26/2014 11:04:17 AM	
Windows security	2/26/2014 10:01:53 AM	
Threat: Memory-parsing malware attack detection	2/25/2014 2:57:11 PM	
Threat: Dexter and project hook malware detection	2/25/2014 2:47:55 PM	
LDAP: Directory Object added	2/25/2014 12:33:07 PM	
LDAP: Directory Object deleted	2/25/2014 12:33:07 PM	
LDAP: Directory Object modified	2/25/2014 12:33:07 PM	

Figure 3

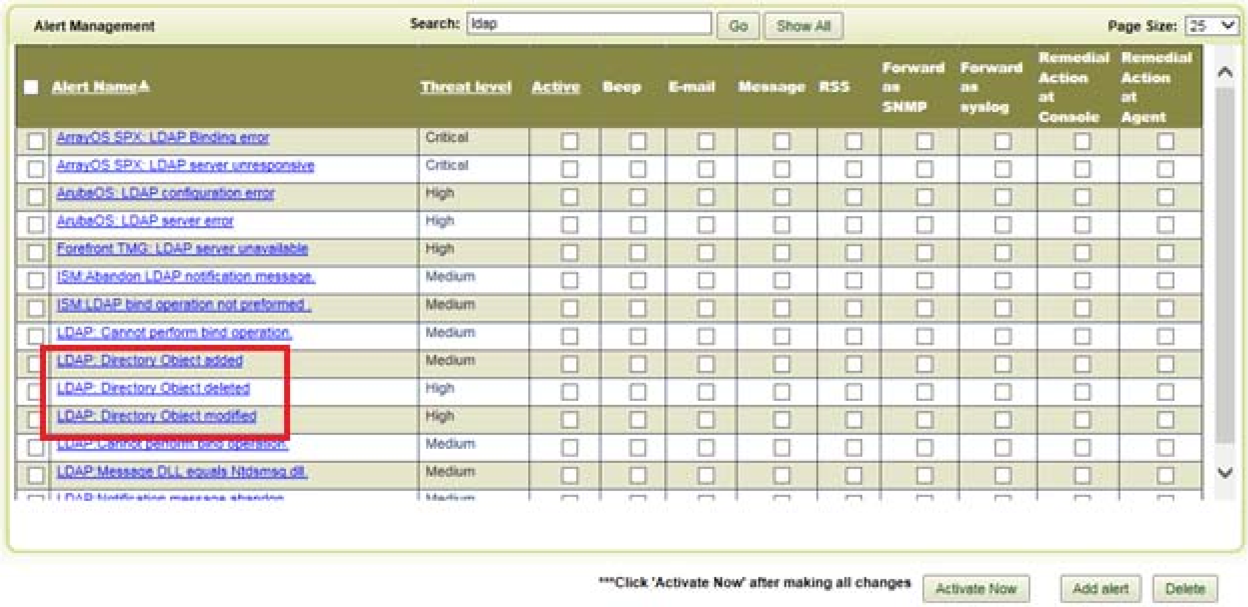
Verify Alerts

1. Logon to EventTracker Enterprise.

2. To verify alerts, click the **Admin** menu and then select **Alerts**.

3. In **Search:** box, enter the search criteria '**LDAP**'.

   All alerts related to LDAP display.



Alert Management

Search: ldap

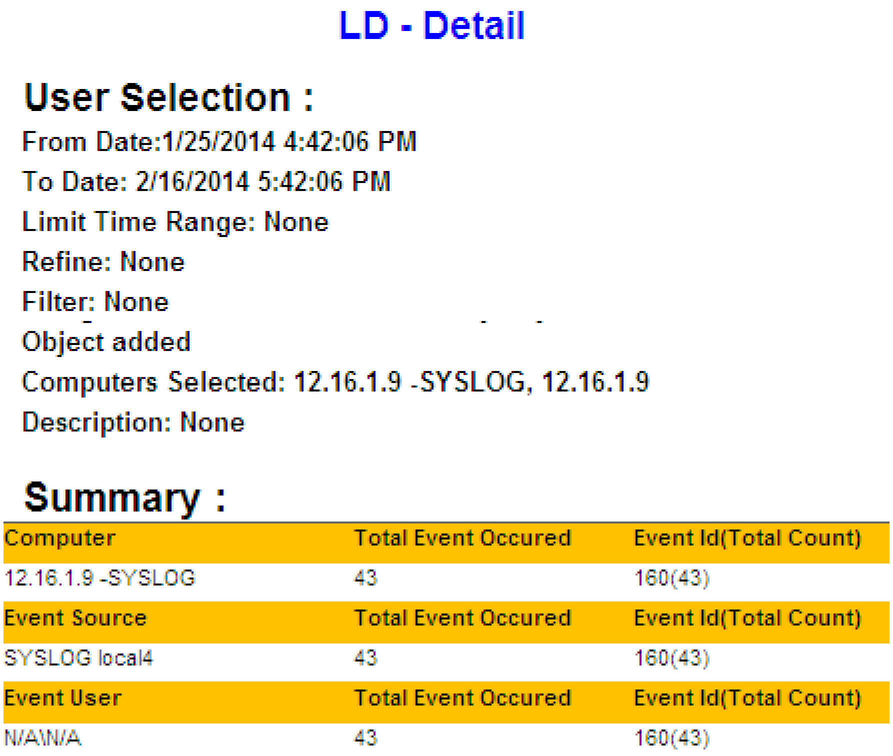
□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
□	ArrayOS SPX: LDAP Binding error	Critical	□	□	□	□	□	□	□	□	□
□	ArrayOS SPX: LDAP server unresponsive	Critical	□	□	□	□	□	□	□	□	□
□	ArubaOS: LDAP configuration error	High	□	□	□	□	□	□	□	□	□
□	ArubaOS: LDAP server error	High	□	□	□	□	□	□	□	□	□
□	Forefront TMG: LDAP server unavailable	High	□	□	□	□	□	□	□	□	□
□	ISM Abandon LDAP notification message.	Medium	□	□	□	□	□	□	□	□	□
□	ISM LDAP bind operation not preformed.	Medium	□	□	□	□	□	□	□	□	□
□	LDAP: Cannot perform bind operation.	Medium	□	□	□	□	□	□	□	□	□
□	LDAP: Directory Object added	Medium	□	□	□	□	□	□	□	□	□
□	LDAP: Directory Object deleted	High	□	□	□	□	□	□	□	□	□
□	LDAP: Directory Object modified	High	□	□	□	□	□	□	□	□	□
□	LDAP: Cannot perform bind operation.	Medium	□	□	□	□	□	□	□	□	□
□	LDAP Message DLL equals Ntdsmsg dll.	Medium	□	□	□	□	□	□	□	□	□
□	LDAP Notification message abandon	Medium	□	□	□	□	□	□	□	□	□

***Click 'Activate Now' after making all changes

Figure 4

Sample Reports

The details of sample Summary Report is given below



LD - Detail

User Selection :

From Date:1/25/2014 4:42:06 PM

To Date: 2/16/2014 5:42:06 PM

Limit Time Range: None

Refine: None

Filter: None

Object added

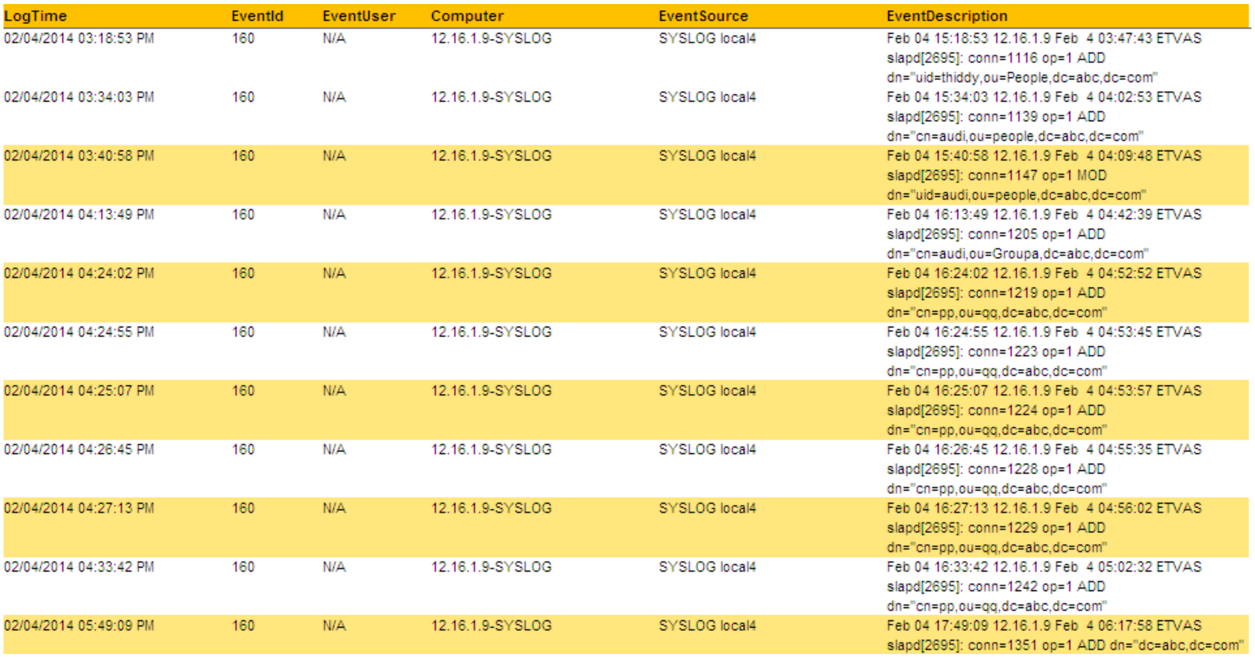
Computers Selected: 12.16.1.9 -SYSLOG, 12.16.1.9

Description: None

Summary :

Computer	Total Event Occured	Event Id(Total Count)
12.16.1.9 -SYSLOG	43	160(43)
Event Source	Total Event Occured	Event Id(Total Count)
SYSLOG local4	43	160(43)
Event User	Total Event Occured	Event Id(Total Count)
N/A\N/A	43	160(43)

Information regarding Detail Reports is given below.



LogTime	EventId	EventUser	Computer	EventSource	EventDescription
02/04/2014 03:18:53 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 15:18:53 12.16.1.9 Feb 4 03:47:43 ETVAS slapd[2695]: conn=1116 op=1 ADD dn="uid=thiddy,ou=People,dc=abc,dc=com"
02/04/2014 03:34:03 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 15:34:03 12.16.1.9 Feb 4 04:02:53 ETVAS slapd[2695]: conn=1139 op=1 ADD dn="cn=audi,ou=people,dc=abc,dc=com"
02/04/2014 03:40:58 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 15:40:58 12.16.1.9 Feb 4 04:09:48 ETVAS slapd[2695]: conn=1147 op=1 MOD dn="uid=audi,ou=people,dc=abc,dc=com"
02/04/2014 04:13:49 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:13:49 12.16.1.9 Feb 4 04:42:39 ETVAS slapd[2695]: conn=1205 op=1 ADD dn="cn=audi,ou=Groupa,dc=abc,dc=com"
02/04/2014 04:24:02 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:24:02 12.16.1.9 Feb 4 04:52:52 ETVAS slapd[2695]: conn=1219 op=1 ADD dn="cn=pp,ou=qq,dc=abc,dc=com"
02/04/2014 04:24:55 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:24:55 12.16.1.9 Feb 4 04:53:45 ETVAS slapd[2695]: conn=1223 op=1 ADD dn="cn=pp,ou=qq,dc=abc,dc=com"
02/04/2014 04:25:07 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:25:07 12.16.1.9 Feb 4 04:53:57 ETVAS slapd[2695]: conn=1224 op=1 ADD dn="cn=pp,ou=qq,dc=abc,dc=com"
02/04/2014 04:26:45 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:26:45 12.16.1.9 Feb 4 04:55:35 ETVAS slapd[2695]: conn=1228 op=1 ADD dn="cn=pp,ou=qq,dc=abc,dc=com"
02/04/2014 04:27:13 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:27:13 12.16.1.9 Feb 4 04:56:02 ETVAS slapd[2695]: conn=1229 op=1 ADD dn="cn=pp,ou=qq,dc=abc,dc=com"
02/04/2014 04:33:42 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 16:33:42 12.16.1.9 Feb 4 05:02:32 ETVAS slapd[2695]: conn=1242 op=1 ADD dn="cn=pp,ou=qq,dc=abc,dc=com"
02/04/2014 05:49:09 PM	160	N/A	12.16.1.9-SYSLOG	SYSLOG local4	Feb 04 17:49:09 12.16.1.9 Feb 4 06:17:58 ETVAS slapd[2695]: conn=1351 op=1 ADD dn="dc=abc,dc=com"