Abstract

This guide provides instructions to configure Centrify Server Suite to send syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and Centrify Server Suite 2015.

Audience

Centrify Server Suite users, who wish to forward Events to EventTracker Manager and monitor events using Event Tracker.

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

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

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract .................................................................................................................................................. 1

Overview ................................................................................................................................................ 3

Prerequisites ........................................................................................................................................... 3

Configure syslog to send Centrify Unix agent syslog events to EventTracker server .................... 3

Configure Centrify Windows Agent machine to send events to EventTracker Manager ................ 4

EventTracker Knowledge Pack ............................................................................................................. 6

Categories .............................................................................................................................................. 6

Unix Agent ............................................................................................................................................. 6

Windows Agent .................................................................................................................................... 7

Alerts ..................................................................................................................................................... 8

Reports .................................................................................................................................................. 8

Import Centrify Server Suite Knowledge Pack into EventTracker ..................................................... 9

Import Category ..................................................................................................................................... 9

Import Alerts ........................................................................................................................................ 11

Import Token Templates ...................................................................................................................... 12

Import Reports ...................................................................................................................................... 13

Verify Centrify Server Suite knowledge pack in EventTracker ........................................................... 14

Verify Categories .................................................................................................................................. 14

Verify Alerts ......................................................................................................................................... 14

Verify Tokens ....................................................................................................................................... 16

Verify Reports ....................................................................................................................................... 16

Create Dashboards in EventTracker .................................................................................................... 17

Schedule Reports ................................................................................................................................. 17

Create Dashlets .................................................................................................................................... 19

Sample Dashboards ............................................................................................................................ 23

Sample Reports ...................................................................................................................................... 24
Overview

Centrify Server Suite secures the industry's broadest range of mission-critical servers from identity-related insider risks and outsider attacks, making security and regulatory compliance repeatable and sustainable. The solution leverages existing Active Directory infrastructure to centrally manage authentication, access controls, privileged identities, policy enforcement and compliance for on-premises and cloud resources.

Prerequisites

- EventTracker v7.x should be installed.
- Centrify Server Suite should be installed.
- Centrify Unix Agent should be Installed.
- Centrify Windows Agent should be installed.

Configure syslog to send Centrify Unix agent syslog events to EventTracker server

1. Open `rsyslog.conf` in **VI Editor**. (with required privilege to edit rsyslog.conf file)
2. Insert the following entry to specify the EventTracker Manager.
   
   If required change the IP address and port number based on requirement.
   
   **E.g.:**
   
   ```
   auth.INFO @@172.16.1.1:514
   auth = Syslog facility
   INFO = priority
   192.168.1.1 = IP address of EventTracker Manager
   514 = default syslog listening port number of EventTracker Manager
   **NOTE:**
   Use ‘@@’ for TCP and ‘@’ for UDP to forward log to EventTracker. It can support both.
   ```
3. Save and restart the **rsyslog** service
Configure Centrify Windows Agent machine to send events to EventTracker Manager

Install EventTracker Agent on Centrify system. Please refer EventTracker Agent Deployment Manual for more details in order to install the Agent.

To create filter exception in agent, please follow the steps given below.

1. Launch EventTracker Agent configuration.
2. Click Event Filters tab, and then click Filter Exception.

![EventTracker Agent Configuration](image)

3. Click the New button.
Integrate Centrify Server Suite

Event Details window displays.

4. In Log Type: drop down, select Application.

5. In Match in Source: box, enter Centrify AuditTrail.

Similarly create two new Filter Exceptions for Match in Source: as DirectAuthorize Agent and DirectAudit Agent.

6. Click OK, and then click the Save button.
EventTracker Knowledge Pack

Categories

Unix Agent

- **Centrify: Adclient agent started** - This category based report provides information related to when adclient agent service has started.

- **Centrify: Adclient agent stopped** - This category based report provides information related to adclient agent stopped

- **Centrify: Auditing Enabled** - This category based report provides information related to Centrify Unix agent auditing enabled.

- **Centrify: Configuration settings reloaded** - This category based report provides information related to configuration settings reloaded in Unix agent.

- **Centrify: Dzdo execution denied** - This category based report provides information related to dzdo (command for Centrify privileged access) command execution denied.

- **Centrify: Dzdo execution granted** - This category based report provides information related to dzdo (command for Centrify privileged access) command execution granted.

- **Centrify: Local cache flushed** - This category based report provides information related to local cache flushed.

- **Centrify: PAM Account management granted** - This category based report provides information related to PAM account management granted.

- **Centrify: PAM Authentication Failed** - This category based report provides information related to PAM authentication failures.

- **Centrify: PAM Authentication successful** - This category based report provides information related to successful PAM authentications.

- **Centrify: PAM Session closed** - This category based report provides information related to closed PAM sessions.

- **Centrify: PAM Session opened** - This category based report provides information related to opened PAM sessions.

- **Centrify: SSHD denied** - This category based report provides information related to Centrify SSHD denied.
- **Centrify: SSHD granted** - This category based report provides information related to Centrify SSHD granted.

**Windows Agent**

- **Centrify: Create desktop failure** - This category based report provides information related to Centrify desktop creation failure.
- **Centrify: Create desktop success** - This category based report provides information related to Centrify desktop creation success.
- **Centrify: DirectAuthorize agent started** - This category based report provides information related to started DirectAuthorize agents.
- **Centrify: DirectAuthorize agent stopped** - This category based report provides information related to stopped DirectAuthorize agents.
- **Centrify: Join to zone success** - This category based report provides information about successfully joined agents to zone.
- **Centrify: Leave from zone failed** - This category based report provides information related to agent which tries to leave zone, but failed.
- **Centrify: Network access success** - This category based report provides information related to successfully accessed network resources.
- **Centrify: Remote login failure** - This category based report provides information related to failed remote logins.
- **Centrify: Remote login success** - This category based report provides information related to successful remote logins.
- **Centrify: Run as role attempt failed** - This category based report provides information related to failed run as role attempts.
- **Centrify: Run as role attempt succeed** - This category based report provides information related to successful Run as role attempts.
- **Centrify: Switch desktop success** - This category based report provides information related to successful switching between Centrify desktop and default user desktop.
Alerts

- **Centrify: Adclient agent stopped** - This alert is generated by Centrify Linux/Unix agent when Unix agent service stopped.

- **Centrify: Configuration settings reloaded** - This alert is generated by Centrify Linux/Unix agent when configuration settings reloaded.

- **Centrify: Create desktop failure** - This alert is generated by Centrify Windows Agent when user failed to create desktop.

- **Centrify: DirectAuthorize agent stopped** - This alert is generated by Centrify Windows Agent when DirectAuthorize Agent service stopped.

- **Centrify: Dzdo execution denied** - This alert is generated by Centrify Linux/Unix agent when dzdo command execution denied.

- **Centrify: Dzdo execution granted** - This alert is generated by Centrify Linux/Unix agent when dzdo execution granted.

- **Centrify: Join to zone success** - This alert is generated by Centrify Windows Agent when agent successfully joined to the zone.

- **Centrify: PAM Authentication failed** - This alert is generated by Centrify Linux/Unix agent when PAM authentication is failed.

- **Centrify: Remote login failed** - This alert is generated by Centrify Windows Agent when remote log in failed.

- **Centrify: Run as role attempt failed** - This alert is generated by Centrify Windows Agent when Run as role attempt failed

- **Centrify: SSHD denied** - This alert is generated by Centrify Linux/Unix agent when Centrify SSHD denied.

Reports

- **Centrify Adclient agent started**: This report provides information related to when adclient agent service has started.

- **Centrify Adclient agent stopped**: This report provides information related to adclient agent stopped.
• **Centrify Dzdo execution denied**: This report provides information related to dzdo (command for Centrify privileged access) command execution denied.

• **Centrify Dzdo execution granted**: This report provides information related to dzdo (command for Centrify privileged access) command execution granted.

• **Centrify PAM Account management granted**: This report provides information related to PAM account management granted.

• **Centrify PAM Authentication Failed**: This report provides information related to PAM authentication failures.

• **Centrify PAM Authentication successful**: This report provides information related to successful PAM authentications.

• **Centrify PAM Session closed**: This report provides information related to closed PAM sessions.

• **Centrify PAM Session opened**: This report provides information related to opened PAM sessions.

• **Centrify SSHD denied**: This report provides information related to Centrify SSHD denied.

• **Centrify SSHD granted**: This report provides information related to Centrify SSHD granted.

**Import Centrify Server Suite Knowledge Pack into EventTracker**

1. Launch EventTracker Control Panel.

2. Double click ExportImport Utility, and then click the Import tab.

   Import *Category/Alert/Flex reports/Token/Knowledge Object* as given below.

**Import Category**

1. Click Category option, and then click the browse button.
2. Locate **All Centrify Server Suite AD client group categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

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

1. Click Alert option, and then click the ‘browse’ button.

![Export Import Utility](Image)

Figure 6

2. Locate All Centrify Server Suite AD client group of alerts.isalt file, and then click the Open button.

3. To import alerts, click the Import button. EventTracker displays success message.

![Export Import Utility](Image)

Figure 7

4. Click OK, and then click the Close button.
Import Token Templates

1. Click the **Token Value** option, and then click the ‘browse’ button.

![Figure 8](image)

2. Locate **All Centrify Server Suite tokens.istoken** file, and then click the **Open** button.
3. To import tokens, click the **Import** button.
   
   EventTracker displays success message.

![Figure 9](image)

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

1. Click Reports option, and then click the ‘browse’ button.
2. Locate All Centrify Server Suite group reports.issch file, and then click the Open button

![Figure 10](image)

3. To import reports, click the Import button. EventTracker displays success message.

![Figure 11](image)

4. Click OK, and then click the Close button.
Verify Centrify Server Suite knowledge pack in EventTracker

Verify Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. To view the imported categories, in the Category Tree, expand Centrify Server Suite group, expand Unix Agent and Windows Agent subgroup folders.

![Category Management](image)

Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search box, type Centrify, and then click the GO button.
   Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

![Successfully saved configuration.](image)

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Verify Tokens

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.
   The imported Centrify Server Suite tokens are added in Token-Value Groups list.

   ![Parsing Rule](image)

   **Figure 15**

   **NOTE:** Please specify appropriate systems in Report wizard for better performance.

Verify Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click Centrify Server Suite group folder.

   Scheduled Reports are displayed in the Reports configuration pane.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **Centrify Server Suite** in report groups. Check **Defined** option.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.

   ![Select columns to persist](image)

   **Figure 20**

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

**Create Dashlets**

1. **EventTracker 8** is required to configure flex dashboard.

2. Open **EventTracker** in browser and logon.

   ![EventTracker dashboard](image)

   **Figure 21**
3. Navigate to Dashboard>Flex.

Flex Dashboard pane is shown.

4. Click + to add a new dashboard.

Flex Dashboard configuration pane is shown.

5. Fill fitting title and description and click Save button.

6. Click 🔄 to configure a new flex dashlet.

Widget configuration pane is shown.
7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.

Evaluated chart is shown.
16. If satisfied, click **Configure** button.

17. Click ‘customize’ to locate and choose created dashlet

18. Click **+** to add dashlet to earlier created dashboard.
Sample Dashboards

1. Centrify-Server-Suite Adclient Status

![Figure 27](image)

2. Centrify-Server-Suite PAM Authentication Status

![Figure 28](image)
### Sample Reports

1. **Centrify-Server-Suite PAM Authentication Status**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User</th>
<th>Client IP</th>
<th>Service</th>
<th>TTY</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/13/2015 09:57:20 PM</td>
<td>Jack</td>
<td>none</td>
<td>gdm-password</td>
<td>0</td>
<td>DENIED</td>
<td>There's error in PAM Conversation</td>
</tr>
<tr>
<td>10/13/2015 09:57:20 PM</td>
<td>Johnson</td>
<td>none</td>
<td>su</td>
<td>pts/0</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/13/2015 09:57:20 PM</td>
<td>michel</td>
<td>192.168.1.20</td>
<td>sshd</td>
<td>ssh</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/13/2015 09:57:20 PM</td>
<td>mary</td>
<td>192.168.1.20</td>
<td>sshd</td>
<td>ssh</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/13/2015 09:57:20 PM</td>
<td>john</td>
<td>none</td>
<td>su</td>
<td>pts/0</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/13/2015 09:57:21 PM</td>
<td>Harsh</td>
<td>192.168.1.40</td>
<td>sshd</td>
<td>ssh</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/14/2015 09:49:41 AM</td>
<td>Harsh</td>
<td>192.168.1.40</td>
<td>sshd</td>
<td>ssh</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/14/2015 09:49:41 AM</td>
<td>Jack</td>
<td>none</td>
<td>gdm-password</td>
<td>0</td>
<td>DENIED</td>
<td>There's error in PAM Conversation</td>
</tr>
<tr>
<td>10/14/2015 09:49:41 AM</td>
<td>Johnson</td>
<td>none</td>
<td>su</td>
<td>pts/0</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/14/2015 09:49:43 AM</td>
<td>michel</td>
<td>192.168.1.20</td>
<td>sshd</td>
<td>ssh</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/14/2015 09:49:43 AM</td>
<td>mary</td>
<td>192.168.1.20</td>
<td>sshd</td>
<td>ssh</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/14/2015 09:49:43 AM</td>
<td>john</td>
<td>none</td>
<td>su</td>
<td>pts/0</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/14/2015 09:50:29 AM</td>
<td>Jack</td>
<td>none</td>
<td>gdm-password</td>
<td>0</td>
<td>DENIED</td>
<td>There's error in PAM Conversation</td>
</tr>
<tr>
<td>10/14/2015 09:50:29 AM</td>
<td>Harsh</td>
<td>192.168.1.40</td>
<td>sshd</td>
<td>ssh</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/14/2015 09:50:29 AM</td>
<td>Johnson</td>
<td>none</td>
<td>su</td>
<td>pts/0</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/14/2015 09:50:30 AM</td>
<td>john</td>
<td>none</td>
<td>su</td>
<td>pts/0</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/14/2015 09:50:30 AM</td>
<td>michel</td>
<td>192.168.1.20</td>
<td>sshd</td>
<td>ssh</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/14/2015 09:50:30 AM</td>
<td>mary</td>
<td>192.168.1.20</td>
<td>sshd</td>
<td>ssh</td>
<td>GRANTED</td>
<td></td>
</tr>
<tr>
<td>10/14/2015 09:50:31 AM</td>
<td>Harsh</td>
<td>192.168.1.40</td>
<td>sshd</td>
<td>ssh</td>
<td>DENIED</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>10/14/2015 09:50:31 AM</td>
<td>Jack</td>
<td>none</td>
<td>gdm-password</td>
<td>0</td>
<td>DENIED</td>
<td>There's error in PAM Conversation</td>
</tr>
</tbody>
</table>

Figure 27
2. **Centrify-Server-Suite Adclient Status**

![Integrate Centrify Server Suite](image)

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>service name</th>
<th>service status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/14/2015 10:32:49 AM</td>
<td>CENTRIFY</td>
<td>maria</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:32:49 AM</td>
<td>CENTRIFY</td>
<td>johnson</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:32:49 AM</td>
<td>CENTRIFY</td>
<td>johanna</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:32:49 AM</td>
<td>CENTRIFY</td>
<td>jula</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:32:49 AM</td>
<td>CENTRIFY</td>
<td>robert</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:32:49 AM</td>
<td>CENTRIFY</td>
<td>michel</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:32:50 AM</td>
<td>CENTRIFY</td>
<td>maria</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:32:50 AM</td>
<td>CENTRIFY</td>
<td>johanna</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:32:50 AM</td>
<td>CENTRIFY</td>
<td>johnson</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:32:51 AM</td>
<td>CENTRIFY</td>
<td>julio</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:32:51 AM</td>
<td>CENTRIFY</td>
<td>robert</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:32:51 AM</td>
<td>CENTRIFY</td>
<td>michel</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:36:53 AM</td>
<td>CENTRIFY</td>
<td>johanna</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:36:53 AM</td>
<td>CENTRIFY</td>
<td>maria</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:36:53 AM</td>
<td>CENTRIFY</td>
<td>johnson</td>
<td>adclient</td>
<td>started</td>
</tr>
<tr>
<td>10/14/2015 10:36:54 AM</td>
<td>CENTRIFY</td>
<td>julio</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:36:54 AM</td>
<td>CENTRIFY</td>
<td>robert</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:36:54 AM</td>
<td>CENTRIFY</td>
<td>michel</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:36:55 AM</td>
<td>CENTRIFY</td>
<td>julio</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:36:55 AM</td>
<td>CENTRIFY</td>
<td>robert</td>
<td>adclient</td>
<td>stopped</td>
</tr>
<tr>
<td>10/14/2015 10:36:55 AM</td>
<td>CENTRIFY</td>
<td>michel</td>
<td>adclient</td>
<td>stopped</td>
</tr>
</tbody>
</table>

Figure 28