# RSA NetWitness Platform

Event Source Log Configuration Guide



# Salesforce

Last Modified: Tuesday, November 5, 2019

# **Event Source Product Information:**

Vendor: Salesforce Event Source: CRM Versions: API v1.0

#### **RSA Product Information:**

Supported On: Security Analytics 10.6.2 and later Event Source Log Parser: cef

Note: The CEF parser parses this event source as device.type=salesforce

Collection Method: Plugin Framework Event Source Class.Subclass: Host.Cloud This document contains the following sections:

- Getting Started with NetWitness and Salesforce Integration
- Configure the Salesforce Event Source
- Set Up the Salesforce Event Source in RSA NetWitness
- Salesforce Collection Configuration Parameters

# Getting Started with NetWitness and Salesforce Integration

The Salesforce event monitoring product gathers information about your Salesforce organization's operational events. You can use this information to analyze usage trends and user behavior. You can interact with event monitoring data by querying fields on the **EventLogFile** object (such as **Event Type** and **LogDate**). To view the underlying event data, query the **LogFile** field. The Event Type determines the schema of this field. For more information, see EventLogFile Supported Event Types on the Salesforce Developers Website.

# **Configure the Salesforce Event Source**

This document describes how to configure the Salesforce event source using either the Classic View or the Lightning Experience View:

- Configure the Salesforce Event Source using Classic View or,
- Configure the Salesforce Event Source using Lightning Experience View

# **Configure the Salesforce Event Source using Classic View**

To configure Salesforce, you must complete these tasks:

- I. Create a Salesforce connected app (Classic)
- II. Create a custom read-only profile (Classic)
- III. Create a user under Salesforce admin account (Classic)

#### Create a Salesforce connected app (Classic)

- 1. Log into to your Salesforce account through Salesforce portal: login.salesforce.com
- 2. In Salesforce Classic view, click on the Setup tab as shown here:



3. In Quick Find/ Search box enter Apps, then select Apps (under Build | Create).

Home Ch	atter +
Apps	0 Q
	Expand All   Collapse All
Administer	
	pps tod Apps
Connec	ted Apps OAuth
Usage	and Apps OAuth
Арр Ме	nu
🔽 Google Ap	ps
Google	Apps Settings
Build	
Create	
Apps	

4. In the Connected Apps section, click New.

Connected A	pps	New
Action	Connected App Name	
Edit   Manage	Logcollector	
Edit   Manage	RSA_Logcollector	
Edit   Manage	<u>RsaNW_test</u>	
Edit   Manage	TestCA	

5. Make sure the following settings are defined in Salesforce to enable your new app:

Setting	Value
Connected App Name	Enter a name for the app, for example Logcollector.
API Name	This setting is populated automatically with the Connected App Name you enter.
Contact Email	Enter a valid email address.
Enable OAuth Settings	Make sure this is selected.
Callback URL	Enter the callback URL (endpoint) that Salesforce calls back to your application during OAuth. This is the OAuth redirect URI. Depending on which OAuth flow you use, the URL is typically the one that a user's browser is redirected to after successful authentication. Because this URL is used for some OAuth flows to pass an access token, the URL must use secure HTTPS or a custom URI scheme.
Selected OAuth Scopes	Select Access and manage your data (api).

6. Click Save to complete your Connected App setup.

	Save Cancel
<b>Basic Information</b>	
Connected	App Name LCTest
	API Name LCTest
Co	ntact Email your@email.com
Cor	tact Phone
Logo	mage URL 🕜
	Upload logo image or <u>Choose one of our sample logos</u>
	Icon URL 🥝
	Choose one of our sample logos
	Info URL
I	Description 🥥
<ul> <li>API (Enable OAuth Settings)</li> </ul>	
Enable OAuth Settings 🖉	
Enable for Device Flow	Ilsafa con
4	► 4
Use digital signatures	
Selected CAuth Scopes	Available Odusth Senses Selected Odusth Senses
Ac Ac Ac Ac Ac Ac Bill Ful Per Per Per	se add manage your Shafer (ada (chailer_ga)) as and manage your Whom (data) (cover, ga)) as and manage your Whom (data) (cover, ga)) as coursed previous discriments (cir. profile, email, address, phone) access (by our manage interfer (open)) access (by our manage interfer (open)) de access (b coultim applications (viewallocce)) de access (b coultim applications (viewallocce)) de access (b coultim applications (viewallocce)) de access (b coultim applications (viewallocce)) w
Include ID Tokeno	
Enable Single Logouto	

## New Connected App

- 7. After you save the connected app, you are redirected to a new page. Click **Continue**.
- 8. From this page, you can copy your Consumer Key. Select **Click to reveal** to see your Consumer Secret, and copy that as well.

**Note:** You need the Consumer Key and Consumer Secret values later, while configuring **Client ID** and **Client Secret** values in RSA NetWitness.

Connected App Name				
« Back to List: Custom Apps				
	Edit	elete Manage		
Allow from 2-10 minutes for your changes t	to take effect on the server before using the connect	ted app.		
	Version	1.0		
	API Name	Logcollector		
	Created Date	1/2/2018 5:21 AM		
		By: Martin and Antonio		
	Contact Email	your@email.com		
	Contact Phone	100010 5 01 401		
	Last Modified Date	1/2/2018 5:21 AM		
	Description	BY: STARE ROOM STOR		
	Description			
	INIO ORE			
▼ API (Enable OAuth Settings)				
Consumer Key			Consumer Secret	Click to reveal
Selected OAuth Scopes	Access and manage your data (api)		Callback URL	https://lcsfdc.com
	Full access (full)			
Frankla for Davies Flow	Allow access to your unique identifier (openid)		Denvice Connect for Web Connect Flow	
Enable for Device Flow			Require secret for web server Flow	4
Token Valid for	0 Hour(s)		Include Custom Attributes	
Include Custom Permissions				
Enable Single Logout	Single Logout disabled			

After you create the connected app, you need to edit its policies, as described in the following procedure.

#### To edit the policies for a connected app:

1. Click on Connected Apps under Manage Apps tab as shown below:

salesforce	earch Search	
Home Chatter +		
Quick Find / Search 0 Q Expand All   Collapse All	Connected Apps Manage access to apps that connect to this Salesforce organization.	
$\gg$ 7	App Access Settings	
Lightning Experience Migration Assistant Switch to the modern, intelligent Salesforce.	Allow users to install canvas personal apps	
Get Started	View: All  Create New View	
Salesforce Mobile Quick Start	Action Master Label *	Application Version
E	Edit 📥 Ant Migration Tool	5.0
Force.com Home	Edit App1	1.0
Administer	Edit 📩 Dataloader Bulk	7.0
Administer	Edit 📥 Dataloader Partner	7.0
Manage Users	Edit 📥 Force.com IDE	5.0
Manage Apps	Edit <u>LCTest</u>	1.0
Connected Apps	Edit Logcollector	1.0
Connected Apps OAuth	Edit <u>NetworkLogCollector</u>	1.0
App Menu	Edit <u>RsaNW_test</u>	1.0
Manage Territories	Edit <u>RSA_LogCollector</u>	1.0

2. Click the **Edit** button for the connected app you created, as shown below:

Home Chatter +		
Quick Find / Search () Q Expand All   Collapse All	Connected Apps Manage access to apps that connect to this Salesforce organization.	
♣ →  Lightning Experience	App Access Settings	
MIgration Assistant Switch to the modern, intelligent Salesforce.	Allow users to install canvas personal apps	
Get Started	View: All V Create New View	
	Action Master Label *	Application Version
Force com Home	Edit Ant Migration Tool	5.0
	Edit App1	1.0
A dminister	Edit Andreader Bulk	7.0
Aummister	Edit 📥 Dataloader Partner	7.0
Manage Users	Edit 📥 Force.com IDE	5.0
Manage Apps	Edit LCTest	1.0
Connected Apps	Edit Logcollector	1.0
Connected Apps OAuth	Edit NetworkLogCollector	1.0
Usage	Edit RsaNW_test	1.0
App Menu	Edit RSA_Logcollector	1.0
Manage Territories	Edit Alesforce for Outlook	7.0
Company Profile	Edit 📥 Salesforce Mobile Dashboards	7.0
Security Controls	Edit A Salesforce Touch	80
Domain Management		10
Communication lemplates		3.0
Data Management		Show mo fower & records

3. In the OAuth policies section, from the IP Relaxation drop-down menu, select Relax IP restrictions.

Connected App LCTest			Help for this Page 🥹
Connected App Edit			
0.		Version 1 Description	
Basic Information			= Required Information
Start URL	i	Mobile Start URL	1
OAuth policies			
Permitted Users Enable Single Logout	All users may self-authorize	IP Relaxation Refresh Token Policy:	Relax IP restrictions

4. Save your changes.

# Create a custom read-only profile (Classic)

RSA NetWitness uses OAuth Username-password flow to authenticate between a Connected App and the Salesforce API. Creating a read-only custom profile restricts the users to have read-only access to Salesforce API logs.

1. In the Salesforce UI, go to Manage Users > Profiles, then click New Profile.

Home Chatter 🛨					
Quick Find / Search 🕜 Q Expand All   Collapse All	Profiles				
$ \Rightarrow \mathbf{f} $	All Profiles   Edit   Delete   Create New View  New Profile				
Migration Assistant	Action	Profile Name 1	User License	Custom	
Switch to the modern, intelligent	Edit   Clone	Analytics Cloud Integration User	Analytics Cloud Integration User		
Salesforce.	Edit   Clone	Analytics Cloud Security User	Analytics Cloud Integration User		
Get Started	Edit   Clone	Authenticated Website	Authenticated Website		
Octoballed	Edit   Clone	Authenticated Website	Authenticated Website		
	Edit   Clone	Chatter External User	Chatter External		
Salesforce Mobile Quick Start	Edit   Clone	Chatter Free User	Chatter Free		
Farme and Hama	Edit   Clone	Chatter Moderator User	Chatter Free		
Force.com Home	Edit   Del	. <u>cloneadmin</u>	Salesforce	1	
0 desinistar	Edit   Clone	Contract Manager	Salesforce		
Administer	Edit   Clone	Cross Org Data Proxy User	XOrg Proxy User		
Manage Users	Edit   Del	. Custom: Marketing Profile	Salesforce	1	
Adoption Manager	Edit   Del	. Custom: Sales Profile	Salesforce	1	
Mass Email Users	Edit   Del	. Custom: Support Profile	Salesforce	1	
Roles	Edit   Clone	Customer Community Login User	Customer Community Login		
Permission Sets	Edit   Clone	Customer Community Plus Lo	Customer Community Plus Login		
Profiles	Edit   Clone	Customer Community Plus User	Customer Community Plus		

2. Choose the **Custom-Profile Name** option for the **existing profile** field. This existing profile should have **Salesforce** in the **User License** field, as shown below.

# **Clone Profile**

Enter the name of the new profile.

You must select an existing profile	to clone from.
	•
Existing Profile	Custom: Sales Profile 🔹
Liser License	Salasfarsa
OSCI LIVENSE	
Profile Name	TestNWLC
	Save Cancel

For more details about User Licenses, see .

see the User Licenses article in the Salesforce online help.

- 3. Click Save.
- 4. After you save the profile, you are redirected to a new page where you can view the new custom profile. Click **Edit** to change settings to minimize user access to

Salesforce event logs.

Profile TestNWLC « Back to List: Profiles			
Users with this profile have the permissi	ons and page layouts listed below. Administrators can change a user's profile by editing that	user's personal i	nforma
If your organization uses Record Types,	use the Edit links in the Record Type Settings section below to make one or more record type	oes available to u	sers wi
Login IP Ranges (0)   Enabled. Profile Detail	Apex Class Access (0)   Enabled Visualforce Page Access (0)   Enabled External Data Source Access (0)   Enabled Custom Permissions (0) Edit Clone Delete View Users	Enabled Named Cr	edential
Name	TestNWLC		
User License	Salesforce	Custom Profile	$\checkmark$
Description			
Created By	Lakshmi prasanna, 1/23/2018 1:52 AM	Modified By	Lakshr

**Note:** Copy the custom profile name: you need to use this profile later, while creating a new user under the Salesforce admin account.

- 5. Assign permission sets and enable the connected app for this profile, as follows:
  - a. In the **Custom App Settings** section, select and enable the **Sales (standard\_Sales)** option as shown below.

Profile Edit		Save	Cancel		
Name	NWLogcolle	ector			
User License	Salesforce		Custom Profile	$\checkmark$	
Description					
Custom App Settings					
	Visible	Default		Visible	Default
App Launcher (standard_AppLauncher)		$\bigcirc$	Salesforce Chatter (standard_Chatter)		0
Community (standard_Community)		$\bigcirc$	Sample Console (standard_ServiceConsole)		$\bigcirc$
Content (standard_Content)		$\bigcirc$	Service (standard_Service)		0
Marketing (standardMarketing)		$\bigcirc$	Service Console (standard_LightningService)		$\bigcirc$
Sales (standard_LightningSales)		0	Site.com (standard_Sites)		0
Sales (standard_Sales)	*	۲	Work.com (standard_Work)		$\odot$
Sales Console (standard_LightningSalesConsole)		0			

b. In the **Connected App Access** section, select the connected app that you created in <u>Create a Salesforce connected app (Classic</u>). Optionally, select **Workbench** to use the UI for querying the data using the REST API.

Connected App Access		
Ant Migration Tool	RsaNW_test	
Dataloader Bulk	Salesforce for Outlook	
Dataloader Partner	Salesforce Mobile Dashboards	
Force.com IDE	Salesforce Touch	
Logcollector	Workbench	•
RSA_Logcollector		

c. In the Administrative Permissions section, select the API Enabled option as

shown below.

	strative Permissions	
Manage Knowledge Article Import/Export	Access Chatter For SharePoint	
Manage Letterheads	Access Community Management	
Manage Lightning Sync 📃 👔	Access Libraries	
Manage Login Access Policies	Add People to Direct Messages	
Manage Macros Users Can't Undo	w Inclusion of Code Snippets from UI	
Manage Mobile Configurations	API Enabled 🕢	
Manage Package Licenses	Assign Permission Sets	
Manage Password Policies	Author Apex 📄 👔	
Manage Profiles and Permission Sets	Bulk API Hard Delete	
Manage Promoted Search Terms	Can Approve Feed Post and Comment	
Manage Public Documents	Chatter Internal User 🗸	
Manage Public List Views 📄 👔	Configure Custom Recommendations	
Manage Public Templates 🛛 📋	Create and Customize Dashboards	
Manage Reporting Snapshots	Create and Customize List Views	
Manage Reports in Public Folders	Create and Customize Reports	
Manage Roles	Create and Own New Chatter Groups	
Manage Salesforce CRM Content	Create and Set Up Communities	
Manage Salesforce Knowledge	reate and Update Second-Generation	
Manage Session Permission Set Activations	Create Content Deliveries	
Manage Sharing	Create Dashboard Folders	
Manage Synonyms 📄 👔	Create Public Links	
Manage United Access		

d. In the **General User Permissions** section, select the **View Event Log File** option as shown below.

Edit Tasks		Show Custom Sidebar On All Pages	
Edit Topics		Transfer Cases	<b>i</b>
Email-Based Identity Verification Option		Transfer Leads	<b>i</b>
Enable Work.com Calibration		Two-Factor Authentication for API Logins	i
Export Reports	🗌 🚺	Two-Factor Authentication for User Interface Logins	
Import Leads	<b>i</b>	Upload AppExchange Packages	<b>i</b>
Import Personal Contacts	<b>i</b>	View Encrypted Data	
Import Solutions	<b>i</b>	View Event Log Files	
Insert System Field Values for Chatter Feeds		View My Team's Dashboards	
Knowledge One			

e. In the **Standard Object Permissions** section, make sure to uncheck all available options.

Standard Object Permissions													
The permissions defined here control acces create different groups of permissions for in	is at the objective object	ect level. Acc tributors, ma	cess to indi inagers, an	vidual reco d administ	rds within that rators. How d	object type is	controlled by the sharing model. Set access	s levels bas	ed on the fur	nctional rec	uirements t	for the profile.	For example
	Basic Acc	055			Data Admir	istration		Basic Acc				Data Admin	istration
	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All
Accounts							Goal Links						
Assets							Ideas						
Campaigns							Leads						
Cases							Macros						
Coaching							Metrics						
Contacts							Metric Data Links						
Contracts							Opportunities						
D&B Companies							Orders						
Documents							Performance Cycles						
Duplicate Record Sets							Price Books						
Feedback Questions							Push Topics						
Feedback Question Sets	-						Scorecards						
Feedback Requests	-						Scorecard Metrics						
Feedback Templates							Solutions						
Goals							Streaming Channels	-					-
								0	-			-	0

6. Click Save to save your changes to the profile.

Desktop Integration Clients	
Choose whether users with this profile Configurations permission and define a Offline	can use a client, update a client, see client update alerts, or be forced to update to the latest version. To set permissions for Salesfor lettings in Outlook configurations. On, updates w/o alerts •
Session Settings	
Session times out after	2 hours of inactivity   Session security level required at login  -None
Password Policies	
User passwords expire in	90 days 🔻
Enforce password history	3 passwords remembered
Minimum password length	8
Password complexity requirement	Must mix alpha and numeric characters
Password question requirement	Cannot contain password 🔻
Maximum invalid login attempts	10 🔻
Lockout effective period	15 minutes
Obscure secret answer for password resets	
Require a minimum 1 day password lifetime	
	Save

# Create a user under Salesforce Admin account (Classic)

- In the Salesforce UI, go to Home > Manage Users > Users, then click the New User tab.
- 2. Define the settings as described in the following table.

Setting	Value
Last Name	Enter user's last name
Alias	Enter an alias for the new user
Email	Enter a valid email address where the new user can be contacted
Username	This setting is automatically populated, based on the email address
Nickname	This setting is automatically populated, based on the email address
Role	Select <none specified=""> from the drop-down menu</none>
User License	Select Salesforce from the drop-down menu
Profile	From the drop-down menu, select the custom profile you created in <u>Create a custom read-only profile (Classic)</u>

New User						
User Edit		Sav	Save & New	Cancel		
General Information						
	First Name				Role	<none specified=""></none>
	Last Name	John			User License	Salesforce 🔻
	Alias	john			Profile	LogCollector
	Email	your@email.com			Active	×
	Username	your@email.com			Marketing User	
	Nickname	your	1		Offline User	
	litle		_		Knowledge User	
	Company			F	Force.com Flow User	
	Department				Service Cloud User	
	Division			Site.c	om Contributor User	
				Site	.com Publisher User	
					Work.com User	
					Data.com User Type	None 🔻 👔
				Data.com Me	onthly Addition Limit	Default Limit (300) 🔻 👔
				Accessibility	Mode (Classic Only)	
				High-Contra	ast Palette on Charts	
				Force.com	QUICK Access Menu	

3. In the Approver Settings section, make sure to select Generate new password and notify user immediately.

Approver Settings	
Delegated Approver	9
Manager	
Receive Approval Request Emails	Only if I am an approver
Generate new password and notify us	ar immediately
	Save Save & New Cancel

4. Click Save.

Salesforce sends a message to the email account entered for the user account, with the subject **Verify your account**.

- 5. From the email message, click the verify account hyperlink, then change the password.
- 6. Save the username and password, since you need them later when you are configuring the Salesforce event source in RSA NetWitness.

# Configure the Salesforce Event Source using Lightning Experience View

To configure Salesforce, you must complete these tasks:

- I. Create a Salesforce connected app (Lightning)
- II. Create a custom read-only profile (Lightning)

III. Create a user under Salesforce admin account (Lightning)

#### Create a Salesforce Connected App (Lightning)

- 1. Log into to your Salesforce account through Salesforce portal: login.salesforce.com
- 2. In Lightning Experience view, you can use the App Manager to create a connected app.
  - a. On the Setup page, type the keyword App in the Quick Find box.
  - b. Select App Manager.
  - c. Click New Connected App.

Setup 🔻 Home	Object Manag	ger 🗸									
Q. Quick Find		SETUP Lightning Experi	ence App M	anager	MG 17		( <i>_7116*</i> 5346)	Ne	ew Lightning App N	ew Connect	ed App
Setup Home				~((\$ .¥))//	$\approx$		e .W//~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	$\square$		8 .W//C	e Cr
Lightning Experience	22 item	s • Sorted by App Name • Filter	ed by TabSet Type •								*
ADMINISTRATION		APP NAME 🕇	V DEVELOPER	NAME	✓ DE	ESCRIPTION	LAST MODIF	IED 🗸	APP TYPE	v vi v	
> Users	1	Ant Migration Tool	Forcecom_N	ligration_Tool	Th	he Force.com Migration Tool is a Java/Ant-based command-line utility for movi	11/7/2017 5	:22 PM	Connected (Manage	i)	<b>v</b>
> Data	2	App Launcher	AppLaunche	r	Ap	pp Launcher tabs	11/7/20178	36 AM	Classic	~	¥
> Email	3	Community	Community		Sa	alesforce CRM Communities	11/7/20178	36 AM	Classic	~	Ŧ
DI ATEODM TOOLS	4	Content	Content		Sa	alesforce CRM Content	11/7/20178	:36 AM	Classic	~	¥
PLATFORM TOOLS	5	Dataloader Bulk	Dataloader_	Bulk	Th	he Data Loader is an easy to use graphical tool that helps you to get your data i	11/7/2017 5	21 PM	Connected (Manage	i)	¥
✓ Apps	6	Dataloader Partner	Dataloader_I	Partner	Th	he Data Loader is an easy to use graphical tool that helps you to get your data i	11/7/2017 5	:22 PM	Connected (Manage	i)	¥
App Manager	7	Force.com IDE	Forcecom_II	DE	Th	he Force.com IDE is a powerful client application for creating, modifying, testin	11/7/2017 5	22 PM	Connected (Manage	1)	Ŧ
AppExchange Marketplace	8	Marketing	Marketing		Be	est-in-class on-demand marketing automation	11/7/20178	36 AM	Classic	$\checkmark$	¥
Connected Apps	9	Platform	Platform		Th	he fundamental Force.com platform	11/7/20178	36 AM	Classic		¥

3. Make sure the following settings are defined in Salesforce to enable your new app:

Setting	Value
Connected App Name	Enter a name for the app, for example Logcollector.
API Name	This setting is populated automatically with the Connected App Name you enter.
Contact Email	Enter a valid email address.
Enable OAuth Settings	Make sure this is selected.
Callback URL	Enter the callback URL (endpoint) that Salesforce calls back to your application during OAuth. This is the OAuth redirect URI.
	Depending on which OAuth flow you use, the URL is typically the one

Setting	Value
	that a user's browser is redirected to after successful authentication. Because this URL is used for some OAuth flows to pass an access token, the URL must use secure HTTPS or a custom URI scheme.
Selected OAuth Scopes	Select Access and manage your data (api).

4. Click Save to complete your Connected App setup.

New Connected App				
				ave Cancel
Basic Information			-	
basic information				
	Connected App Name	Logcollector		
	API Name	Logcollector		
	Contact Email	vour@email.com	_	
	Contact Phone	Jourgeman.com		
	1			
	Logo Image URL9	Helend lane impact of Change and of	aus samala l	4548
	Icon URLo	Upload logo image or Undose one of	our sample	000
		Choose one of our sample logos		
	Info URL			
	Description			
<ul> <li>API (Enable OAuth Settings)</li> </ul>				
Enable OAuth Settings 🛞				
Enable for Device Flow				
Callback URL 0 http:	s://ics/de.com			
4		b z		
Use digital signatures		//)		
Selected OAuth Scopes				
làm.	Available cess and manage your Challer da	(Chatter ani)		Selected OAuth Scopes
Act	cess and manage your Eclair data	(eclair_api)	<u> </u>	
Act	cess and manage your Wave data	(wave_api)	Add	
Acti	cess custom permissions (custom) cess your basic information (id. or	_permissions) offeremail address phone)		
Alk	ow access to your unique identifier	r (openid)		
Ful	l access (full)		hemove	
Per	rform requests on your behalf at a	ny time (refresh_token, offline_access)		_
Pro	ovide access to your data via the V	Veb (web)	Ψ.	*
Require Secret for Web Server Flowo			_	
Include ID Token 📦 📋				
Enable Single Logouto				

- 5. After you save the connected app, you are redirected to a new page. Click **Continue**.
- 6. From this page, you can copy your Consumer Key. Select **Click to reveal** to see your Consumer Secret, and copy that as well.

**Note:** You need the Consumer Key and Consumer Secret values later, while configuring Client ID and Client Secret values in RSA NetWitness.

Connected App Name				
« Back to List: Custom Apps				
	Edit De	elete Manage		
Allow from 2-10 minutes for your changes to	take effect on the server before using the connect	ted app.		
, °	· · · ·			
	Version	1.0		
	API Name	Logcollector		
	Created Date	1/2/2018 5:21 AM		
		By:		
	Contact Email	your@email.com		
	Contact Phone	100010 5 01 111		
	Last Modified Date	1/2/2018 5:21 AM		
		By: state and state		
	Description			
	INTO UKL			
API (Enable OAuth Settings)				
Consumer Key			Consumer Secret	Click to reveal
Selected OAuth Scopes	Access and manage your data (api)		Callback URL	https://lcsfdc.com
	Full access (full) Allow access to your unique identifier (openid)			
Enable for Device Flow			Require Secret for Web Server Flow	<b>V</b>
Token Valid for	0 Hour(s)		Include Custom Attributes	
Include Custom Permissions				
Enable Single Logout	Single Logout disabled			

For more details about creating a Connected App, see the Create a Connected App article in the Salesforce online help.

After you create the connected app, you need to edit its policies, as described in the following procedure.

#### To edit the policies for a connected app:

- 1. Click on Manage Connected Apps under the Connected Apps tab.
- 2. Click the Edit button for the connected app you created, as shown below:

-	Q. Search Setup	
Setup 🔻 Home Obje	ect Manager 🗸	
ADMINISTRATION > Users	Manage Connected Apps	
> Data		
> Email	View: All  Create New View	
PLATFORM TOOLS	Action Master Label +	Application Version
∨ Apps	Edit 📥 Ant Migration Tool	5.0
App Manager	Edit App1	1.0
	Edit <u>A Dataloader Bulk</u>	7.0
AppExchange Marketplace		7.0
✓ Connected Apps		1.0
Connected Apps OAuth Us	Edit Logcollector	1.0
	Edit NetworkLogCollector	1.0
Manage Connected Apps	Edit <u>RsaNW_test</u>	1.0
Installed Packages	Edit RSA_Logcollector	1.0
N 14 1 1 1	Edit Alesforce for Outlook	7.0
> Mobile Apps	Edit Alesforce Mobile Dashboards	7.0

3. In the OAuth policies section, from the IP Relaxation drop-down menu, select Relax

#### **IP** restrictions.

Connected App LCTest				Help for this Page 🥹
Connected App Edit				
6		Version 1 Description		
Basic Information				= Required Information
Start URL	i	Mobile Start URL	1	
OAuth policies				
Permitted Users Enable Single Logout	All users may self-authorize	IP Relaxation Refresh Token Policy:	Relax IP restrictions Immediately expire refresh token	•

4. Save your changes.

#### Create a Custom Read-Only Profile (Lightning)

RSA NetWitness uses OAuth Username-password flow to authenticate between a Connected App and the Salesforce API. Creating a read-only custom profile restricts the users to have read-only access to Salesforce API logs.

1. In the Salesforce UI, go to Home > Users > Profiles, then click New Profile.

-		Q Search Se	tup	
Setup 🔻 Hom	ne Object Manager 🗸			
Q Quick Find	SETUP Prof	, , files	JRNS-91 (- 7776-5311) (- 7776-5311) (- 7776-5311) (- 7776-5311) (- 7776-5311) (- 7776-5311) (- 7776-5311) (- 7	
Setup Home	C We y			<u> </u>
Lightning Experience	Profiles			
ADMINISTRATION	All Profiles <b>•</b>	Edit   Delete   Create New View		
∨ Users	New Profile	2		
Adoption Manager	Action	Profile Name 🔹	User License	Custom
Permission Sets	Edit   Clone	Analytics Cloud Integration User	Analytics Cloud Integration User	
	Edit   Clone	Analytics Cloud Security User	Analytics Cloud Integration User	
Profiles	Edit   Clone	Authenticated Website	Authenticated Website	
Public Groups	Edit   Clone	Authenticated Website	Authenticated Website	
0.000	Edit   Clone	Chatter External User	Chatter External	
Queues	Edit   Clone	Chatter Free User	Chatter Free	

2. Choose the **Custom-Profile Name** option for the **existing profile** field. This existing profile should have **Salesforce** in the **User License** field, as shown below.

SETUP Profiles	
Clone Profile Enter the name of the new profile.	
You must select an existing profile t	to clone from.
Existing Profile User License Profile Name	Custom: Sales Profile  Salesforce NWLogcollector
	Save

For more details about User Licenses, see .

see the User Licenses article in the Salesforce online help.

- 3. Click Save.
- 4. After you save the profile, you are redirected to a new page where you can view the new custom profile. Click **Edit** to change settings to minimize user access to Salesforce event logs.

Profile NWLogcollect	tor							
Users with this profile I	have the permiss	ions and page layo	uts listed below. Adm	iinistrators ca	in change a user	's profile by editing that	user's personal ir	nformat
If your organization us	es Record Types	, use the Edit links i	in the Record Type S	ettings section	on below to make	e one or more record typ	es available to u	sers wi
Login IP Ra	nges [0]   Enablec	I Apex Class Access [0]	Enabled Visualforce	Page Access (C	]   <u>Enabled Exten</u> Enabled Custo	nal Data Source Access [0] om Permissions [0]	Enabled Named C	Credentia
Profile Detail	Name	NWLogcollector	Edit	Delete	View Users			
	User License	Salesforce					Custom Profile	$\checkmark$
	Description Created By	MERICAN)	, 12/28/2017 2:12 AM				Modified By	Laks

**Note:** Copy the custom profile name: you need to use this profile later, while creating a new user under the Salesforce admin account.

- 5. Assign permission sets and enable the connected app for this profile, as follows:
  - a. In the **Custom App Settings** section, select and enable the **Sales (standard\_Sales)** option as shown below.

Profile Edit		Save	Cancel		
Name User License Description	NWLogcolle Salesforce	ector	Custom Profile	✓	
Custom App Settings					
	Visible	Default		Visible	Default
App Launcher (standard_AppLauncher)		$\bigcirc$	Salesforce Chatter (standard_Chatter)		$\bigcirc$
Community (standard_Community)		$\bigcirc$	Sample Console (standardServiceConsole)		0
Content (standard_Content)		$\bigcirc$	Service (standard_Service)		0
Marketing (standardMarketing)		$\bigcirc$	Service Console (standard LightningService)		$\bigcirc$
Sales (standard_LightningSales)		0	Site.com (standard_Sites)		0
Sales (standard_Sales)	1	۲	Work.com (standard_Work)		0
Sales Console (standard Lightning SalesConsole)		0			

b. In the **Connected App Access** section, select the connected app that you created in <u>Create a Salesforce Connected App (Lightning)</u>. Optionally, select **Workbench** to use the UI for querying the data using the REST API.

Connected App Access		
Ant Migration Tool	RsaNW_test	
Dataloader Bulk	Salesforce for Outlook	
Dataloader Partner	Salesforce Mobile Dashboards	
Force.com IDE	Salesforce Touch	
Logcollector	Workbench	•
RSA_Logcollector		

c. In the Administrative Permissions section, select the API Enabled option as shown below.

Administrative Permissions			
Access Chatter For SharePoint		Manage Knowledge Article Import/Export	
Access Community Management		Manage Letterheads	1
Access Libraries		Manage Lightning Sync	
Add People to Direct Messages		Manage Login Access Policies	
Allow Inclusion of Code Snippets from UI		Manage Macros Users Can't Undo	
API Enabled		Manage Mobile Configurations	
Assign Permission Sets		Manage Package Licenses	
Author Apex	<b>i</b>	Manage Password Policies	
Bulk API Hard Delete		Manage Profiles and Permission Sets	
Can Approve Feed Post and Comment		Manage Promoted Search Terms	
Chatter Internal User	$\checkmark$	Manage Public Documents	1
Configure Custom Recommendations		Manage Public List Views	
Create and Customize Dashboards		Manage Public Templates	
Create and Customize List Views		Manage Reporting Snapshots	1
Create and Customize Reports	<b>i</b>	Manage Reports in Public Folders	
Create and Own New Chatter Groups		Manage Roles	
Create and Set Up Communities		Manage Salesforce CRM Content	
Create and Update Second-Generation		Manage Salesforce Knowledge	
Create Content Deliveries		Manage Session Permission Set Activations	
Create Dashboard Folders		Manage Sharing	
Create Public Links		Manage Synonyms	
0 D F-11	-	Manager Halland Courses	

d. In the **General User Permissions** section, select the **View Event Log File** option as shown below.

Edit Tasks		Show Custom Sidebar On All Pages	
Edit Topics		Transfer Cases	<b>i</b>
Email-Based Identity Verification Option		Transfer Leads	i
Enable Work.com Calibration		Two-Factor Authentication for API Logins	i
Export Reports	<b>i</b>	Two-Factor Authentication for User Interface Logins	
Import Leads	<b>i</b>	Upload AppExchange Packages	<b>i</b>
Import Personal Contacts	<b>i</b>	View Encrypted Data	
Import Solutions	<b>i</b>	View Event Log Files	
Insert System Field Values for Chatter Feeds		View My Team's Dashboards	
Knowledge One			

e. In the **Standard Object Permissions** section, make sure to uncheck all available options.

Standard Object Permissions													
he permissions defined here control accest reate different groups of permissions for in	as at the obje Idividual con	ect level. Acc tributors, ma	ess to indinagers, an	vidual recor d administr	rds within that ators. <u>How do</u>	object type is	controlled by the sharing model. Set acces	is levels base	ed on the fur	nctional req	uirements f	or the profile.	For example,
	Basic Acc	055			Data Admini	istration		Basic Acc	055			Data Admini	istration
	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All
Accounts							Goal Links						
Assets							Ideas						
Campaigns							Leads						
Cases							Macros						
Coaching							Metrics						
Contacts							Metric Data Links						
Contracts							Opportunities						
D&B Companies							Orders						
Documents							Performance Cycles						
Duplicate Record Sets							Price Books						

6. Click Save to save your changes to the profile.

Desktop Integration Clients	
Choose whether users with this profile Configurations permission and define Offline	can use a client, update a client, see client update alerts, or be forced to update to the latest version. To set permissions for Salesfor ettings in Outlook configurations. On, updates w/o alerts •
Session Settings	
Session times out after	2 hours of inactivity   Session security level required at login  -None-
Password Policies	
User passwords expire in	90 days 🔹
Enforce password history	3 passwords remembered
Minimum password length	8
Password complexity requirement	Must mix alpha and numeric characters
Password question requirement	Cannot contain password V
Maximum invalid login attempts	10 🔻
Lockout effective period	15 minutes
Obscure secret answer for password resets	0
Require a minimum 1 day password lifetime	
	Save

#### Create a User under Salesforce Admin Account (Lightning)

- 1. In the Salesforce UI, go to Home > Users > Users, then click the New User tab.
- 2. Define the settings as described in the following table.

Setting	Value
Last Name	Enter user's last name
Alias	Enter an alias for the new user
Email	Enter a valid email address where the new user can be contacted
Username	This setting is automatically populated, based on the email address
Nickname	This setting is automatically populated, based on the email address
Role	Select <b><none specified=""></none></b> from the drop-down menu
User License	Select Salesforce from the drop-down menu
Profile	From the drop-down menu, select the custom profile you created in <u>Create a Custom Read-Only Profile (Lightning)</u>
New User	
User Edit	Save 8 New Cancel

User Edit		Save	Save & New	Cancel				
General Information								1
	First Name					Role	<none specified=""></none>	¥ 1
	Last Name	John				User License	Salesforce	*
	Alias	john				Profile	LogCollector	•
	Email	your@email.com				Active	×	
	Username	your@email.com				Marketing User		
	Nickname	your	1			Offline User		
	litle					Knowledge User		
	Company				For	ce.com Flow User		
	Department				S	ervice Cloud User		
	Division				Site.com	Contributor User		
					Site.co	om Publisher User		
						Work.com User		
					Da	ta.com User Type	None V i	
					Data.com Mont	hly Addition Limit	Default Limit (300)	Y i
					Accessibility Mo	ode (Classic Only)	🔲 🚺	
					High-Contrast	Palette on Charts	🔲 🚺	
					Force.com Qu	uick Access Menu	•	

3. In the Approver Settings section, make sure to select Generate new password and notify user immediately.

Approver Settings			
Delegated Approver	9		
Manager	<u></u>		
Receive Approval Request Emails	Only if I am an approver		
Generate new password and notify user immediately			
	Save Save & New Cancel		

4. Click Save.

Salesforce sends a message to the email account entered for the user account, with the subject **Verify your account**.

- 5. From the email message, click the verify account hyperlink, then change the password.
- 6. Save the username and password, since you need them later when you are configuring the Salesforce event source in RSA NetWitness.

# Set Up Salesforce Event Source in RSA NetWitness

In RSA NetWitness Suite, perform the following tasks:

- 1. Deploy the CEF parser from Live
- 2. Configure the event source

# **Deploy the Salesforce Files from Live**

Salesforce requires resources available in Live in order to collect logs.

#### To deploy the Salesforce content from Live:

- 1. In the RSA NetWitness Platform menu, select Live.
- 2. Browse Live for the Common Event Format (cef) parser, using RSA Log Device as the Resource Type.
- 3. Select the cef parser from the list and click **Deploy** to start the Deployment Wizard. The wizard deploys the parser to the appropriate the Log Decoders.
- You also need to deploy the Salesforce package. Browse Live for Salesforce EventLogs content, typing "Salesforce" into the Keywords text box, then click Search.
- 5. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

**Note:** On a hybrid installation, you need to deploy the package on both the VLC and the LC.

6. Restart the **nwlogcollector** service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Resource Guide* on RSA Link.

# **Configure the Salesforce Event Source in NetWitness**

This section contains details on setting up the event source in RSA NetWitness Suite. In addition to the procedure, the Salesforce Collection Configuration Parameters are described.

#### To configure the Salesforce Event Source:

- 1. In the RSA NetWitness Platform menu, select Administration > Services.
- In the Services grid, select a Log Collector service, and from the Actions menu, choose View > Config.
- 3. In the Event Sources tab, select Plugins/Config from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

The Available Event Source Types dialog is displayed.

Available Event Source Types $ extsf{eq}  imes$			
	Name 🔨		
	azure_ad_audit	t	
	azure_ad_signi	n	
	azureaudit		
	cloudtrail		
	salesforce		
		Cancel	ОК

5. Select salesforce from the list, and click OK.

The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

Add Source		
Basic		•
Name *		
Enabled	M	
Instance URL *		
User Name *		
Password *	****	
Client ID *		
Client Secret *	****	
Production System		
Start From (In Days) *	0 \$	
Userld Refresh Time (In Hours) *	24	
Use Proxy		
Proxy Server		]
Proxy Port		
Proxy User		•
	Cancel	Ж

The Add Source dialog is displayed.

- Define parameter values, as described in <u>Salesforce Collection Configuration</u> Parameters.
- 8. Click Test Connection.

The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

**Note:** The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click OK.

The new event source is displayed in the Sources panel.

10. Repeat steps 4–9 to add another Salesforce plugin type.

# **Salesforce Collection Configuration Parameters**

The following tables describe the configuration parameter for the Salesforce integration with RSA NetWitness Platform. Fields marked with an asterisk (\*) are required.

The Add Source dialog is divided into Basic and Advanced sections.

# **Basic Parameters**

The following table describes the Basic parameters.

Parameter	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Instance URL	To view instance details in Company Information:
	<ul> <li>In Salesforce Lightning Experience UI (LEX): Setup &gt; Company Settings &gt; Company Information</li> </ul>
	<ul> <li>In Salesforce Classic UI (Aloha): Setup &gt; Company Profile &gt; Company Information</li> </ul>
	The URL should be https:// <i>{instance}.salesforce.com</i> , where <i>{instance}</i> is the name of your organization instance.
User Name *	Enter the user name you created, which has permissions to view the logs.
Password *	Enter the password that matches the User Name.
Client ID *	Enter your connected application Consumer key.
Client Secret *	Enter your connected application Consumer Secret.
Production System	By default, the environment type is set to <b>Production</b> . Clear this checkbox to use the sandbox instead.
	<ul> <li>For Production environment, Oauth uses https://login.salesforce.com/services/oauth2/token for the Token URL.</li> </ul>
	<ul> <li>For Sandbox environment, Oauth uses https://test.salesforce.com/services/oauth2/token for the Token URL.</li> </ul>
Start From (In Days) *	Enter the number of days, between 0 and 30. This represents the number of days in the past (using the current timestamp) from which to start collection. The default is <b>0</b> (current day).
Userld Refresh Time * (In Hours)	The time interval, in hours, to update the mapped <b>userid</b> (the username information stored in RSA NetWitness Suite from the User Salesforce API Object). By default, refresh time is set to 24 hours.
Use Proxy	Select to enable a proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.

Parameter	Description
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	A custom value chosen to represent the IP address for the Salesforce Event Source in the customer environment. The value of this parameter is captured by the <b>device.ip</b> meta key. This value can help you to query or group events collected by a particular instance of the plugin.
Test Connection	Checks the configuration parameters you set to verify they are correct.

# **Advanced Parameters**

 $\operatorname{Click}^{\bigodot}$  next to Advanced to view and edit the advanced parameters, if necessary.

Name	Description		
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is <b>180</b> . For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.		
	<b>Note:</b> The Salesforce event source generates events every 24 hours, and max polling interval can be set to 24 hours as well in RSA NetWitness. Therefore, RSA recommends setting the Polling Interval to 60 minutes, and then change as necessary, depending on the number of events, bandwidth and load of the system.		
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. RSA recommends that you do not set this value to zero (0), since logs are collected every 24 hours. The collection of logs depends on the polling time + polling interval time set. The following factors contribute to how you should set these values: 1. Load on the system		
	<ol> <li>Number of events generated by the event source</li> <li>Bandwidth for data transfer from the event source to Log Collector or Remote/Virtual Log Collector.</li> </ol>		
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).		

Name	Description
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	<b>Caution:</b> Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector.
	<ul> <li>Off = (default) disabled</li> <li>On = enabled</li> </ul>
	• Verbose = enabled in verbose mode - adds thread information and source context information to the messages.
	This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enable	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

# Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.