Splunk Integration User Guide

This document describes the integration of ITM On-Prem with Splunk software.

Note: Currently documentation is being rebranded from ObserveIT to ITM On-Prem. Anything referred to as ITM On-Prem means ObserveIT and anything referred to as ObserveIT is ITM On-Prem.

FEATURES

ITM On-Prem includes the following to collect and manage the data:

- **ObserveIT Technology Add-on** (ObserveIT TA): Connects Splunk to the ObserveIT RESTful API to continuously pull the latest user activity and alert events. ObserveIT TA pulls data from ObserveIT into Splunk as follows:
 - Subscribes to User Activity and/or Alert events
 - · Polls events from multiple ObserveIT instances
- ObserveIT App for Splunk: Leverages the data collected by ObserveIT TA to provide fullfeatured User Activity and Alert dashboards. Direct session-playback links for each session from Splunk to the ObserveIT console bring instant deep analysis of user behavior to Splunk and includes:
 - · Detailed summary of user sessions and alerts -drill down into individual user activities
 - · Charts to highlight risky users and applications
 - Direct link to Session Player from all user activities and alerts

PREREQUISITES

- Download and install ObserveIT TA and ObserveIT App for Splunk from Splunkbase
- ObserveIT TA communicates with your ObserveIT API directly, typically on port 443
- ObserveIT (Minimum version: 7.12)
- Splunk Enterprise: Platform Version: 9.1, 9.0, 8.2, 8.1, 8.0

Splunk Deployment Architecture

SINGLE-INSTANCE SPLUNK ENTERPRISE DEPLOYMENT

Splunk is a simple non-distributed deployment on the same network as ITM On-Prem. ObserveIT TA and ObserveIT App are installed on the same node.



DISTRIBUTED SPLUNK ENTERPRISE DEPLOYMENT

Splunk is a distributed deployment on the same network as ITM On-Prem.

ObserveIT TA is installed on a Splunk heavy forwarder that sends data. (Installation of ObserveIT TA on a Universal Forwarder or SHC is not supported.)

The ObserveIT App is installed on the search heads that handles the search management functions.



SPLUNK CLOUD DEPLOYMENT

Splunk Cloud can be used to store and search for ITM On-Prem data. To forward the data to Splunk Cloud, ObserveIT TA is installed on a Splunk heavy forwarder on the same network as ObserveIT. The ObserveIT App is installed on Splunk Cloud.



Splunk Configuration

You configure ObserveIT TA to reach the ObserveIT REST API and retrieve report data.

CREATING APPLICATION IN ITM ON-PREM

To integrate ITM On-Prem with Splunk using RESTful API, you register the application to authenticate access. Oauth2 is the method of authenticating access to the ObserveIT RESTful API.

This procedure describes how to generate a token that you use when you configure ObserveIT TA for Splunk.

1. From the ITM On-Prem (ObserveIT) Web Console, click the ? in the upper-right corner and select **Developer Portal** from the menu.

Note: If the Developer Portal is not installed by default, you will be prompted to install it.

2. From the Developer Portal, select Credentials and then click the Create App button.

observe IT			
Library Report API	+ Create App		
Report Analytics API	Application name	Application Id	
Auth API	Agent Updater	0000000-0000-0000-000000001000	4/前
Control API	Notification Service	9DBD4842-F7F6-4AC3-A6BC-07D1CD0EE8F6	4 / î
Activity API	Screenshot Storage Optimizer	4DBDE487-6670-48BB-ACBE-0E61E2429965	4/前
Credentials	Health Monitoring Service	55FC641C-29C0-4726-A989-5CFC65AED86B	4/前
Documentation	splunk	E008D4FF-E91D-4219-8F15-D0C55BF69E7C	4/m
Getting Started	Web Console	8D950498-5B5C-4F1E-AB72-E14F0C7C923E	4 / D
Code Examples	Agent Installation	CD5917C5-1808-4ADE-854D-F4A69D102B69	4 / 🗊
Legal			

The Create Application dialog box displays. This is where you register the application.

Create Application	×
Application Name	
Splunk	
Allowed Scopes separate by space for multiple scopes, example its report:*	
*	
Allowed Grants	
Password	
Authorization Code	
Refresh Token	
Implicit	
Redirect URIS used for authorization_code and token(implicit) flows	
Redirect URI	
Redirect URI	
Redirect URI	
Cancel	ave

- 3. Do the following:
 - 1. In the **Application Name** field, enter a name. It is recommended that you choose a name you can recognize, such as **Splunk**, **Splunk1** etc.
 - 2. In Allowed Grants, check Client Credentials.
 - 3. Click **Save** and the application is added to the list.

observeit

Library Report API	+ Create App		
Report Analytics API	Application name	Application Id	
Auth API	Agent Updater	0000000-0000-0000-0000-00000001000	チョー 前
Control API	Notification Service	9DBD4842-F7F6-4AC3-A6BC-07D1CD0EE8F6	4 / 🗊
Activity API	Screenshot Storage Optimizer	4DBDE487-6670-48BB-ACBE-0E61E2429965	4/前
Credentials	Health Monitoring Service	55FC641C-29C0-4726-A989-5CFC65AED86B	チノ前
Documentation	splunk	E008D4FF-E91D-4219-8F15-D0C55BF69E7C	4/面
Getting Started	Web Console		4 1 11
Resource Query Language	web console	0/350438-565C-4FTE-A672-ET4FUC7C325E	7 × W
Code Examples	Agent Installation	CD5917C5-1808-4ADE-854D-F4A69D102B69	4 / 亩
Legal			

4. Click the application you just created. The dialog box for generating a token displays.

splunk ×
Grant Type
client_credentials -
Client Id
E008D4FF-E91D-4219-8F15-D0C55BF69E7C
Client Secret
GMgB6wugb4evaCd1Ne2hFICdqw6HpChgTXq538w5p4
Scope
*
Close Generate Token

Note: Note the Client Id and Client Secret values. You will enter them into the configuration screen of the Splunk add-on.

Creating New Index for ObserveIT (example "oit" index)

1. Create a new index from the **Indexes** screen.

splunk >enterpris	e Apps 🕶							🛕 Adminis	rator 🔹 🕕 Messages 👻 Settings 💌	Activity • Help •	Q Find
Indexes A repository for data	in Splunk Enterprise. Indexes r	eside in flat files	on the Splunk Enterpr	se instance known as t	he indexer. Learn mo	ore ඵ					New Inde
3 Indexes	filter	٩									20 per page
Name *	Actions	Type ©	App 0	Current Size ¢	Max Size \$?	Event Count ¢	Earliest Event ¢	Latest Event 0	Home Path 0	Frozen Path \$	Status ¢
_audit	Edit Delete Disable	E Events	system	46 MB	488.28 GB	500K	a month ago	a few seconds ago	\$SPLUNK_DB\audit\db	N/A	✓ Enabled
_configtracker	Edit Delete Disable	E Events	system	4 MB	488.28 GB	485	a month ago	10 hours ago	\$SPLUNK_DB_configtracker\db	N/A	✓ Enabled
_internal	Edit Delete Disable	Events	system	832 MB	488.28 GB	14.2M	a month ago	a few seconds ago	\$SPLUNK_DB_internaldb\db	N/A	✓ Enabled
_introspection	Edit Delete Disable	E Events	system	1.63 GB	488.28 GB	1.44M	14 days ago	a few seconds ago	\$SPLUNK_DB_introspection\db	N/A	✓ Enabled
_metrics	Edit Delete Disable	@Metrics	system	285 MB	488.28 GB	7.75M	14 days ago	a few seconds ago	\$SPLUNK_DB_metrics\db	N/A	✓ Enabled
_metrics_rollup	Edit Delete Disable	@Metrics	system	1 MB	488.28 GB	0			<pre>\$SPLUNK_DB_metrics_rollup\db</pre>	N/A	✓ Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	54	18 days ago	10 hours ago	\$SPLUNK_DB_telemetry\db	N/A	✓ Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB\fishbucket\db	N/A	✓ Enabled
history	Edit Delete Disable	E Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB\historydb\db	N/A	✓ Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB\defaultdb\db	N/A	✓ Enabled
olt	Edit Delete Disable	Events	TA-ObserveIT	1 MB	500 GB	418	13 days ago	5 minutes ago	\$SPLUNK_DB\olt\db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	E Events	system	0 B	488.28 GB	0			\$SPLUNK_DB\splunklogger\db	N/A	Disabled
summary	Edit Delete Disable	E Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB\summarydb\db	N/A	✓ Enabled

- 2. Click New Index and the New Index dialog box opens.
- 3. Provide an Index Name. In the example, the new index is "oit".

General Settings		
Index Name	st 🔸	
	Set index name (e.g., INDEX_NAME). Search using inc	fex-INDEX_NAME.
Index Data Type	Events	Ø Metrics
	The type of data to store (event based or metrics).	
Home Path	optional	
	Hot/warm db path. Leave blank for default (\$SPLUNK,	_DB/INDEX_NAME(db).
Cold Path	optional	
	Cold db path. Leave blank for default (\$SPLUNK_DB/	NDEX_NAME/colddb).
Thawed Path	optional	
	Thewediresurrected db path. Leave blank for default	(\$SPLUNK_DB/INDEX_NAME/thaweddb).
Data Integrity Check	Enable	Disable
	Enable this if you want Splunk to compute hashes on	every slice of your data for the purpose of data integr
Max Size of Entire Index	500	G8 -
	Maximum target size of entire index.	
Max Size of	auto	68 *
Hot/Warm/Cold Bucket	Maximum target size of buckets. Enter jauto. high yea	ume' for high-volume indexes.
	Continued	
Frozen Path	Prozen bucket archive path. Set this if you want Splur	is to automatically archive frozen buckets.
1.00		
App	005	ervell •
Storage Optimization		
Tsidx Retention Policy	Enable Reduction	Disable Reduction
	Warning: Do not enable reduction without understand reduced buckets. Learn More LE	ing the full implications. It is extremely difficult to rebu

In the example below, you can see the button to create the "New Index:, example "oit"

CONFIGURING OBSERVEIT TA FOR SPLUNK

This procedure describes the registration process in Splunk.

Your ObserveIT instance(s) need to be registered as the Splunk Technology Add-on (TA). The access token (with the Client ID and Client Secret you generated in the ObserveIT Developer Portal will be used to authenticate with the API.

Note: If you would like to store ObserveIT events in their own index, create it on the indexer before following these configuration steps.

1. Open the ObserveIT TA app in Splunk and click Create New Input.

splunk>enterprise Apps +					A	Administrator *	Messages •	Settings •	Activity *	Help •	Find
Inputs Configuration Search										0	TA-ObserveIT
Inputs Manage your data inputs										c	reate New Input
1 Input 10 Per Page •			filter		Q						
i Name -	interval e	Index a		Status e			Acti	ions			
> olt	10	ot		Enabled			1	0 1			

2. Complete the Add ObserveIT API dialog box.

date ObserveIT API	
Nome	
	Enter a unique name for the data input
Interval	10
	Time interval of input in seconds.
Index	fo
Reports API URL	https://sales-demo.itmdemo.iocal/v2/apis/reportz
	API URL optionally including port, E.p.
	https://observeit.mycompany.com.4431v2/apis/report/realm-observeit/reports
Client ID	E008D4FF-E91D-4219-8F15-D0C558F69E7C
	Create app in API Console, e.g.
	https://observeit.mycompany.com/v2/apps/portal/home.html?
	Acreds
Client Secret	
Historical Data To Pull	7 days • X
	WARNING: Updating this value on an active input will result
	in data duplication.
Events Pagination	10000
	Amount of events to index per input invocation
Reports To Collect	UI Activities × Command Activities ×
	Alerts \times . File Activity \times . Email Activity \times
CA Certificate chain	ceritmdemo-sales-demo-ca.cer
	たいめんちん アス メンルがストンカル がいうんだい メント・コンドウト ストム 単さたし ひかい しかたおさ
	Cancel

- 1. Enter a unique **Name** that represents the ObserveIT instance, for example use the hostname such as Splunk.
- 2. In the **Interval** and **Events Pagination** fields, enter values you want. Make sure that their combination is sufficient to ingest your anticipated event rate.
- 3. The Reports API URL is formatted as:

```
https://<hostname>:<port>
/v2/apis/report;realm=observeit/reports
```

- 4. In the **Client ID** and **Client Secret**, enter the values you copied when the application was created in ObserveIT. (See: Creating Application in O.)
- 5. To include existing events on your system, in the **Historical Data To Pull** field, select the time period you want to go back to. Select **None**, if you want only new events to be loaded.
- 6. Select Reports to Collect.
- The input requires CA certificate (mandatory). You must provide the path to CA certificate chain file, relative to \$SPLUNK_HOME. Default CA certificates will be used if

no file name provided. For example, the certificate file name is: **cer\itmdemo-sales-demo-ca.cer**.

- 3. Choose the reports you want to load in Splunk:
- UI Activities: User interface activity events from Windows or Mac agents
- Command Activities: Commands run on UNIX agents
- Alerts: Alert events from all agents

Note: This is a less secure option and should not be used in production.

Splunk Usage

VIEWING EVENTS

You view events logged as soon as ITM On-Prem data collection is configured and enabled in the ObserveIT TA. You can start using the data in Splunk searches and reports.

Li	st 🗸 🖌 Format	t 50 Per Page ~ < Prev 1	2
i	Time	Event	
>	6/6/18 5:43:18.446 PM	<pre>{ [-] accessedSiteName: accessedUr1: null appLicationName: Windows Shell Experience Host collectorUr1: https://code1.preview.observeit.net// commandParams: createdAt: 2018-06-06T17:43:18.446Z domainName: code1.observeit.net endpointId: E035BBC2-1D72-48A0-ABBC-AA4DE0BC5AF1 endpointId: E035BBC2-1D72-48A0-ABBC-AA4DE0BC5AF1 endpointId: E035BBC2-1D72-48A0-ABBC-AA4DE0BC5AF1 endpointId: E035BBC2-1D72-48A0-ABBC-AA4DE0BC5AF1 endpointMame: LC2AMAZ-18L6TVS id: 7330EB6D-ABBB-4F25-9408-2BD807FB7B13 loginName: Administrator observedAt: 2018-06-06T17:43:18.163Z os: Windows playbackUr1: https://code1.preview.observeit.net/0bserveIT//SlideViewer.aspx?SessionID=1A8B52A9-EDAC- A8BB-4F25-9408-2BD807FB7B13 processExecutable: shellexperiencehost remoteAddress: 127.0.0.1 remoteHostName: Michaels-MacBoo risingValue: 2018-06-06T17:43:18.446Z secondaryLoginName: n/a sessionId: 1A8B52A9-EDAC-448E-9871-79DB21D53C28 sessionId: 1A8B52A9-EDAC-448E-9871-79DB21D53C28 sessionId: https://code1.preview.observeit.net//v2/apis/activity/sessions/1A8B52A9-EDAC-448E-9871-1 timezoneOffset: 0 windowTitle: Start } </pre>	-4
>	6/6/18	{ [-]	

DASHBOARDS

The ObserveIT App provides a comprehensive dashboard to view summary information about risky users and applications as well as drilldowns and links to view recorded user sessions.

Note: Installation of ObserveIT TA is a prerequisite for using the ObserveIT App.

Alerts Dashboard

The **Alerts** dashboard shows the top alerts and top risky users and applications. All alerts are listed, with a link to launch the ITM On-Prem (ObserveIT) player so you can playback the user's session. The session column lets you drill-down to the individual activities that comprise the alerted session.

unk'> App:	o: ObservelT ∽							Adm	ninistrator 🗸	2 Messa	ges ∽ Settings ∽	Activity ∽ Help ∽	Find	
s User Ses	ssions Search											<u></u> 0b	<u>serv</u>	<u>/0</u>
erts													Edit Export	•
			_											
ar to date	*	Submit	Hide Filters											
sky users					Top Risk Desktop Ap	plications/W	/ebsites			Top F	isk Alerts			
		1					3					3		
	us	sers				app	lications					alert types		
					Windows Explorer, 5.2	63%				rming larg	e irregular hours, 5.263%			
					Windows PowerShell 36 9	428				ng Commi	n Administrator 36.842%			
					mindows rowershell, 50.0	- 16.70		SSMS, 57.89	95%	ing continu			Running databas	zed work
			Administrator, 1009	196										
							^							
rts - Year t	to date - 19 alert(s) found	I											
t Name		Login			Secondary User		Endpoi	nt		OS Type				
t Name	S .	Login All	c	3 v	Secondary User	⊙ .	All	nt	© .	OS Type All	Q	Submit	C+ Reset	
Name	⊗ .	All	C	3 .	Secondary User All Search produced no results	Ø v	All	nt	© ,	OS Type All	G	Submit	C Reset	
Name	C T	All	€ Alert Name ⊕	3 ·	Secondary User All Search produced no results	⊘ ▼	All	I ogin Name G	Secondary	OS Type	© Endaciat ≙	Submit	C Reset	Vide
Name	time 0	Login All	Alert Name \diamond Running Command Lit	3 T	Secondary User All Search produced no results rograms as Administrator	♥ *	All	Login Name \diamond Administrator	Secondary	OS Type All	C Endpoint 0 EC2AMAZ-18L6TVS	Submit Client O Spike-964.local	C Reset	Vide
: Name ⊥t 1 <u>Ω</u> 20 2 <u>Ω</u> 20	time 0 2018-05-31 17:56:41.90 2018-05-24 23:26:25.02	Login All 77	Alert Name \circ Running Command Lit Running database ma	3 • ine Shell pr anagement	Secondary User All Search produced no results rograms as Administrator t tools on an unauthorized of	S vorkstation	Endpoir All	Login Name Administrator Administrator	Secondary	OS Type All	Endpoint ¢ EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS	Client Client Submit	Reset	Vide
: Name ⊥t 1 ♀ 20 2 ♀ 20 3 ♀ 20	time 0 2018-05-31 17:56:41.90 2018-05-24 23:26:25.02 2018-05-24 23:27:22.95	Login All 77 33 33	Alert Name © Running Command Lin Running database ma Running database ma	3 T	Secondary User All Search produced no results rograms as Administrator t tools on an unauthorized of tools on an unauthorized of t	vorkstation vorkstation	Endpoir All	Login Name Administrator Administrator Administrator	Secondary	OS Type All	Endpoint 0 EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS	Client Spike-964.local Michaels-MacBoo Michaels-MacBoo	Reset	
Name 1 Q 20 2 Q 20 3 Q 20 4 Q 20	time 0 2018-05-31 17:56:41.90 2018-05-24 23:26:25.02 2018-05-24 23:27:22.95 2018-05-24 23:26:21.36	Login All 77 33 33 60	Alert Name ° Running Command Lir Running database ma Running database ma Running database ma	3 T	Secondary User All Search produced no results rograms as Administrator t tools on an unauthorized v t tools on an unauthorized v t tools on an unauthorized v	vorkstation vorkstation vorkstation	Endpoin All	nt Login Name © Administrator Administrator Administrator	Secondary	OS Type All	Endpoint © EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS	Client Spike-964.local Michaels-MacBoo Michaels-MacBoo	C Reset	
Name 1 0, 1t 2 0, 20 3 0, 20 4 0, 20 5 0, 20	time 0 2018-05-31 17:56:41.90 2018-05-24 23:26:25.02 2018-05-24 23:27:22.95 2018-05-24 23:27:22.95 2018-05-05 11:38:29.53	Login All 77 33 33 30 00	Alert Name © Running Command Lin Running database ma Running database ma Running database ma	ine Shell pa anagement anagement anagement	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized v tools on an unauthorized v tools on an unauthorized v	vorkstation vorkstation vorkstation vorkstation	Endpoin All	nt Login Name O Administrator Administrator Administrator Administrator Administrator	Secondary	OS Type All	Endpoint © EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS	Client Client Spike-964.local Michaels-MacBoo Michaels-MacBoo Spike-964.local	C Reset	
Name 1 Q 20 2 Q 20 3 Q 20 4 Q 20 5 Q 20 6 Q 20 6 Q 20 7 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	time 0 2018-05-31 17:56:41.90 2018-05-24 23:26:25 02 2018-05-24 23:27:22.95 2018-05-24 23:26:21.36 2018-06-05 11:38:29.53	Login All 77 33 33 30 00 7	Alert Name © Running Command Lin Running database ma Running database ma Running database ma	3	Secondary User All Search produced no results regrams as Administrator tools on an unauthorized tools on an unauthorized tools on an unauthorized tools on an unauthorized	vorkstation vorkstation vorkstation vorkstation	Endpoin All	nt Login Name O Administrator Administrator Administrator Administrator Administrator	Secondary	OS Type All	Endpoint © EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS EC2AMAZ-18L6TVS	Client Client Spike-964.local Michaels-MacBoo Michaels-MacBoo Michaels-MacBoo Spike-964.local Spike-964.local	C Reset	
Name 1 Q 20 2 Q 20 3 Q 20 4 Q 20 5 Q 20	time 0 1018-05-24 23-26-25 02 1018-05-24 23-26-25 02 1018-05-24 23-26-21 36 1018-06-05 11 38-29 53 1018-06-05 11 38-29 53 1019-06-05 11 58-29 58 1019-06-05 11 58-29 58 1019-06-05 11 58-29 58 1019-06-05	Login All All 33 33 30 00 00 7	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma	The set of the se	Secondary User All Search produced no results regrams as Administrator tools on an unauthorized v tools on an unauthorized v tools on an unauthorized v tools on an unauthorized v	vorkstation vorkstation vorkstation	Endpoin	t Login Name Administrator Administrator Administrator Administrator	Secondary	OS Type All User 0	Endpoint © EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS	Client Client Submit	C Reset	
Name 1 0 2t 2 0 2t 3 0 2t 4 0 2t 5 0 2t	time 0 2018-06-31 17:56-41.90 2018-06-34 23:26:25.02 2018-06-24 23:26:21.36 2018-06-24 23:26:21.36 2018-06-51 17:40:44 21 2018-06-51 17:40:44 21 0 date - 19 alert(s	Login All 77 33 39 00 00 7 5) found	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma	ine Shell pr anagement anagement anagement	Secondary User All Search produced no results regrams as Administrator tools on an unauthorized v tool	vorkstation vorkstation vorkstation	Endpoi	t Login Name Administrator Administrator Administrator Administrator Administrator	Secondary	OS Type All	Endpoint © ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS	Client Client Submit	C Reset	
t Name 1 Q 2t 2 Q 2t 3 Q 2t 4 Q 2t 5 Q 2t	Lime 0 1018-05-21 17:56-41:90 1018-05-24 23:26:25 02 1018-05-24 23:27:22 95 1018-05-24 23:27:22 95 1018-06-25 11:32:29:53 1018-06-05 11:32:29:53 1018-06-05 11:32:29:53 1018-06-05 11:32:29:53 1018-06-05 11:32:29 0 date - 19 alert(s	Login All All 33 36 00 7 5) found Login	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma Running database ma	ine Shell pr anagement anagement	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized v secondary User	vorkstation vorkstation vorkstation vorkstation	Endpoir	nt Login Name © Administrator Administrator Administrator Administrator Administrator	Secondary	OS Type All User 0	Endpoint © ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS ECZAMAZ-18L6TVS	Client Client Client Client Michaels-MacBoo Michaels-MacBoo Michaels-MacBoo Spike-964.local	Reset	Vide
Image: Name 1	time 0 2018-05-31 17:56-41.90 2018-05-24 32:36:25 02 2018-06-24 32:36:21 04 2018-06-05 11:38:29 53 2018-06-05 11:38:29 53 2019-06-05 2019-06-05 2019-06-06-05 2019-06	Login All 77 13 13 13 16 10 7 7 8 9 10 10 7 7 9 10 10 10 7 7 10 10 10 10 10 10 10 10 10 10 10 10 10	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma Running database ma	ine Shell pa anagement anagement anagement anagement anagement	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized v Secondary User All	vorkstation vorkstation vorkstation vorkstation	Endpoin All Endpoin All	nt Login Name O Administrator Administrator Administrator Administrator	Secondary	OS Type All User 0 OS Type All	Endpoint © EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS	Client Client Submit	C Reset	Vide C C C C C C C
I	time 0 2018-05-31 17:56-41.90 2018-05-24 32:26:25 02 2018-06-24 32:26:25 02 2018-06-24 32:26:21 02 2018-06-25 11:32:26:21 02 2018-06-25 12:32:26:21 02 2019-06-25 12:32:25 2019-06-25 2019-06-25 2019-06	Login All 3 3 60 60 7 5) found Login All	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma Running database ma	3 • ine Shell pu anagement anagement anagement anagement anagement	Secondary User All Search produced no results rograms as Administrator Itools on an unauthorized vit tools on an unauthorized vite comments are a declinicated or search produced no results Secondary User All Search produced no results Search produced no results	vorkstation vorkstation vorkstation	Endpoir All Endpoir All	nt Login Name O Administrator Administrator Administrator Administrator	Secondary	OS Type All User 0 OS Type All	Endpoint © EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS	Client Client Submit Client Spike-964.local Michaels-MacBoo Michaels-MacBoo Spike-964.local Spike-964.local Spike-964.local Spike-964.local	Creset	Vide
1	C + 19 alert(s	Login All 33 360 00 7 36) found Login All	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma Running database ma Running database ma	3 × ine Shell paragement anagement anagement anagement 3 ×	Secondary User All Search produced no results rograms as Administrator Itools on an unauthorized vit tools on an unauthorized vit tools on an unauthorized vit tools on an unauthorized vitools on an unauthori vitools on an una	vorkstation vorkstation vorkstation	Endpoir All Endpoir All	nt Login Name O Administrator Administrator Administrator Administrator	Secondary	OS Type All User 0 OS Type All	Control Contro	Client C spike-964.local Michaels-MacBoo Michaels-MacBoo spike-964.local spike-964.local spike-964.local spike-964.local spike-964.local spike-964.local	C Reset	Vide
1	time 0	Login All All 33 30 00 7 7 8) found Login All	Alert Name © Running Gommand Lin Running database ma Running database ma	3 ine Shell paragement anagement anagement anagement 3 3 •	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized vi tools on an una	vorkstation vorkstation vorkstation	Endpoir All Endpoir All	nt Login Name O Administrator Administrator Administrator Administrator Administrator	Secondary	OS Type All User 0 OS Type All User 0	Control Contro	Client © spike-964.local Michaels-MacBoo Michaels-MacBoo spike-964.local michaels-MacBoo spike-964.local spike-964.local spike-964.local spike-964.local	C Reset	Vide
1 ↓ ↓ 1 ↓ 2 2 ↓ 2 3 ↓ 2 5 ↓ 2 6 ↓ 2 7 8 8 8 8 8 8 8 8 8 8 8 8 8	time 0 tore 43262502 tore 4120 tore 43262502 tore 43262502 tore 43262136 tore 43262136 tore 419 alert(s tore 419 alert(s tore 419 tore	Login All 17 13 13 13 13 10 10 10 10 10 10 10 10 10 10 10 10 10	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma Running database ma Running Command Lin Alert Name © Running Command Lin	The shell present of the	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized v Secondary User All Ograms as Administrator	vorkstation vorkstation vorkstation	Endpoint All Endpoint All	nt Login Name O Administrator Administrator Administrator Administrator Administrator Administrator t Login Name O Administrator	Secondary	OS Type All User 0 OS Type All VUser 0	Endpoint © EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS COMMA2-18L6TVS EC2AMA2-18L6TVS	Client Spike-964.local	C Reset	Vide
1 Aarme 1 A 22 2 A 22 3 A 22 4 A 2 22 5 A 22 5 A 22 5 A 22 6 A 22 7 The second secon	time 0	Login All 33 36 30 50 50 50 50 50 50 50 50 50 50 50 50 50	Alert Name © Running Gormand Lin Running database ma Running database ma Running database ma Running database ma Running database ma Running Gormand Lin Alert Name © Running Command Lin Windows	The Shell provide the She	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized v tools on an unauthorized v tools on an unauthorized v search produced no results Secondary User All Search produced no results ograms as Administrator r to work of the search produced no results	vorkstation vorkstation vorkstation	Endpoin All Endpoin All	nt Login Name © Administrator Administrator Administrator Administrator Administrator Cogin Name © Administrator	Secondary Secondary Secondary	OS Type All User 0 OS Type All	Endpoint © EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L5TVS	Client Cl	C Reset	Vide
1 Aarme		Login All All 3 3 3 0 0 0 0 2 3 5) found All 7 7	Alert Name © Running Command Lin Running database ma Running database ma Running database ma Running database ma Running database ma Running Command Lin Kunning Command Lin Windows Select Adm	 > >	Secondary User All Search produced no results rograms as Administrator tools on an unauthorized v tools on an unauthorized v tools on an unauthorized v Secondary User All Search produced no results ograms as Administrator v Intervention ograms as Administrator r. Windows PowerShell	vorkstation vorkstation vorkstation	Endpoir All Endpoir	nt Login Name © Administrator Administrator Administrator Administrator Administrator	Secondary Secondary Secondary	OS Type All User 0 OS Type All v User 0	Endpoint © EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS EC2AMA2-18L6TVS	Client Cl	C Reset	Vide

Note: If you want to view only the alert list, use horizontal collapse bar to hide the pie views.

User Session Dashboard

The User Session dashboard shows the most active users and endpoints as well as the most used applications.

A summary view of each user session is available, including the start and end time of the session, the number of unique activities, and the user involved.

A link to the ITM On-Prem (ObserveIT player to replay the session is also included.

A drilldown shows more details about the individual activities that comprise the session.

When the user session dashboard is opened via alert drill-down, you see only that individual single session's activities.

Alerts	User Sessions Search									obser\	10 it
Use	r Sessions									Edit Export	•
		_									
Year	to date ~	Submit Hide Filters									
Mos	t Active Applications					Most Activ	ve Users and Endpo	pints			
	De	esktop Apps Unix/	Linux Comma	ands			Login A	ccounts	Secondary Users	Endpoints	
		10 Applicaton	S						Login Accounts		
	OTHI Windows Explo SSM IIS Manag Google Chron	ER, 0.124% orer, 0.09% MS, 0.152% Her, 0.476% ne, 3.429%		un Chall Functioner Un	A DE 7392					minianana 100%	
			windo	ws Shell Experience Hos	t, 95.728%				Ad	ministrator, 100%	
Use	r Sessions - Year to date -	24 Sessions found		Endpoint		0° Turo		Client			
All	Ø .	All	() v	All	(C) v	All	Ø v	All	Ø .	Submit Reset	
		Search produced no results									
i	Start Time 0	End Time 0		Login Name 0	Secondary	User 0	Endpoint Name 0		OS 0	Unique Activities 🗘	Video 0
~	1 2018-06-05 19:52:33	2018-06-05 20:10:2	1	Administrator			EC2AMAZ-18L6TVS		I Windows	5	
	Application Name		Activity								
	Google Chrome		ObservelT - Co ObservelT - Do ObservelT - Lo	nfiguration - LDAP Setti main Name Alias - Goog gin Page - Google Chron	ngs - Google Chrom Ile Chrome (2) ne (1)	ie (2)					
>	2 2018-06-04 22:26:09	2018-06-04 22:28:39	9	Administrator			EC2AMAZ-18L6TVS		III Windows	5	
2amaz-1	Ricture-ARRA/ObservelT/Slide/Jewe	r serv2SeesionID=0062EEE7	EE16-4407-BB	AF 262225000052			EC2AMAZ-18L6TVS		III Windows	1	

Splunk Troubleshooting and Support

TROUBLESHOOTING

Events not flowing: If you have configured ObserveIT TA and do not see events flowing into the system, check the internal logs for any error messages.

In the Splunk console, search ta_observeit_observeit_api.log for non-INFO messages:

index=_internal sourcetype="ta:observeit:log" NOT "INFO"

Error: "No previous instances" in TA log

If in the TA log in SPLUNK_HOME\var\log\splunk\ta_observeit_observeit_api.log

A message displays, for example:

2024-01-02 07:01:01,625 INFO pid=612 tid=MainThread file=base_modinput.py:log_ info:295 | No previous instances of input 'oit' were found.

This message indicates that you must create the **oit** index as described in "Creating New Index for ObserveIT (example "oit" index)" on page 6.

SUPPORT

For help using the ITM On-Prem (ObserveIT) platform, contact Proofpoint support organization.

https://proofpointcommunities.force.com/community/s/