



# HOWTO – Integrate Amazon VPC Flows

## Contents

Change Control .....	2
AWS VPC Flow Overview .....	2
Create a User attached to the ReadOnlyAccess policy .....	2
Create a Log group .....	3
Create log streams for the VPC you want to obtain flows from .....	4
Select the interfaces that you want to generate flows .....	5
View the log streams you created .....	5
Create credential(s) in FortiSIEM for AWS CloudWatch .....	6
Extra Goodies! .....	7
The Reports .....	8
The Dashboard .....	9



## Change Control

Date (DD-MMM-YYYY)	Change Summary
01-MAR-2019	First Release by Dusan Tomic.

Document Owner: International FortiSIEM CSE Team

## AWS VPC Flow Overview

FortiSIEM can process amazon flow logs, the process is somewhat complicated and will be explained below.

We need a role that can access flows, a user attached to that role, a log group and to set the several interfaces we want to retrieve flows from to actually publish them to CloudWatch (publishing to S3 is another option we won't go over in this HOWTO).

Amazon frequently changes their services so an up to date user guide to flows can be found at <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

## Create a User attached to the ReadOnlyAccess policy

1. In your AWS Console, go to IAM > Users > Add User
2. Define your user name and select Programmatic access as the Access Type

### Add user



#### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[+ Add another user](#)

#### Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

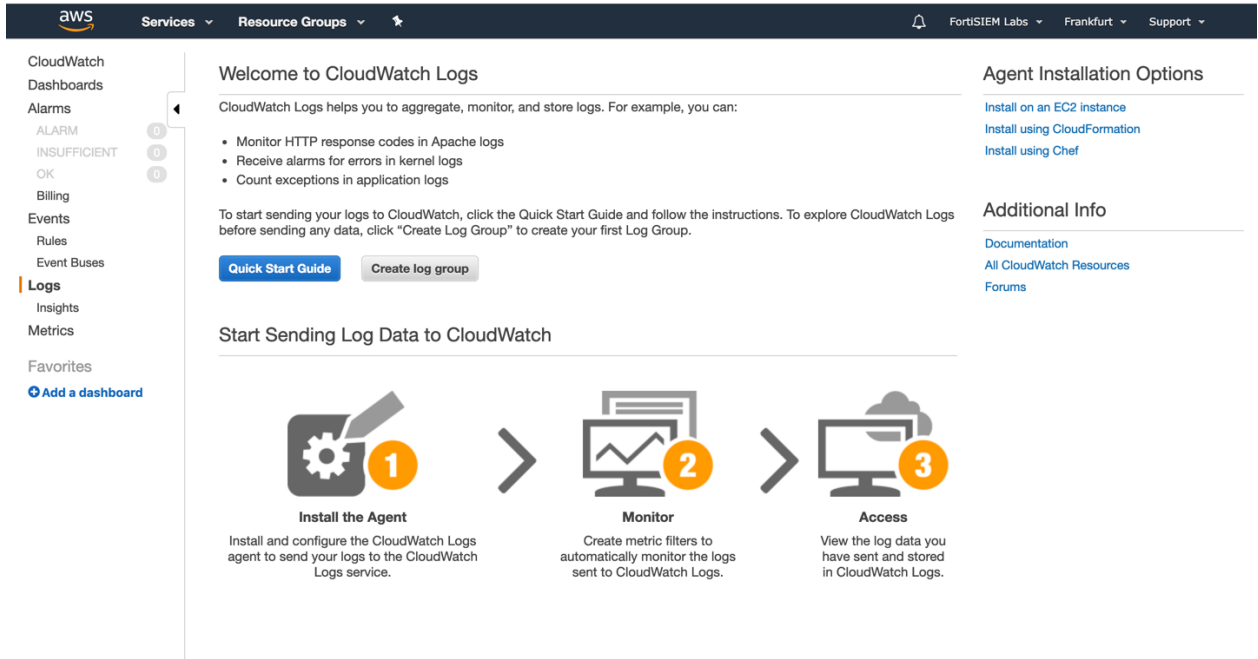
- Access type\*
- Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
  - AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

3. Click on Next: Permissions
4. Add user to the ReadOnlyAccess policy.
5. Save your Access key ID and the Secret access key, you will need this to populate credentials in FortiSIEM.

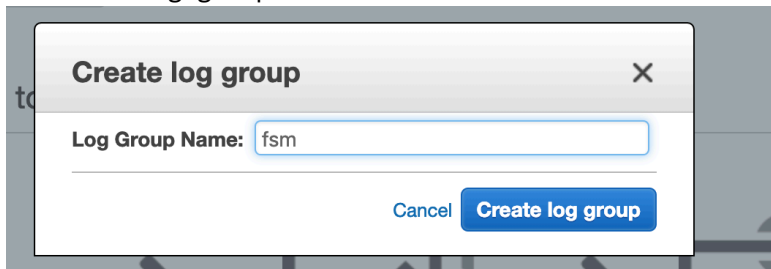


## Create a Log group

1. Go to Services > CloudWatch > Lets get Started (if its there) > Logs and Click **Create log group**



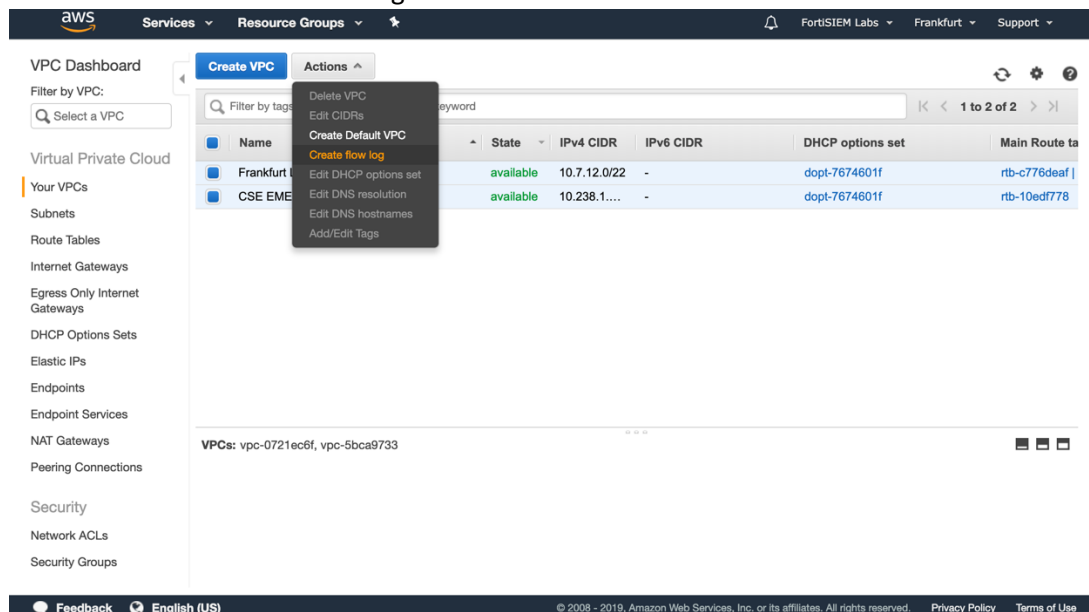
2. Create a log group called fsm





## Create log streams for the VPC you want to obtain flows from

1. Go to Services > VPC > Your VPCs
2. Select the VPC or VPCs you want to enable flows for
3. Click on Actions > Create flow log



4. In the Filter, select Accept, Reject or All (depending what you want from your flows)
5. Set Destination to Send to CloudWatch logs
6. Set the Destination log group to the log group you created in the previous step
7. Set the IAM role to a role that has permissions to access flows.

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html#flow-logs-iam>

VPCs > Create flow log

### Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple subscriptions to send traffic to different destinations. [Learn more](#)

Resources vpc-0721ec6f,vpc-5bca9733

Filter\* All

Destination  Send to CloudWatch Logs  Send to an S3 bucket

Destination log group\* fsm

IAM role\* flowlogsRole

The IAM role must have permission to publish to the CloudWatch Logs log group. [Set Up Permissions](#)

IAM role ARN arn:aws:iam::690013591054:role/flowlogsRole

\* Required

Cancel Create

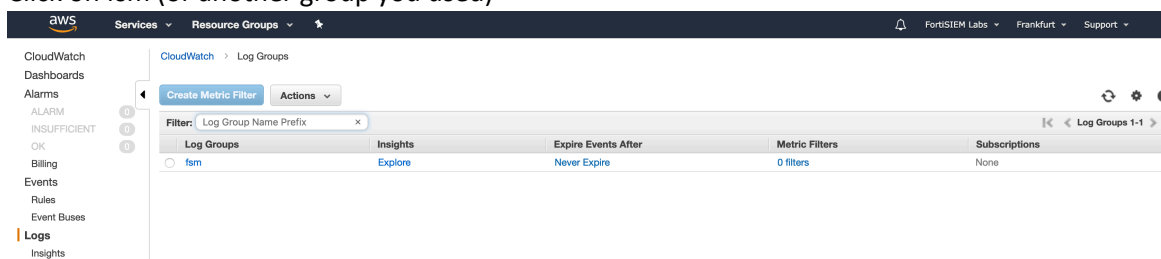


## Select the interfaces that you want to generate flows

1. Go to Services > EC2 > Network Interfaces
2. Select each interface you want to generate flows and click Actions > Create flow log
3. Repeat Steps 4-7 above

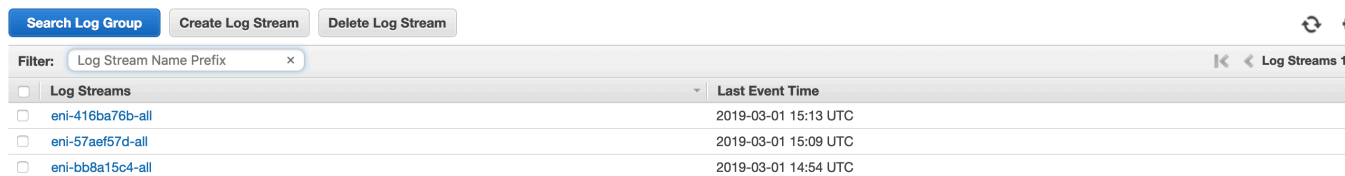
## View the log streams you created

1. Go to Services > CloudWatch > Logs
2. Click on fsm (or another group you used)



3. You will see all the streams (interfaces) that are generating flows

CloudWatch > Log Groups > Streams for fsm



4. Write the names of these Log Streams somewhere, you will need them when creating the CloudWatch credential. Each interface generates a separate stream, so we will need as many credentials as there are log streams



## Create credential(s) in FortiSIEM for AWS CloudWatch

You will need your User/IAM Access Key ID, user/IAM Secret Key, region, log group name, log stream name(s)

### 1. Populate the credential in FortiSIEM:

Access Method Definition
✕

Name:

Device Type:

Access Protocol:

Region:

AWS Account:

Log Group Name:

Log Stream Name:

Password config:

Access Key ID:

Secret Key:

Confirm Secret Key:

Description:

### 2. Associate the credential to amazon.com

**Step 2: Enter IP Range to Credential Associations**

Name / IP / IP Range	Credential Name
amazon.com	AWS CloudWatch, AWS CT, AWS EC2



- Test the Credential. This will create a job that will start pulling flows, we don't Discover any devices when we add CloudWatch or CloudTrail credentials.

Test Connectivity Results ✕

Columns 1/1

IP	Access	Status	Name	Type	Description
205.251.242.103	aws cloudwatch(AWS CloudWatch)	succeeded	amazon.com	Amazon AWS CloudWatch	

Test Complete.

Close

## Extra Goodies!

In version 5.1.2 (latest as of this writing), we don't have any Reports out of the box that leverage VPC flows. Below you can find two new reports that will allow you to create a dashboard such as the one below to visualize the traffic from your VPC.

The screenshot shows the FortiSIEM dashboard with the following components:

- Navigation Bar:** DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, ADMIN.
- Context:** Amazon Web Services Dashbo... | Summary | Performance | Login | CloudTrail | CloudWatch x
- Report 1: Amazon VPC Flow - Top Accepted Source, Dest, Port**

Reporting IP,Source IP,Destination IP,Destination TC	COUNT(Matches)	Trend
10.7.12.121,109.14.142.11,10.7.12.121,443	339	[Line Chart]
10.7.12.121,154.233.177.6,10.7.12.121,443	162	[Line Chart]
10.7.12.121,186.11.107.16,10.7.12.121,443	28	[Line Chart]
10.7.12.121,10.7.12.121,52.94.205.59,443	26	[Line Chart]
10.7.12.121,10.7.12.121,52.94.204.192,443	21	[Line Chart]
10.7.12.121,10.7.12.121,54.239.55.74,443	18	[Line Chart]
10.7.12.121,10.7.12.121,54.239.55.102,443	17	[Line Chart]
10.7.12.121,10.7.12.121,54.239.55.68,443	16	[Line Chart]
- Report 2: Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes**

Reporting IP	Event Name	Destination	Destination	Source Act	Source IP	SUM(Received Bytes)	SUM(Sent Bytes6)
10.7.12.1...	AWS flow log accept	85.245.6...	59737	ACCEPT	10.7.12.1...	5,07 MB	
10.7.12.1...	AWS flow log accept	154.233...	62666	ACCEPT	10.7.12.1...	2 MB	
10.7.12.1...	AWS flow log accept	10.7.12.1...	443	ACCEPT	109.14.1...	1.86 MB	
10.7.12.1...	AWS flow log accept	186.11.1...	28016	ACCEPT	10.7.12.1...	1.33 MB	
10.7.12.1...	AWS flow log accept	85.245.6...	61762	ACCEPT	10.7.12.1...	1.29 MB	
10.7.12.1...	AWS flow log accept	85.245.6...	50732	ACCEPT	10.7.12.1...	1001.04 KB	
10.7.12.1...	AWS flow log accept	85.245.6...	55721	ACCEPT	10.7.12.1...	942.52 KB	
10.7.12.1...	AWS flow log accept	10.7.12.1...	443	ACCEPT	154.233...	717.12 KB	
- Report 3: Amazon VPC Flow - Top Accepted Source, Dest, Port**

COUNT(Matched Events):	154.233.177.6:486	186.11.107.16:443
109.14.142.11:1017	443:162	443:339
10.7.12.121:678	443:162	443:339
443:339	443:162	443:339
- Map:** A map of Europe with red location pins over the United Kingdom, France, Germany, and Italy.



## The Reports

You can save each of the XML structures below into an .xml file and import them in Resources > Reports > Import in your FortiSIEM HTML5 GUI.

### Amazon VPC Flow – Top Accepted Source, Dest, Port

```
<?xml version="1.0" encoding="UTF-8"?><Reports><Report baseline="" rsync=""><Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name><Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description><CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope><SelectClause>
<AttrList>reptDevIpAddr,srclpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause><PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srclpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause><userRoles>
<roles custId="1">1681500</roles>
</userRoles><SyncOrgs/><ReportInterval>
<Low>1551454378</Low>
<High>1551454977</High>
</ReportInterval></Report></Reports>
```

### Amazon VPC Flows – Src, Dst, Port, Action, Received Bytes, Sent Bytes

```
<?xml version="1.0" encoding="UTF-8"?><Reports><Report baseline="" rsync=""><Name>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes</Name><Description>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes - 01:13:33 PM Feb 27 2019</Description><CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope><SelectClause>
<AttrList>reptDevIpAddr,eventType,eventName,destIpAddr,destIpPort,srcAction,srclpAddr,SUM(recvBytes64),SUM(sentBytes64)</AttrList>
</SelectClause><PatternClause>
<SubPattern id="194817050" name="">
<SingleEvtConstr>(eventType CONTAIN "AWS_VPC_FLOW") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,eventType,destIpAddr,destIpPort,srcAction,srclpAddr</GroupByAttr>
</SubPattern>
</PatternClause><userRoles>
<roles custId="1">1681500</roles>
</userRoles><SyncOrgs/><ReportInterval>
<Low>1551454665</Low>
<High>1551455264</High>
</ReportInterval></Report></Reports>
```





## The Dashboard

Once you have imported the reports, you copy/paste the following XML structure to a dashboard.xml file and import it into a Dashboard:

```
<?xml version="1.0" encoding="UTF-8"
standalone="no"?><DashboardConfigs><group><name>CloudWatch</name><description/><type>Widget</type><d
ashboard><columns>2</columns></dashboard><Widgets><widget pos="0">
<name>Amazon VPC Flow - Top Accepted Source, Dest, Port</name>
<description/>
<horizontalCell>0</horizontalCell>
<verticalCell>0</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings/>
<dataParam>twIndex:4;dtIndex:0;barType:overlaid;numResults:10;timeInterval:0;bizSvcId:0;</dataParam>
<dataProviderType>Report</dataProviderType>
<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551274433305">
<Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name>
<Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,srclpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srclpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget><widget pos="1">
<name>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes</name>
<description/>
<horizontalCell>2</horizontalCell>
<verticalCell>2</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings>1,SUM(Received Bytes64):1:0|0|0.33|0.67|1:0,SUM(Sent
Bytes64):1:0|26890|368955.67|711021.33|1053087:0,0</displaySettings>
<dataParam>twIndex:4;dtIndex:4;numResults:50;timeInterval:300000;bizSvcId:0;</dataParam>
<dataProviderType>Report</dataProviderType>
```



```

<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551273213669">
<Name>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes</Name>
<Description>Amazon VPC Flows - Src, Dst, Port, Action, Received Bytes, Sent Bytes - 01:13:33 PM Feb 27
2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,eventType,eventName,destIpAddr,destIpPort,srcAction,srcIpAddr,SUM(recvBytes64),SUM(
sentBytes64)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817050" name="">
<SingleEvtConstr>(eventType CONTAIN "AWS_VPC_FLOW") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,eventType,destIpAddr,destIpPort,srcAction,srcIpAddr</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget><widget pos="2">
<name>Amazon VPC Flow - Top Accepted Source, Dest, Port</name>
<description/>
<horizontalCell>4</horizontalCell>
<verticalCell>6</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings/>
<dataParam>twIndex:4;dtIndex:7;numResults:10;timeInterval:300000;bizSvcId:0;chartSet:2,3,4,0</dataParam>
<dataProviderType>Report</dataProviderType>
<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551274433305">
<Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name>
<Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>

```



```

<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget><widget pos="3">
<name>Amazon VPC Flow - Top Accepted Source, Dest, Port</name>
<description/>
<horizontalCell>4</horizontalCell>
<verticalCell>6</verticalCell>
<posX>0</posX>
<posY>0</posY>
<displaySettings/>
<dataParam>twIndex:4;dtIndex:9;numResults:50;timeInterval:300000;bizSvcId:0;</dataParam>
<dataProviderType>Report</dataProviderType>
<dataProviderNaturalId/>
<Report naturalId="PH_SYS_Report_1551274433305">
<Name>Amazon VPC Flow - Top Accepted Source, Dest, Port</Name>
<Description>Amazon VPC Flow - Top Accepted Source, Dest, Port - 01:33:53 PM Feb 27 2019</Description>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<SelectClause>
<AttrList>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort,COUNT(*)</AttrList>
</SelectClause>
<PatternClause>
<SubPattern id="194817051" name="">
<SingleEvtConstr>(eventType = "AWS_VPC_FLOW_ACCEPT") AND (phCustId IN (1))</SingleEvtConstr>
<GroupByAttr>reptDevIpAddr,srcIpAddr,destIpAddr,destIpPort</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="1">1681500</roles>
</userRoles>
<SyncOrgs/>
<ReportInterval>
<Low>1551454781</Low>
<High>1551455380</High>
</ReportInterval>
</Report></widget></Widgets></group></DashboardConfigs>

```