E-Center Anomaly Detection Service (ADS)

06/14/2011

Prasad Calyam, Maxim Grigoriev, Jialu Pu, Mukundan Sridharan

Version 1.2

Changed on (from version)	Description	Author
5/27/11	original version	Mukundan Sridharan, Jialu Pu, Prasad Calyam
6/09/11 (v1.0)	updated supported operations, new response format. Only bwctl and owamp left as supported data types. Request parameters list was reduced to the supported ones.	Maxim Grigoriev
6/14/11 (v1.1)	updated response with src_hub,dst_hub and metaid	Maxim Grigoriev

Introduction

The E-center consists of collection of the loosely coupled applications. The Anomaly Detection Service is designed for detecting anomalies in the data collected through the perfSONAR-PS service and it is designed to work with the DRS E-center service, which retrieves and caches the measurement data.

The ADS implements a number of detectors for anomalies. The list of detectors currently implemented are:

1. Adaptive Plateau Detector: Adapts the sensitivity of the plateau detector
2. Static Plateau Detector: Plateau detector with static sensitivity

The ADS serviec is implemented as REST webservice with GET and POST HTTP operations supported. The list of supported response formats include JSON, XML, YAML but JSON is preferred. The only supported format for the data string request is JSON.

ADS Request

ecenter_server_hostname := <hostname of the E-Center data service>;
ipv4 := <ipv4 address, dotted>;
datetime := < YYYY-MM-DD%20hh:mm:ss >;
data_type :='/', ['bwctl'|'owamp'];
response_format := ['.json'];
detector_type=['apd'|'spd'];
data_request := <JSON encoded response from the DRS which can be supplied as data string>;

detection_request := ‘ GET http://’, ecenter_server_hostname , ‘/ads/’,
detector_type, response_format, ‘?’,'data_type=', data_type,
('&data=',data_request,)?
, (‘&sensitivity=’,integer)?,(‘&elevation1=’,float]?, (‘&elevation2=’,float)?, (‘&swc=’,integer)?,
[‘src_ip=’, ipv4|’src_hub=’,string],’&’, [
‘dst_ip=’, ipv4|’dst_hub=’,string], (‘&start=’, datetime)?, (‘&end=’,
datetime)?,(‘&resolution=’,integer)?,(‘&timeout=’,integer)?;

Detector specific parameters for APD and SPD:
detector_type has option of 'spd' or 'apd' to determine the algorithm to us
elevation1/elevation2 is in the scale of percentage.
swc stands for summary window count.
All the parameters for analysis (i.e. **sensitivity, elevation1, elevation2, swc**) are **optional**.
The **data** parameter is optional but it will be used over the supplied DRS parameters. If you want to get data from the DRS then do not use this parameter but supply **start,end,src_hub(ip)/dst_hub(ip)** instead. The ADS will analyse **owamp** or **bwctl** data for each ***source/destination*** pair of IPS separately and return results accordingly, see below.

Example of ADS request:

GET http://ecenter.fnal.gov:9055/ads/spd.json?sensitivity=2&elevation1=20&data_type=owamp&
src_ip=131.243.24.11&dst_ip=198.32.44.130&start=2010-06-05 06:01:02&end=2010-06-05 07:02:01

ADS Response

The query response will return the anomalous data only.
Responser is formatted as:
number := float|integer;
parameters:= { ['metaid:'|'src_hub:'|'dst_hub']+,':',string }+, { ['plateau_size', 'swc', 'sensitivity',
'elevation1','elevation2'],':', number,','}+;

src_ip := ipv4;
dst_ip := ipv4;
status_data := ['critical'|'warning'],': {', { timestamp,': {','anomaly_type: ', ['plateau'|'other'], ', value: ',
number,'}' }+
status := 'OK'|status_data;
response := { src_ip,': { dst_ip,': {', parameters, 'status:', status, '} }' }*;

Below is an example of the ADS response:


```
{
    192.12.15.23: {
        134.79.104.209: {
            src_hub: "BNL",
            dst_hub: "SLAC",
            metaid: "1234",
            sensitivity: 2,
            status: "OK",
            elevation1: 0.2,
            elevation2: 0.4,
            plateau_size: "7",
```

```
                swc: 20,
            }
        },
        134.79.104.209: {
            192.12.15.23: {
                src_hub:  "SLAC",
                dst_hub: "BNL",
                metaid: "123434",
            sensitivity: 2,
            status: {
                critical: {
                    1304479767: {
                        anomaly_type: "plateau",
                        value: 730181000,
                    }
                },
                warning: {
                    1304472510: {
                        anomaly_type: "plateau",
                        value: 301539000,
                    }
                }
                },
                elevation1: 0.2,
                elevation2: 0.4,
                plateau_size: "7",
                swc: 20,
            }
        }
}
```