



Protect 2014

Washington, D.C. September 8-11

Introduction to HP ArcSight ESM Web Services APIs

Shivdev Kalambi

Software Development Manager (Correlation Team)

#HPProtect

Agenda

Overview

- Some applications of APIs

ESM Web Services APIs

- Login Service
- Query Viewer Service
- Report Service

Examples

- REST
- SOAP

Q&A



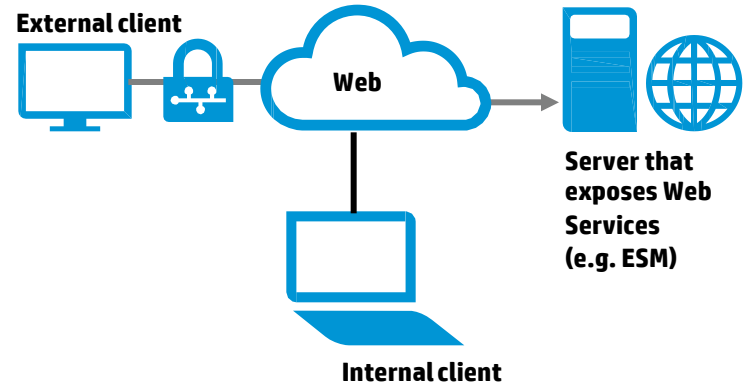
Overview



Web Services APIs

What are web services?

Web services are typically application programming interfaces (API) or web APIs that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services.



ESM Web Services APIs in practice

The idea is simple

Fetch your data out of ESM and apply it to your business use case

- **Risk Insight App:** Periodically fetch Asset Data from ESM and calculate scores
- **Custom Analytics:** Fetch event data and plot geo coordinates as a bubbles on a map
- **Command Line Utility:** Fetch event data from ESM and send it to standard output



Got data?

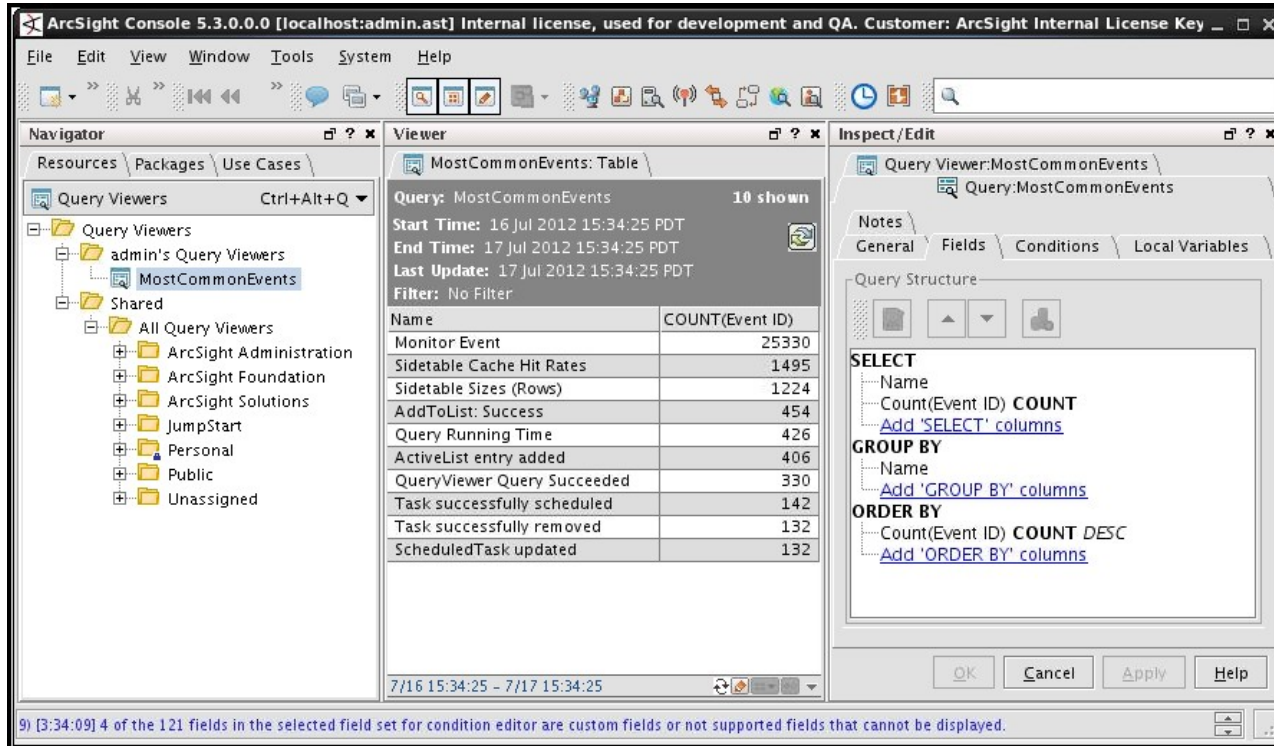
Prerequisites

- ESM Expertise: Intermediate – Advanced
 - Create the right content that needs to be retrieved
- Knowhow of Web Services in general
 - Ability to write code for simple SOAP/REST clients



Use cases

Top 10 most common events



The screenshot shows the ArcSight Console interface with the following components:

- Navigator:** Shows a tree view of resources, including 'Query Viewers' and 'MostCommonEvents'.
- Viewer:** Displays the 'MostCommonEvents' query results. The query is 'MostCommonEvents' with 10 results shown. The start time is 16 Jul 2012 15:34:25 PDT and the end time is 17 Jul 2012 15:34:25 PDT. The filter is 'No Filter'.
- Table:** A table showing the top 10 most common events.

Name	COUNT(Event ID)
Monitor Event	25330
Sidetable Cache Hit Rates	1495
Sidetable Sizes (Rows)	1224
AddToList: Success	454
Query Running Time	426
ActiveList entry added	406
QueryViewer Query Succeeded	330
Task successfully scheduled	142
Task successfully removed	132
ScheduledTask updated	132

The 'Inspect/Edit' pane shows the query structure:

```
SELECT
  Name
  Count(Event ID) COUNT
  Add 'SELECT' columns
GROUP BY
  Name
  Add 'GROUP BY' columns
ORDER BY
  Count(Event ID) COUNT DESC
  Add 'ORDER BY' columns
```

Fetch query viewer data

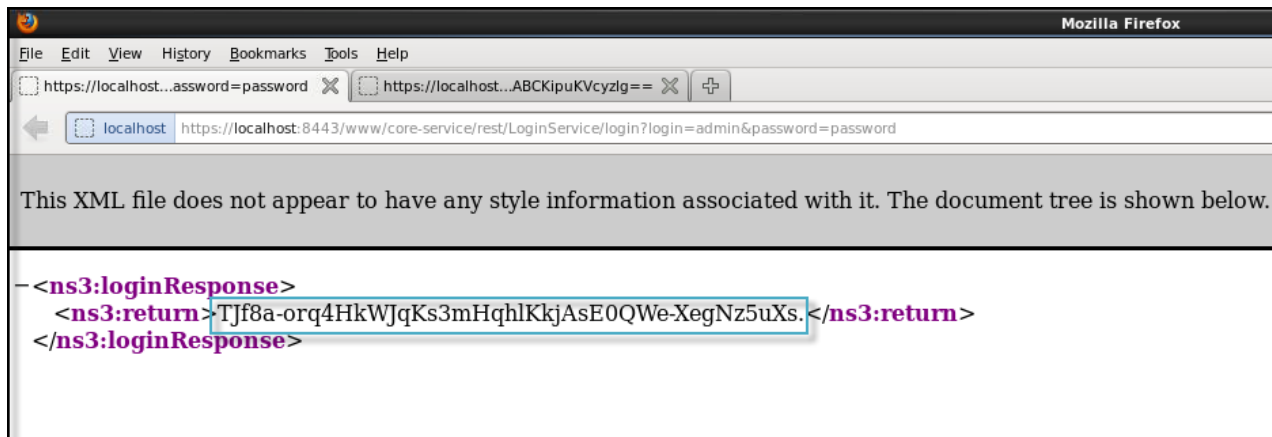
- Sample Query Viewer
- Fetch data
 - Using REST
 - Using SOAP



Use case 1

REST call to Login Service from a browser

<https://localhost:8443/www/core-service/rest/LoginService/login?login=admin&password=password>



Test the REST

- From the browser
- Invoke LoginService
 - Copy the *authToken*
- Invoke QueryViewerService
 - Pass the QueryViewer *ID*

https://localhost:8443/www/manager-service/rest/QueryViewerService/getMatrixData?authToken=__&id=__



Use case 1

REST call to Query Viewer Service from a browser

https://localhost:8443/www/manager-service/rest/QueryViewerService/getMatrixData?authToken=__&id=__

QueryViewerService using REST

```
<ns20:getMatrixDataResponse>
  <ns20:return>
    <endTimeStamp>1343252101953</endTimeStamp>
    <startTimeStamp>1343165701953</startTimeStamp>
    <timestamp>1343252221302</timestamp>
    <colHeaderTS>1343252221303</colHeaderTS>
    <columnHeaders>Name</columnHeaders>
    <columnHeaders>COUNT(Event ID)</columnHeaders>
    <maxColumns>2</maxColumns>
    <properties/>
    <rows xsi:type="listWrapper">
      <value xsi:type="xs:string">Monitor Event</value>
      <value xsi:type="xs:string">122325</value>
    </rows>
    <rows xsi:type="listWrapper">
      <value xsi:type="xs:string">Sidetable Sizes (Rows)</value>
      <value xsi:type="xs:string">7232</value>
    </rows>
    <rows xsi:type="listWrapper">
      <value xsi:type="xs:string">ASM Database Responsiveness - Last Hour</value>
      <value xsi:type="xs:string">292</value>
    </rows>
  </ns20:return>
</ns20:getMatrixDataResponse>
```

```
arc sight@svsvm0045 WebServices UC]$
arc sight@svsvm0045 WebServices UC]$ ~/java/jdk1.6.0_26/bin/java -classpath ./build
/classes/./build/lib/manager-ws-client-1.2.0.release.107.jar:./build/lib/core-ws-c
lient-1.5.0.release.51.jar:./build/lib/coma-infrastructure-1.4.0.release.240.jar co
n.protect.esm.QueryViewerExample

Name          COUNT(Event ID)
Monitor Event 122325
Sidetable Sizes (Rows) 7232
Sidetable Cache Hit Rates 7225
Task successfully scheduled 723
Task successfully removed 723
ScheduledTask updated 717
ActiveList entry expired 569
Event Throughput 551
ASM Database Responsiveness - Last Hour 382
Database Insert Time - Last Hour 292
arc sight@svsvm0045 WebServices UC]$
```

QueryViewerService using SOAP



Use case 2

SOAP example using the SDK : Login Service

// Set the Base URL

```
System.setProperty("com.arcsight.coma.client.ws.baseURL", "https://" + host + "/www/"); //  
localhost:8443
```

// Get the LoginService and login

```
LoginServiceClientFactory factory = new LoginServiceClientFactory();  
LoginService service = factory.createClient();  
String authToken = service.login(null, "admin", "password"); // This authToken is required in  
subsequent calls
```



Use case 2

SOAP example using the SDK : Query Viewer Service

```
// Get the QueryViewerService and get the data
```

```
QueryViewerServiceClientFactory factory = new QueryViewerServiceClientFactory ();  
QueryViewerService service = factory.createClient();  
MatrixData md = service.getMatrixData(authToken, "cswswTlzgBABCKipuKVcyzlg==");
```

```
// Get the Column Names
```

```
List<String> headers = md.getColumnHeaders();  
int col = 0;  
for (String header : headers) {  
    System.out.printf((col++%2 == 0 ? "%60s" : "%20s\n"), header);  
}
```

```
// Get the Data
```

```
List<ListWrapper> rows = md.getRows();  
for (ListWrapper row : rows) {  
    List value = row.getValue();  
    for (Object obj : value) {  
        System.out.printf((col++%2 == 0 ? "%60s" : "%20s\n"), obj);  
    }  
}
```



Use case 2

Keep in mind

I found that I needed the following **static block** to trust the hostname

// Static Block

```
static {  
    HttpURLConnection.setDefaultHostnameVerifier(new HostnameVerifier() {  
        public boolean verify(String hostname, SSLSession session) {  
            // Make sure that hostname is valid  
            return true;  
        }  
    });  
}
```

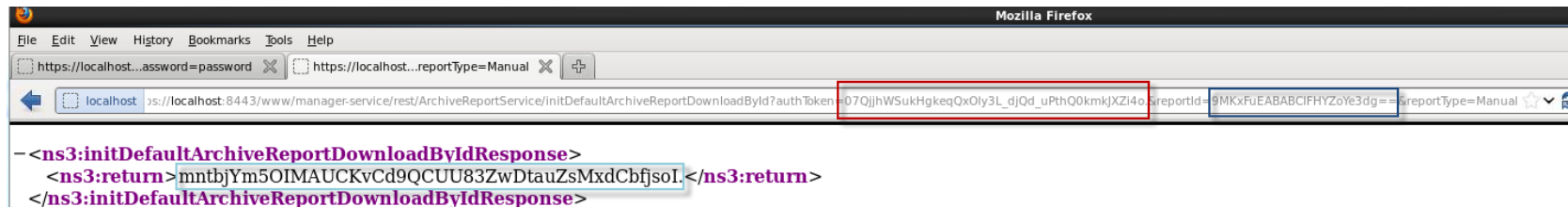


Use case 3

REST call to Archive Report Service

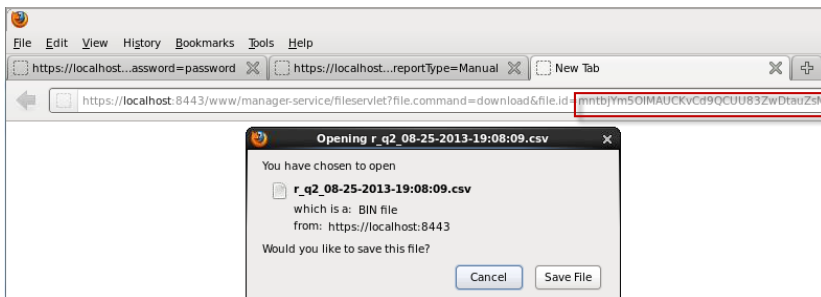
Step 1: Start the Report Generation

https://localhost:8443/www/manager-service/rest/ArchiveReportService/initDefaultArchiveReportDownloadById?authToken=_&reportId=_&reportType=Manual



Step 2: Get the Download ID and download the report

<https://localhost:8443/www/manager-service/fileservlet?file.command=download&file.id=DOWNID>



Required libraries and interesting observations

Tips from an end user

- Even though it's SOAP under the covers **AXIS2** libraries didn't work
 - **manager-ws-client-1.2.0.release.107.jar**
 - **core-ws-client-1.5.0.release.51.jar**
 - **coma-infrastructure-1.4.0.release.240.jar**
- For now, the SOAP APIs can only be written in Java and using these libraries
- I was not able to get it to work with **AXIS2** libraries in the **CLASSPATH**
 - Marshalling Errors
- Don't forget to implement a **HostnameVerifier** (by default it will NOT be a verified hostname)
- Documentation is available on Protect 724



Recap

Key takeaways

- REST – for simple use cases
- SOAP – For now, Java clients using the provided libraries
- GWT-RPC is also used by our UI team



Please give me your feedback

Session 3139 **Speaker Shivdev Kalambi**

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.



Thank you

