Deployment Guide

Document version 1.6

What's inside:

Business Partner

Ready for Security Intelligence

Deploying the BIG-IP Application Security Manager with IBM InfoSphere Guardium

Welcome to the F5 deployment Guide for securing your infrastructure with the BIG-IP Application Security Manager (ASM) and IBM® InfoSphere Guardium, IBM's database security appliance. This document provides guidance on how to deploy the BIG-IP ASM with IBM InfoSphere Guardium. By combining the powerful security and reporting features in BIG-IP ASM with the advanced database inspection functionality and reporting of Guardium, organizations can now gain an unparalleled real-time view into the operation of their websites.

IBM InfoSphere Guardium provides a simple, scalable, and powerful solution for real-time database activity monitoring. By deploying Guardium appliances to collect information from databases, your organization gains up-to-the-second insight into the activity happening at the application and data level. Now, by deploying the Database Security functionality within the BIG-IP system, you can correlate front-end information with database information. This information allows administrators to take a variety of actions, such as preventing attacks, enforcing controls, auditing access and many other essential database tasks. For example, using Guardium and BIG-IP ASM, an administrator can run a dashboard which shows in real-time which SQL statements are generated by a front-end user.

Why F5

F5 and IBM have partnered to bring this innovative solution to our joint customers. The real-time integration between BIG-IP and Guardium provides a level of introspection into the operation of your website that exceeds other solutions on the market today. The benefits of this integration include:

- BIG-IP ASM and Guardium integration allows end-user information to be correlated to individual SQL actions on the database in real-time.
- Guardium can also correlate and report on events that do not have an SQL component, enhancing the value of the Guardium solution.

For more information of IBM Guardium see: *http://www-01.ibm.com/software/data/guardium/*

For more information on the F5 BIG-IP system, see *http://www.f5.com/products/big-ip*

Products and versions tested

Product	Version
BIG-IP LTM and ASM	11.3 HF-1 or later
IBM InfoSphere Guardium	v 9.0 with Patch p02_GPU_October_2012 or later

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/ibm-guardium-asm-dg.pdf*

Critical → *For both the BIG-IP system and Guardium, the versions listed are absolute requirements.*

Prerequisites and configuration notes

The requirements for this integration are primarily connectivity and network communication between the BIG-IP appliance and the Guardium appliance.

- You must meet the version and software requirements for BIG-IP and Guardium. Specifically, ***you must be running BIG-IP with ASM software version 11.3 Hotfix 1 or higher*** and the ***Guardium appliance(s) with version 9.0 Patch Level 2 (9.0p02_GPU_October_2012) or higher.***

- You must have TCP/IP Network connectivity between your BIG-IP devices and the Guardium appliance(s). The BIG-IP system initiates a connection to Guardium on TCP port 16016 from BIG-IP system's Self IP address. Configure your firewalls or filters to allow the source (BIG-IP Self IP), destination (Guardium appliance or virtual server IP address) and TCP port (default 16016).

- You must have an HTTP or HTTPS based application that traverses BIG-IP LTM and ASM. ASM and Guardium work together to correlate HTTP/S and SQL events, therefore, your primary application should traverse a virtual server on the BIG-IP system which has ASM enabled. Your BIG-IP LTM virtual server must be configured before deploying BIG-IP ASM. For information on configuring the BIG-IP LTM for a specific application, see the F5 deployment guides (http://www.f5.com/products/documentation/deployment-guides/), or the BIG-IP documentation.

  You must have information about your application, including its HTTP or HTTPS URL, the Authentication Type (HTML Forms, Basic Auth or NTLM), the user name and password parameter, and information about that will help validated proper access. An example is provided in *Appendix A - Gathering information to populate the login page entry screen on page 12*.

- For Guardium, you must have one of the supported databases: DB2, Informix, MySQL, Oracle, PostgreSQL, Sybase, Microsoft SQL. Please see Guardium for additional supported systems and databases.

- DNS must be configured on your BIG-IP system, so that the BIG-IP device is able to resolve the host name of your Guardium machine. To configure DNS, expand **System**, click **Configuration**, and then on the Menu bar, from the **Device** menu, click **DNS**. For more information, see the online help or BIG-IP system documentation.

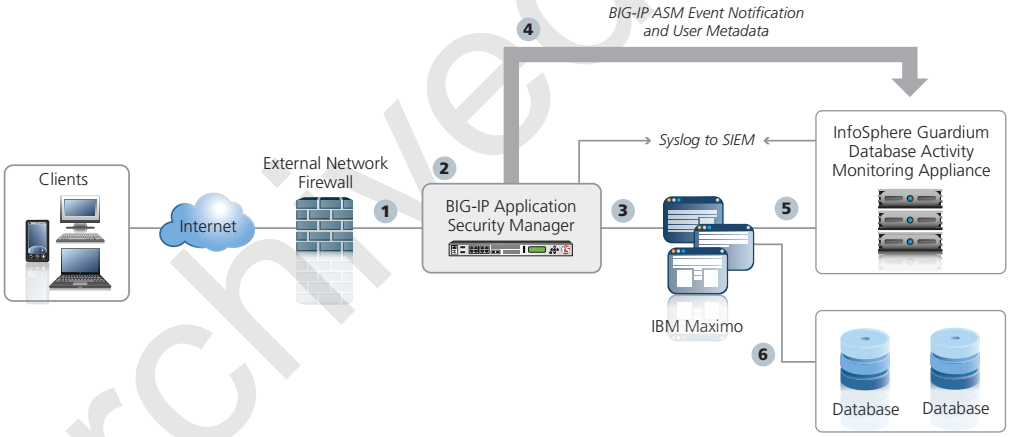
- We recommend you review and consider the deployment guide for load balancing Guardium appliances with BIG-IP Local Traffic Manager: http://www.f5.com/pdf/deployment-guides/ibm-guardium-dg.pdf. By load balancing Guardium appliances, the best possible availability and scaling can be achieved.

Configuration example

In this document we describe the configuration of the front-end BIG-IP system (labeled #2 below). It is a prerequisite that your environment already have an application which will be protected (in our example, IBM Maximo, labeled 3 below) and that you have the InfoSphere Guardium appliance(s) (labelled 5 below) setup.

The following diagram shows the configuration described in this guide. There are five primary components:

1. Web and Application servers that house the content being served,
2. A database used by the application servers,
3. A BIG-IP appliance that provides the front-end Virtual IP for the Application
4. An ASM Module on BIG-IP that is associated with the LTM Virtual IP



Flow:

1. A client request comes into the BIG-IP system to be load balanced to a web application (Tivoli Maximo Asset Management software in our example).
2. BIG-IP ASM examines the request based on the security policy associated with the virtual server.
3. The BIG-IP LTM makes the best load balancing decision at the application level to direct traffic to web servers.
4. The BIG-IP ASM sends associated information to the Guardium appliance.
5. The IBM S-TAP kernel plugin sends a copy of database queries and commands to the Guardium collector appliance. Note that in some instances, port mirroring may be used instead of kernel plugins. This factor does not impact our solution at all.

   See the IBM documentation on the proper installation and configuration of the IBM S-TAP.
6. The application maintains its own database connection as usual.

Not pictured in this diagram is an additional BIG-IP system that can be used to load balance and provide high availability to the Guardium appliance(s). Please see the F5 Deployment Guide for Load Balancing Guardium which will fill in the additional detail on this load balancing at: *http://www.f5.com/pdf/deployment-guides/ibm-guardium-dg.pdf*.

Configuring BIG-IP ASM to send requests to Guardium

In this section, we configure the BIG-IP ASM to send requests to Guardium. Remember that your BIG-IP Local Traffic Manger (LTM) virtual server must be already configured using the best practices for your particular application. Your virtual server must include an associated HTTP profile.

Performing the initial BIG-IP system configuration

While the BIG-IP LTM may already be configured for your application, in this deployment guide we are also configuring the BIG-IP system to communicate, with a TCP connection, to the Guardium appliances. This section is concerned with the initial configuration for the BIG-IP system to communicate with Guardium.

If necessary, create the initial BIG-IP configuration objects (such as VLANs, Self IPs, and Routes) in order to reach the Guardium appliance or, if your Guardium environment is load balanced, the BIG-IP virtual server IP address. Configuring these objects is outside the scope of this document. See the BIG-IP system product documentation, available at http://support.f5.com/kb/en-us/.

Checkpoint

Use the checkpoints to ensure the configuration is working properly up to this point

Checkpoint

After you have configured the VLAN, Self IP, and routing required to reach the Guardium appliance or virtual server IP address for Guardium, use this checkpoint procedure to verify the connectivity. Login to the BIG-IP system console via SSH and check to see if you can ping the IP address of the Guardium appliance or Virtual IP Address. In our example the Guardium appliance is at IP address 10.0.140.245:

```
[root@bigip-ve2:Active] config # ping 10.0.140.245
PING 10.0.140.245 (10.0.140.245) 56(84) bytes of data.
PING 10.0.140.245 (10.0.140.245) 56(84) bytes of data.

64 bytes from 10.0.140.245: icmp_seq=1 ttl=64 time=0.025 ms
64 bytes from 10.0.140.245: icmp_seq=2 ttl=64 time=0.027 ms
64 bytes from 10.0.140.245: icmp_seq=3 ttl=64 time=0.027 ms
64 bytes from 10.0.140.245: icmp_seq=4 ttl=64 time=0.028 ms
```

If the ping is unsuccessful, see *Troubleshooting on page 9.*

Creating the ASM Security Policy

After you have confirmed basic connectivity to the Guardium appliance from the BIG-IP create the ASM Security Policy and Database security connection.

The specific settings you configure in the security policy depend on your application and your environment. The policy we create in the following procedure is an example based on the Tivoli Maximo Asset Management software which we are using to demonstrate this solution.

Important

As noted in the prerequisites, your BIG-IP Local Traffic Manger (LTM) virtual server must be already configured using the best practices for your particular application. Your virtual server must include an associated HTTP profile. In our example we have configured load balancing for IBM Maximo Asset Management.

To create the ASM security policy

1. On the Main tab, expand **Security**, and then click **Application Security**.
2. Click the **Create** button. The Deployment Wizard opens.
3. In the **Local Traffic Deployment Scenario** section, make sure **Existing Virtual Server** is selected, and then click the **Next** button.
4. From the **What type of protocol does your application use** list, select the appropriate protocol.
5. From the **Virtual Server** list, select the virtual server you previously created for your application, and then click **Next**.
6. In the **Deployment Scenario** section, select a method for building and deploying the security policy, and then click **Next**. In our example, we leave the default **Create a policy automatically (recommended)**.
7. From the **Security Policy Language** list, select a language. We leave the default, **Auto Detect**.
8. In the **Security Policy is case sensitive** section, enable or disable case sensitivity for the policy. We leave the default, **Enabled**.
9. In the **Differentiate between HTTP and HTTPS URLs** section, enable or disable this option for the policy, and then click **Next**. In our example, we leave the default, **Enabled** as we are protecting Tivoli Maximo Asset Management software which has both HTTP and HTTPS components.
10. In the Systems section, from the **Available Systems** box, select any of the systems to which you want to protect with the security policy, and then click the Add (**<<**) button. In our example, we select **Unix/Linux**, **Apache**, **Java Servlets/JSP**, and **IBM DB2**.
11. In the Signature Staging section, enable or disable signature staging, and then click **Next**. We leave the default, **Enabled**.
12. From the **Policy Type** list, select a type for the policy. In our example, we leave the default, **Fundamental**.
13. The rest of the settings can be configured as applicable. In our example, we enable **AJAX blocking response behavior** and leave the defaults for the remaining settings.
14. Click **Finished**.

In order to continue to the next step, creating the link to Guardium, you must apply the policy for BIG-IP ASM. Use the following procedure to make sure your policy is applied:

To apply the security policy

1. On the Main tab, expand **Security** and then click **Application Security**.
2. Click the name of the security policy you just created. The name of the security policy is the virtual server name that you selected in Step 5 of the previous procedure.
   Note you can optionally change the name of the policy from this screen.
3. Click the **Apply Policy** button on the right side of the screen.

Configuring connectivity to the Guardium Database Security System

Next, we will configure the connectivity and configuration to the Guardium Database Security System.

To configure Guardium connectivity

1. On the Main tab, expand **Security**. From the **Application Security** menu, select **Integrated Services**, and then click **Database Security**.
2. From the **Current edited policy** list, makes sure the policy you created is selected. If it is not, select it from the list.
3. If you see a warning stating "*Database Security Server is not configured. Please set up your Database Security Server first*" click the **Database Security Server** link to configure the server. The Database Security Configuration page opens.
   a. In the **Server Host Name** box, type the host name of your Guardium server.
   b. In the **Server IP Address** box, type the IP address of the server. This is the IP address of the Guardium appliance or, if you have a load balanced environment, the virtual server IP Address associated with the pool of Guardium appliances.
   c. In the **Server Port Number** box, type the port number if it is different than the default, 16016.
   d. From the **Request Hold Timeout** list, select **Enabled** or **Disabled** as appropriate. In our example, we select **Enabled** and use the default of **5** milliseconds.

      The request hold timeout setting is optional. We enable it here to have the minimum impact because we are setting a threshold of 5 milliseconds for the Guardium Database Firewall to respond with a TCP Ack message. This will have the absolute minimum impact possible on client traffic. Adjust this setting, or disable it if capturing 100% of the traffic to Guardium is more important for your environment than a delay to client traffic
   e. Click **Save**. You return to the Database Security page.

Checkpoint
Use the checkpoints to ensure the configuration is working properly up to this point

Checkpoint

After you press Save, you should be able to login to the Guardium User Interface and view the BIG-IP in the S-TAP host list immediately. If the BIG-IP does not show up in the host list at this point, see Troubleshooting on page 9.

4. In the Database Security Integration row, check the **Enabled (Forward request information to Database Security Server)** box. This enables forwarding request information to the Guardium Database Firewall.
5. From the **User Source** row that appears, if you are using the BIG-IP Access Policy Manager on the BIG-IP system, you can select **APM Usernames and Session ID**. Otherwise, select **Use Login Pages**. In our example , we select Use Login Pages to define login pages manually.
6. If you selected Use Login pages, a warning appears stating "*There are no login pages configured. In order for username to be sent to Database Security, please configure login pages.*" Click the **login pages** link. The Create Login page wizard opens.

   You must now enter the information from *Appendix A - Gathering information to populate the login page entry screen on page 12*.
   a. In the **Login URL** box, type the login URL. In our example, we type **/maximo/webclient/login/login.jsp**.

b. From the **Authentication Type** list, select a type. We use **HTML Form**.

c. In the **Username Parameter Name** box, type the user name parameter. In our example, we type **username.**

d. In the **Password Parameter Name**, type the password parameter. In our example, we type **password**.

e. In the **Access Validation** section, configure any of the settings as applicable for your configuration.
In our example, in the **Expected HTTP response status code** box, we type **200**.

f. Click **Create.**
You may have to go back to Application security, select your profile and press Apply in order to be allowed to save the login page changes. If login page is greyed out, repeat the steps above to apply your changes.

7. Click **Save**.

Configuring session tracking for the Security Policy

Next, we configure session tracking on the security policy you created.

To configure session tracking

1. On the Main tab, expand **Security**, select **Application Security**, and then from the fly menu, click **Sessions and Logins**.
2. On the Menu bar, click **Session Tracking**.
3. From the **Current edited policy** list, makes sure the policy you created is selected. If it is not, select it from the list.
4. In the **Session Awareness** row, check the **Enabled** box.
5. From the **Application Username** list, select **Use Login Pages**.
6. From the **Available** list, select the Login page you created in Step 6 in the preceding procedure and then click the Add (**<<**) button to move it to the **Selected** list.
7. Click the **Save** button.
8. Click the **Apply Policy** button on the right side of the screen.

Configuring IBM Guardium to translate the data stream

Next, the Guardium appliance must be configured to translate data streams from the BIG-IP system to the Application User for SQL parsing. You must use the Guardium command line interface for this procedure.

Prerequisites - Before beginning this section, you need to:

- Note the IP addresses of each of the Application servers with STAP installed that are a part of this solution.
- Note the BIG-IP virtual server IP address created for your application.

To configure Guardium to translate the data stream

1. Login to the Guardium appliance using the Command Line Interface (CLI user). Refer to the Guardium documentation for specific instructions. Typically you would use an SSH application to make this connection.

2. Configure the application server IP address(es) (**appsIP**) and the BIG-IP virtual server IP address (**bigIP**) created for your application and associate them with each other using the following command syntax.

   grdapi F5_add_apps_config appsIP=app server IP Address bigIP=Application Virtual IP Address

   Note that this statement is case sensitive.

   For example, if the application server addresses are 192.168.10.100, 192.168.10.101, and 192.168.10.102 and the BIG-IP virtual server for your application is 172.10.10.100, the appropriate commands would be:

   ```
   grdapi F5_add_apps_config appsIP=192.168.10.100 bigIP=172.10.10.100
   grdapi F5_add_apps_config appsIP=192.168.10.101 bigIP=172.10.10.100
   grdapi F5_add_apps_config appsIP=192.168.10.102 bigIP=172.10.10.100
   ```

3. Configure the parameters that should be captured using the command

   grdapi F5_add_data_params paramName="name1" minData=1 maxData=100

   Note that this statement is case sensitive.

   In our example, we will be capturing the username and so our entry would look like:

   grdapi F5_add_data_params paramName="username" minData=1 maxData=100

   For reference:

   - **paramName** is the name: "paramName" part of a name/value pair in F5 data stream.
   - **minData** is minimum length of value of the pair to be looked at. If unknown, put 1.
   - **maxData** is maximum length of value of pair to be looked at. If unknown, put 100.

   Appendix A - Gathering information to populate the login page entry screen on page 12 contains detailed information on this process.

4. Verify your entries after you are done to check for errors using the following commands:

   grdapi F5_list_apps_config

   and

   grdapi F5_list_data_params

   After you enter these commands, they are automatically committed to the Guardium database and become part of the running configuration.

Next Steps

After the basic connectivity between BIG-IP and the Guardium appliance has been configured and application security has been established on BIG-IP ASM, the next steps are to monitor the application within BIG-IP ASM and write useful reports on the Guardium appliance.

- First, employ comprehensive or unit testing to ensure your application environment is behaving properly after applying application security. Refer to BIG-IP ASM documentation on the best practices surrounding this topic.
- Second, monitor the BIG-IP ASM policy dashboard (on the Main tab, under the Security) to understand how ASM is protecting your site and what, if any changes are recommended as the BIG-IP ASM learns your unique traffic patterns.
- Third, begin using Guardium according to the product documentation, to access real time reports that expose exactly what is happening on your website.

Troubleshooting

Be sure to carefully read all of the prerequisites listed in the beginning of this guide. Pay particular attention to the version requirements for the BIG-IP system and the Guardium appliance, and pay particular attention to the TCP connectivity requirements between the BIG-IP system and Guardium.

No response from a ping to your Guardium Virtual IP Address or Guardium appliance IP address from the BIG-IP system

If you had a failure after the first checkpoint in this document, it is possible that you have a routing issue between your BIG-IP device and the Guardium appliance.

It is also possible that you have a restrictive firewall in between the two devices that is blocking ICMP ping messages. If this is the case, you do not need to resolve this issue. The only communication necessary between the BIG-IP system and Guardium is TCP traffic. ICMP is only used in this example as a means of verifying connectivity.

Considerations

- The BIG-IP appliances must be able to communicate with the Guardium appliances over TCP in a connection initiated from the BIG-IP system and terminated on the Guardium appliance.
- The traffic exiting the BIG-IP will be sourced from a Self IP address in the traffic management side of the BIG-IP, not the management interface.
- There must be a route back to the BIG-IP system from the Guardium appliance.

Steps to resolve the issue

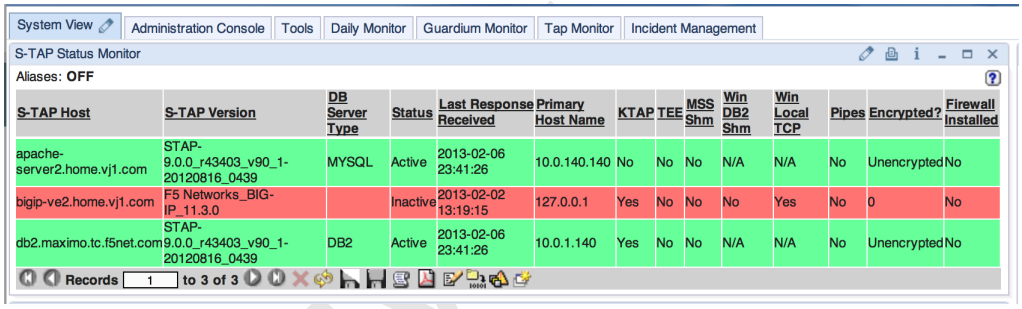
- From the BIG-IP Configuration utility, on the Main tab, expand **Network**. From the Network section, perform the following:
  - » Click **VLANs** to check the VLAN settings. Do you have a VLAN configured on the BIG-IP to handle the outgoing traffic? Is the VLAN tagged or untagged properly? Review your VLAN assignments and if necessary review the F5 product documentation on VLANs, available on Ask F5: *http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-concepts-11-3-0/tmos_vlans.html* .

    Adjust your VLAN settings if necessary.
  - » Click **Interfaces** to check the Interfaces settings. Does the Interface associated with your VLAN show a status of "Up"? Is the Interface associated with the proper VLAN? Adjust your Interface settings from the VLAN menu if necessary.
  - » Click **Self IPs** to check the Self IP settings. Are the Self IP address and subnet mask correct? Is the Self IP address associated with the proper VLAN? Adjust the Self IP address, subnet mask and VLAN association as necessary.
  - » Click **Routes** to check the Route settings. Is there a route that instructs the BIG-IP system where to send traffic for the destination (the Guardium appliance or Virtual IP Address)? Add a default route or a static route. If necessary review the BIG-IP Product Documentation on Routing: *http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-ip-routing-administration-11-3-0.html* specifically the chapters on static route management and default routes.
  - » Check the Guardium appliance and verify that the Guardium appliance has a route back to the BIG-IP system. For specific instructions, see the IBM documentation.

» Check any intermediate routers in between the two appliances to verify that all routes are properly configured. When troubleshooting these issues, a good rule of thumb is to start at "the ends" and work your way towards the middle. In this example we started with the BIG-IP system and the Guardium appliance and then check intermediate devices. The goal is to ensure that routing is properly configured.

The BIG-IP system does not show up in the Guardium appliance User Interface

If you have finished the configuration of the BIG-IP device, the BIG-IP LTM should be visible in the Guardium User Interface. An example of this represented by the following screenshot:



S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Primary Host Name	KTAP	TEE	MSS Shm	Win DB2 Shm	Win Local TCP	Pipes	Encrypted?	Firewall Installed
apache-server2.home.vj1.com	STAP-9.0.0_r43403_v90_1-20120816_0439	MYSQL	Active	2013-02-06 23:41:26	10.0.140.140	No	No	No	N/A	N/A	No	Unencrypted	No
bigip-ve2.home.vj1.com	F5 Networks_BIG-IP_11.3.0		Inactive	2013-02-02 13:19:15	127.0.0.1	Yes	No	No	No	Yes	No	0	No
db2.maximo.tc.f5net.com	STAP-9.0.0_r43403_v90_1-20120816_0439	DB2	Active	2013-02-06 23:41:26	10.0.1.140	Yes	No	No	N/A	N/A	No	Unencrypted	No

In this screenshot, you can see that the BIG-IP system has connected to the Guardium appliance but is showing Inactive. This indicates that there was connectivity at one time, but that connectivity has been lost. In this example, our BIG-IP system was simply turned off.

Also note that the IP address of the BIG-IP system is currently reported as 127.0.0.1 (localhost). This is a known issue.

Considerations

- There must be network connectivity between the BIG-IP system and the Guardium virtual server IP Address or the Guardium appliance.
- TCP connectivity must be allowed between the devices; the default port for Guardium is **16016**.
- The TCP connection is initiated from the BIG-IP system outbound to the Guardium virtual server IP Address or the Guardium appliance.
- The connections involved in this solution are long-lived.

Steps to resolve the issue

- Follow the troubleshooting steps for pinging (above) even if your internal firewalls do not allow ping traffic. Make certain that you have configured your routing properly.
- Make certain that all intermediate firewalls allow port 16016. If your intermediate firewalls are state-full, make certain that they will allow long-lived TCP connections. In other words, make certain your firewall is not terminating the connection prematurely.
- Make certain your Guardium device is listening on the appropriate port. Use the **telnet** command on the BIG-IP system to test connectivity, for example:

[root@bigip-ve2:Active:Standalone] config # **telnet 10.0.1.140 16016**

```
Trying 10.0.1.140…
Connected to 10.0.1.140.
Escape character is '^]'
pp
```

In this example, the telnet connection succeeded, and the **p** characters indicate a successful heartbeat from the Guardium appliance.

- Check the settings in the ASM module Database Security section to make certain you have configure the proper IP Address and TCP Port.
- Finally, if communication still does not work, double check your Guardium setup by connecting another device or appliance, such as a database, to make certain that the Guardium appliance is configured properly.

Appendix A - Gathering information to populate the login page entry screen

In this deployment guide we configure the transmission of user information to the Guardium appliance. In order to identify the user and forward the information related to this user to Guardium, the ASM Database Security Integration uses one of two methods: integration with the BIG-IP Access Policy Manager (APM), or manual configuration of your application. This appendix provides guidance on how to gather information for manual configuration of your application for BIG-IP ASM's Database Security Integration menu.

There are four primary components that must be understood in order to configure this screen:

- The Login type (HTTP/S) and the Login URL (though technically we are referring to the login URI here)
- The Authentication Type
- Username and Password Parameter Names if using HTML Form Authentication
- Access Validation method

In determining the values to capture, both on the BIG-IP ASM and on the Guardium device, the application you are protecting should be analyzed for the useful data that is present. In this Appendix we show two aspects of making this determination, though in reality the building and creation of dynamic security requires some additional planning which is not within the scope of this document. In the first part of this appendix, we describe how to identify the username and password fields for your given application, if the application uses forms based auth. In the second part, we describe how to look at your application traffic after the BIG-IP system has sent the relevant information to Guardium to pull out the most useful parameters.

Basic flow

The four primary components (Login URL, Auth type (Password, Username) and Access Validation) tell the BIG-IP ASM when to start collecting data to be passed on to Guardium. In our example application, IBM Maximo Asset Management, HTML Form Authentication is used (this is the type of authentication where the user is presented with a screen which collects login information). In contrast, the other forms of authentication are automatically detected by the BIG-IP system.

Tools required

The following tools make this process easier:

- A web browser which allows you to view the source code of a page.
- An HTTP analysis plugin. In our example we are using a licensed copy of HTTPWatch (you may also use Fiddler, Yslow, Myriad or other such plug-ins).

Our example: IBM Maximo Asset Management Software

In this deployment guide, we used the IBM Maximo Asset Management system to demonstrate the integration between the BIG-IP system and Guardium. In this section, we walk through the process of how we deciphered the information to populate the Login Page to make it easy to repeat this procedure with your own applications.

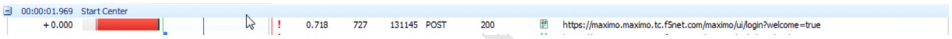
First, using a browser, navigate to your application. Make certain that you are logged out of your application at this point. Because are using HTML Form authentication, your application should have a logout button or you may have to close and reopen your browser to clear the session cookies.

1. Navigate to the login screen of your application and note the URL of the login page. In our example, the URL of the login page is:
   https://maximo.maximo.tc.f5net.com/maximo/webclient/login/login.jsp?welcome=true

   Note the login type is **HTTPS** and the URI we are interested in follows the host name and domain name, specifically: **maximo/webclient/login/login.jsp**.

   We discard the GET variable inserted after the login.jsp (?welcome=true).

   In order to verify this, use HTTPWatch to record the login process. Open the HTTPWatch menu (or similar application), press Record. Look for an HTTP POST request and verify the login URI (often, but not always, the same as the URI in your browser). In our example:

   This confirms our Login type and URI.

   Alternatively you can use a wildcard instead of explicit URI definition by toggling the drop down menu next to the Login Type. In our example, the wildcard match would look like this: **/maximo/webclient/login/login***
   This allows you to be more general in matching a login type.

2. Second, we will identify the Username and Password fields within our application. For this process, there are several ways of accomplishing this task.

   a. Use the **View Source** function on your web browser to open the login page (before you are logged in) and scan the HTML data for the names of the fields that refer to the username and password. In the case of our application, by scanning the source we find the following two lines:

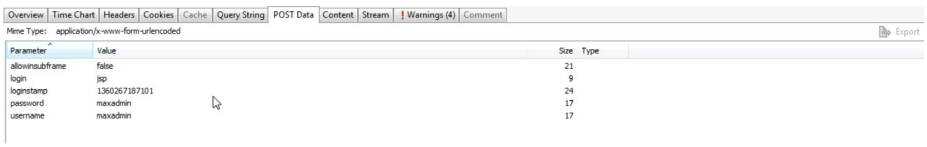
   ```
   <input  class="isc-login-textfield" name="username" id="username"
   langcode="EN" type="text">

   <label for="password" class="isc-login-label">password</label>
   ```

   Note that these two lines were not adjacent to each other in the HTML but they have been condensed here for this example.

   Using this method, we can determine that the Username field is called "username" and the Password field is called "password".

   b. Use the HTTPWatch (or similar) plugin. Again, open HTTPWatch, press Record and record the process of logging in. Examine the HTTPWatch output and find the HTTP Post request which matches the login URI and use the "POST Data" tab to examine the data submission. In our example:

   You can see from this output that the two fields matching the username and password are called, "password" and "username".

   Note, that while many programs use clear and straightforward naming of fields, such as username and password for their respective fields, this is not always the case. The engineers of the Maximo application have implemented clear and straightforward naming.

c. The final option is to determine a method to validate that the login actually happened successfully. There are a number of ways to achieve this. Review the options under the **Access Validation** menu and refer to the product documentation for specific details. In short, the concept is the same; you must either define an HTTP response code, a string that appears in the response, a cookie or a GET value.

   Because Maximo gives a non-HTTP 200 code when the login is unsuccessful, in our example we simply use the "Expected HTTP response status code" of 200 to validate our login was successful.

Finding the parameters in IBM Guardium

In order to find the parameters mentioned in the section on the Guardium appliance, use the following guidance.

You find the name/value pairs by doing the following:

- Make sure the BIG-IP system and STAP (if used) show as connected to gMachine.
- On the Guardium machine, turn on **slon** using the following two commands: **/var/guardium/bin/slon –p on** and **/var/guardium/bin/slon –z on**.
- Log into the application through the new virtual IP you created earlier.
- Do a couple of small actions, and then log out.
- Turn off **slon** using the following two commands: **/var/guardium/bin/slon –p off** and **/var/guardium/bin/slon –z off**.
- The resulting file will be located in **/var/log/guard/analyzer**, search for W_REQ_Login.

Example	Notes
TIME: Mon_30-July-2012_17.21.21.798 **@F5 request (server level)@ - type: CLIENT_REQUEST** **client_request {** **type: W_REQ_LOGIN** **<cut code for brevity>** **user_name: "admin5"** **client_ip {** **ip0: 0** **ip1: 0** **ip2: 65535** **ip3: 673710081** **}** **<cut>** **data {** **type: POST_DATA** **is_truncated: false** **name: "username"** **value: "admin5"** **}** **data {** **type: POST_DATA** **is_truncated: false** **name: "password"** **value: "admin123"** **}** **<cut code for brevity>**	In the data sets where type: POST_DATA, you can see 2 name/value pairs. Pair one, paramName is "username" and the value, in this case, is "admin5". Pair two, paramName is "password" and value, in this case, is "admin123". The cli command to set for the pairs are: **cli> grdapi F5_add_data_params paramName="username" minData=1 maxData=100** **cli> grdapi F5_add_data_params paramName="password" minData=1 maxData=100**

You must add at least two parameters: a username because it appears on the login screen under W_REQ_LOGIN, and an additional parameter that appears on every page you want to track under W_REQ, such as a cookie. This is typically JSESSIONID, but could be another session cookie. If the application does not provide a session cookie, the BIG-IP system can insert a cookie (such as BIGipSession<app_name> cookie). Other common parameters are session_id, email, SID, and so on.

Important

Make sure the parameter(s) you use are present in the HTTP headers of every page you would like tracked. For example, if using an arbitrary application provided ID, make sure the application server transmits this ID on every request. If you use a parameter that is not present on every page, you will have incomplete correlation in Guardium. Some examples of IDs that typically appear on every request include JSessionID, authorization cookies, and cookie-based session IDs.

You must use the Guardium command line interface. The command to set is:

```
cli>  grdapi F5_add_data_params paramName="name1" minData=1 maxData=100
```

Where:

- **paramName** is the name: "paramName" part of a name/value pair in F5 data stream.
- **minData** is minimum length of value of the pair to be looked at. If unknown, put 1.
- **maxData** is maximum length of value of pair to be looked at. If unknown, put 100.

Document Revision History

Version	Description	Date
1.0	New guide	02-11-2013
1.1	- Added BIG-IP ASM Session Awareness instructions. - Added Guardium grdapi instructions. - Added grdapi guidance.	02-21-2013
1.2	- Moved the important note concerning having an existing BIG-IP LTM virtual server to after the Checkpoint on *page 4*. - Corrected the procedure heading in *Configuring connectivity to the Guardium Database Security System on page 6*	06-17-2013
1.3	Updated the diagram in the *Configuration example on page 3* to remove the line between the InfoSphere Guardium Database Activity Monitoring Appliance and the databases below it.	07-15-2013
1.4	Updated step 5 in the traffic flow description in the *Configuration example on page 3* to be more accurate.	09-26-2013
1.5	- Clarified parameter guidance at the end of *Finding the parameters in IBM Guardium on page 14*. - Clarified IP address guidance in *Configuring IBM Guardium to translate the data stream on page 7.*	04-03-2014
1.6	Further modified the IP address guidance in *Configuring IBM Guardium to translate the data stream on page 7.* The previous guidance assumed an infrastructure where the application and the database where on the same host. This version is more clearly detailed for production environment usage.	04-07-2014

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com