Technical white paper

Configure HP DMA and SA to Use the SA Gateway Network as a Proxy Network

HP Database and Middleware Automation versions 10.10 (or later)

Table of Contents

Purpose

This paper describes how to configure HP Database and Middleware Automation (HP DMA) and HP Server Automation (SA) to enable the use of the SA Gateway Network as a Proxy Network for HP DMA communication traffic.

Audience

This white paper is intended for system architects and administrators who are responsible for the turn up of HP DMA and/or SA environments or for planning infrastructure utilizing HP DMA and SA.

Goal

When you follow the instructions provided in this paper, you will create a configuration that allows HP DMA traffic to be routed through the SA Gateway Network from the managed server back to the HP DMA Server. By following the instructions in this paper you can avoid having to open up any extra firewall ports from a Managed Server.

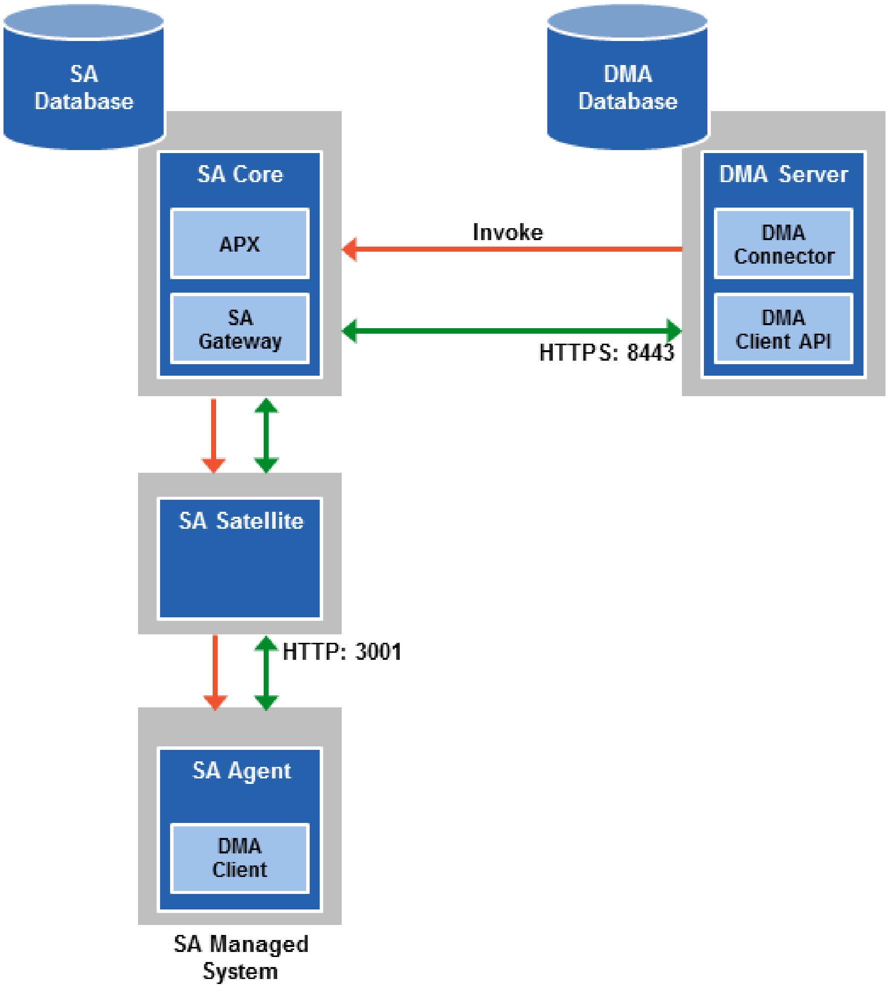
The following diagram shows how HP DMA communications work with an SA Satellite serving as a proxy:

1. HP DMA invokes SA to run the DMA Client on the target SA Managed Server.
2. SA communicates across the SA Satellite to the SA agent on the target server.
3. The SA agent invokes the DMA Client.
4. The DMA Client communicates using HTTPS via the SA Satellite proxy.

In this case, the DMA Client uses the same port used by SA on the SA Satellite to forward information to the SA Gateway. The SA Gateway then routes the information to the HP DMA Server.

Note: You can configure HP DMA with a port other than 8443 (8443 is the default).

Figure 1: Routing HP DMA traffic through an SA Gateway Network from the Managed Server back to the HP DMA Server.



Prerequisites

Before you can perform the procedures in this paper, your environment must meet the following minimum requirements:

- An SA mesh environment (9.x or 10.x) with one or more SA Cores must exist, with optional Satellites (for example, using Satellite to SA Core over a Gateway rather than directly connecting the managed server and HP DMA Server).
- You must have administrative access to all SA Core servers within the mesh and the HP DMA Server.
- HP DMA 10.10 (or later) is required.

Note: An existing HP DMA Server installation is not required. These steps can be completed during the installation process. For more information, see *HP DMA Installation Guide* for version 10.10 (or later), section "Install the HP DMA Client for SA".

Process Overview

You will utilize the following process to complete the configuration:

1. Add the egress filter to the SA Core Gateway configuration. This is required for the HP DMA Server to be allowed as a traffic target. (See Step 1: How to Configure the SA Core Gateway Properties.)
2. Add the SA Realm of the SA Core (that the HP DMA Server is connected to) into the HP DMA Server context file. (See Step 2: How to Configure the SA Realm Parameter in the HP DMA Server.)
3. Add and configure the Custom Fields within the HP DMA Server Environment page. (See Step 3: How to Add and Configure Custom Fields on the HP DMA Server.)

Instructions for making each of these changes are provided here. For more information about the SA Satellite and SA Gateway, see the HP Server Automation documentation library, which is available on the HP Software Product Manuals web site:

http://h20230.www2.hp.com/selfsolve/manuals

Step 1: How to Configure the SA Core Gateway Properties

An EgressFilter rule must be added to the gateway properties of each slice within the SA Core that the HP DMA Server is connected to:

1. If it does not already exist, create the file:

```
/etc/opt/opsware/opswgw-cgws1-<REALM_NAME>/opswgw.custom
```

Note: SA customizations for the SA Core configurations must go in the `opswgw.custom` file. REALM _NAME is the name of the realm for the SA Core, and can be found in the `opswgw.properties` file (look for `opswgw.Realm=<REALM_NAME>`).

2. Add the egress filter in the following form to the `opswgw.custom` file:

```
opswgw.EgressFilter=tcp:<HP DMA Server IP Address>:8443:*:*
```

3. Restart the gateway by issuing the following command:

```
service opsware-sas restart opswgw-cgws
```

4. *Repeat steps 1-3* for each slice with the same realm within the SA Core to which the HP DMA Server is connected.

5. If all slice Core Gateways have been restarted and if a load balancer gateway is used, then restart the load balancer gateway.

   ```
   service opsware-sas restart opswgw-lgws
   ```

   Important: The load balancer gateway must be restarted *after all other gateways*.

Note: An egress filter rule is only necessary on each slice within the same realm within the SA Core that the HP DMA Server is connected to. It is not required for any other SA Core, Satellite, or slices belonging to a different realm.

Step 2: How to Configure the SA Realm Parameter in the HP DMA Server

If the HP DMA Server has already been installed, do the following:

1. Open the following file for editing:

   ```
   /opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml
   ```

2. Ensure that the webServiceUrl parameter is specified with an IP Address, as a hostname specification will not work when using the SA Gateway Network as a Proxy Network.

3. Add the following parameter line beneath the other parameters already specified:

   ```
   <Parameter name="com.hp.dma.conn.sa.SAConnector.saRealm"
   value="REALM_NAME"/>
   ```

   Here, REALM_NAME is the name of the realm of the SA Core that the HP DMA Server is connected to.

4. Restart the HP DMA Server by issuing the following command:

   ```
   service dma restart
   ```

If the HP DMA Server is being installed, repeat the above directions after baselining is completed and before starting the HP DMA Server.

The `dma.xml` file should now look similar to the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<Context allowLinking="true" disableURLRewriting="true"
  path="/dma" privileged="true" swallowOutput="true"
  workDir="/var/opt/hp/dma/work/dma">
<Valve className="org.apache.catalina.valves.AccessLogValve"
  directory="/var/log/hp/dma/" pattern="%h %l %u %t '%r' %s %b
  %S" prefix="localhost_access." suffix=".log"/>
<Parameter name="com.hp.dma.core.webServiceUrl"
  value="https://192.0.2.0:8443/dma"/>
<Parameter name="com.hp.dma.conn.trustAllCertificates" value="false" />
<Parameter name="com.hp.dma.conn.sa.SAConnector.saRealm"
  value="REALM_NAME" />
<Resource auth="container"
  driverClassName="oracle.jdbc.OracleDriver"
  factory="com.hp.dma.util.DmaTomcatContextHandler"
  maxActive="20" maxIdle="5" maxWait="2000" name="jdbc/dma"
  password="{AES}54dd1d97a915c4c3c8d0db986a1218db62008816fb924"
  type="javax.sql.DataSource"
  url="jdbc:oracle:thin:@dma1.mycompany.com: 1521:DMA"
  username="dma"/>
</Context>
```

Note: For more information, see *HP DMA Installation Guide* for version 10.10 (or later), section "Specify the Server Automation Realm.

Step 3: How to Add and Configure Custom Fields on the HP DMA Server

Create and configure the two Custom Fields that instruct HP DMA to route traffic through the proxy server. This procedure is performed in the HP DMA UI or via HP DMA REST API commands. See the API documentation at https://my.dma.server.com:8443/dma/api.

Configuring HP DMA Custom Fields for Proxy Communication

HP DMA uses two Custom Fields to control proxy communication:

- west_proxy_in_use tells HP DMA whether a proxy server will be used. Valid values are TRUE and FALSE: Or SA auto select versus an actual URL.
- `west_proxy_address` contains the full URL of the proxy including the proxy port (or the keyword SA_auto_select).

Note: Set the `west_proxy_address` to SA_auto_select if you want the target server to determine which SA Satellite to use as a proxy.

Tip: It is best practice to only use values of TRUE, FALSE, and field not set. Note that `west_proxy_in_use` is not case-sensitive.

These Custom Fields can be defined at both the organization level and the server level. This enables you to use a proxy server for communication with some targets but not others—or use different proxy servers to communicate with different targets.

If the proxy Custom Fields are defined at both the organization level and the server level, the server level proxy information takes precedence over the organization level proxy information.

The following table shows how HP DMA will communicate if `west_proxy_in_use` has values at both the organization level and the server level.

Proxy Precedence	Server value is TRUE	Server value is FALSE	Server value is not set
Organization value is TRUE	Use the proxy specified for the server	Do not use the proxy specified for this server	Use the proxy specified for the organization
Organization value is FALSE	Use the proxy specified for the server	Do not use the proxy specified for this server	Do not use a proxy for this server
Organization value is not set	Use the proxy specified for the server	Do not use the proxy specified for this server	Do not use a proxy for this server

FAQs

Why is the egress filter only required on one SA Core?

HP DMA uses the SA Realm name to supply a header in its traffic that tells the SA Gateway network which SA Core the traffic should be routed to. The SA Core must be the same one that the HP DMA Server is connected to; therefore it is the only one that requires the egress filter. If there are multiple slices within the SA Core, then the egress filter should be applied to the Core Gateway on each slice that belongs to the same realm as the HP DMA Server.

For more information see the HP SA documentation library: http://h20230.www2.hp.com/selfsolve/manuals.

What if I do not use slices in my SA environment?

If you do not use slices in your SA environment, then you only need to configure the egress filter for the Core Gateway of the SA Core to which the HP DMA Server is attached. This is true for single core and mesh environments where slices are not used.

Why did I get a “403 Forbidden” message when I ran an HP DMA workflow?

A “403 Forbidden” message may indicate a missing egress filter. Re-check the SA Gateway configuration file and the dma.xml configuration file to verify that the egress filter and saRealm parameters have been set.

Why must I use an IP address instead of the hostname for the DMA webServiceUrl setting in the dma.xml?

The gateway routing is IP-based and does not currently work with hostnames, requiring that the DMA server’s webServiceUrl be IP-based when traffic is to be routed through the SA Gateway as a proxy network.

Why do I have to add the saRealm parameter to the dma.xml?

If the realm is not specified correctly, then the SA Gateway routing may not be able to route the traffic correctly back to the DMA Server. ‘403 Forbidden’ messages can be an indicator that the saRealm parameter is missing from the dma.xml file.

To learn more about HP Database and Middleware Automation visit:

hp.com/go/dma

October 2013