DEPLOYMENT GUIDE
Version 1.1

Configuring BIG-IP WOM with Oracle Database Data Guard, GoldenGate, Streams, and Recovery Manager

ORACLE DATABASE READY

Table of Contents

Configuring BIG-IP WOM with Oracle Database Data Guard, GoldenGate, Streams, and Recovery Manager

Configuring BIG-IP WOM with Oracle Database Data Guard, GoldenGate, Streams, and Recovery Manager

Welcome to the F5 deployment guide for the BIG-IP WAN Optimization Module (WOM) and Oracle Database Replication. This guide describes how to configure the BIG-IP WOM for Oracle Data Guard, GoldenGate, Streams and Recovery Manager when you are looking to create an optimized WAN connection between two sites for these Oracle Database services. Oracle's Database replication and integration technologies help enterprises create greater levels of database integration, synchronization, business continuity, disaster recovery, and fast database failover.

Through an innovative, integrated architecture Oracle Data Guard uniquely combines synchronization, replication, and failover services to provide oracle databases with the features needed for mission-critical uptime for Oracle stand alone and Real Application Cluster (RAC) databases.

Oracle GoldenGate's best-in-class solutions enable real-time data integration and continuous data availability by capturing and delivering updates of critical information as the changes occur and providing continuous data synchronization across heterogeneous environments.

Oracle Streams enables the propagation of data, transactions and events in a data stream either within a database, or from one database to another.

Oracle Recovery Manager (RMAN) is an Oracle provided database utility for backing-up, restoring and recovering Oracle Databases.

For more information on Oracle Data Guard, see ***oracle.com/technology/deploy/availability/htdocs/DataGuardOverview.html***.

For more information on GoldenGate, please see ***http://www.oracle.com/goldengate***

For more information on Oracle Streams, see ***oracle.com/technetwork/database/features/data-integration/index-094137.html***
For more information on Oracle RMAM, see ***oracle.com/technetwork/database/features/availability/rman-overview-094650.html***.

The BIG-IP WAN Optimization Module is built to run natively on the BIG-IP hardware platform, and the F5 TMOS® unified architecture, integrating application delivery with WAN optimization technologies. This enables traditional acceleration technologies like SSL offloading, compression, caching, and traffic prioritizing to combine with optimization technologies like TCP Express, symmetric adaptive compression, application quality of service, and data de-duplication, reducing complexity in your data center. For more information on the BIG-IP WAN Optimization Module, see ***www.f5.com/products/big-ip/product-modules/wan-optimization-module.html***.

Using these technologies from F5 and Oracle together can provide enterprise class database replication services for mission critical information.

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this implementation

- You must have two BIG-IP LTMs that are running on one of the following platforms: 3600, 3900, 6900, 8900, or 11000. One BIG-IP LTM will be used for each end of the WAN network you wish to use for WAN Optimization.
- You must be running BIG-IP TMOS version 10.2 or later (with the same version running on each unit), and the WOM license enabled on both devices.
- You must have administrative access to both the Web management and SSH command line interfaces on the BIG-IP system.
- You must have administrative / sysdba level access to the Oracle database servers where database services are running to be able to edit and control those services.
- You must have administrative access to the host OS of the database servers, for modifying the TCP send and receive buffers settings and host IP routing table.
- You must have an existing routed IP network between the two locations where the BIG-IP LTMs will be installed.
- If there are firewalls, you must have TCP port 443 open in both directions. TCP port 22 for SSH access to the command line interface is also needed for configuration verification, but not for actual BIG-IP WOM traffic.
- For more configuration options on the BIG-IP WAN Optimization Module, see the Configuration Guide for BIG-IP WAN Optimization Module, available on ***Ask F5***.
- Before beginning the procedures in this guide, we recommend you back up your configuration. See *Appendix A: Backing up and restoring the BIG-IP system configuration*, on page 22.

Important

You will need to stop and restart both the Oracle Listener and Oracle database on the Primary and Standby servers, for the Oracle configuration changes to take effect. We recommend you schedule a database planned outage.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP WOM	v10.2
Oracle Data Guard	version 11R1 (also applies to R2)
Oracle GoldenGate	version 11R2

Document Version	Description
1.0	New guide
1.1	- Added support for GoldenGate. Added an Optimized Application specific to GoldenGate. - Changed the TCP WAN profile from optional to required.

Configuration example

In this guide, our example deployment contains two data centers, with a BIG-IP system located in each data center. The two Oracle database servers are also located in each data center. One instance of the database is running as the database Primary, and the other is running as the database remote standby. We show how to configure the BIG-IP WOM software to create an SSL secured iSession tunnel between the two BIG-IP systems, enable the TCP and compression features of WOM, and monitor the statistics as database replication traffic is passed from one data center to the other through the WOM tunnel.

Figure 1, on page 4 shows a diagram of the data centers, network, databases, and LTMs in our example. The Wide Area Network in our example is a DS3, 45mb/s link, with a Round Trip Time latency of 50 milliseconds.

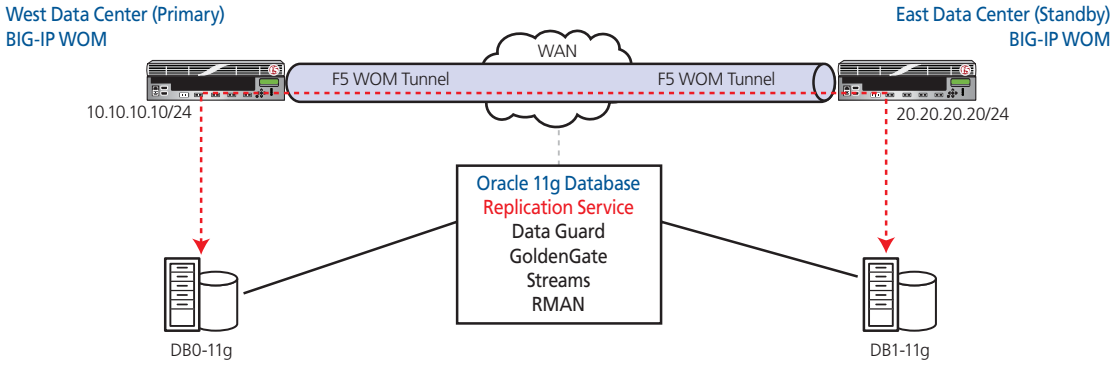

Figure 1 *Configuration example*

Preconfiguration network test

Before starting the configuration procedures in this guide, we recommend you log into each BIG-IP from the command line, and issue a *ping* from one unit to the other to verify IP connectivity and routing is operating as expected. The BIG-IP units must be able to contact each other across the network in order for the WOM module to work properly.

Configuring the BIG-IP WOM

Use the following procedures for configuring the BIG-IP WAN Optimization module.

Some of the procedures in this section (such as iSession profiles) are specific to the Oracle application, follow the procedure applicable to the application you are using.

Creating a new self IP address for the WOM tunnel endpoint

A new dedicated self IP is needed for the WOM tunnel endpoint on each BIG-IP system.

To add a new self IP for the WOM tunnel endpoint

1. On the Main tab, expand **Network**, and then click **Self IPs**.
2. Click the **Create** button.
3. In the **IP Address** box, type the appropriate IP address. In our example, we use **10.10.10.10**.
4. In the **Netmask** box, type the corresponding network mask. In our example, we type a mask of **255.255.255.0**.
5. From the **VLAN** list, select the appropriate VLAN. In our example, we select **VLAN West**.
6. From the **Port Lockdown** list, select **Allow None**.
7. Click **Finished**.

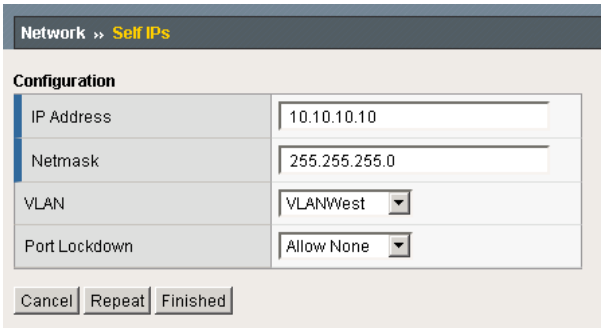

Figure 2 *Self IP configuration*

Creating the profiles

The next task to create the BIG-IP profiles. A ***profile*** is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

For the Oracle Database Replication configuration, we create two new profiles: one TCP profile, and an iSession profile. For more information on BIG-IP LTM profiles, see, the ***Configuration Guide for BIG-IP Local Traffic Management*** for version 10.2 (available on AskF5). Use this guide to manually configure the optimization settings.

Creating the TCP WAN Profile

◆ Note

This TCP profile, with the changes in steps 6 and 7, is required for both Data Guard and GoldenGate software running through the BIG-IP WOM. Streams and RMAN should use the default wom-tcp-wan-optimized profile with no changes.

The TCP WAN Profile is used to configure the TCP parameters for the WOM tunnel, and can be tuned to your particular network. In our example, we use the WOM TCP WAN parent profile with two modifications.

To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **tcp-wan-dataguard**.
5. From the **Parent Profile** list, select **wom-tcp-wan-optimized**.
6. *For Data Guard and GoldenGate only:* From the **Nagle's Algorithm** row, click the **Custom** box, and then click to clear the *Enabled* check box, which disables Nagle's Algorithm.
7. *For Data Guard and GoldenGate only:* From the **Congestion Metric Cache** row, click the **Custom** box, and then click to clear the *Enabled* check box, which disables the Congestion Metrics Cache.
8. Leave the other settings at their defaults.
9. Click the **Finished** button (see Figure 3, on page 7).

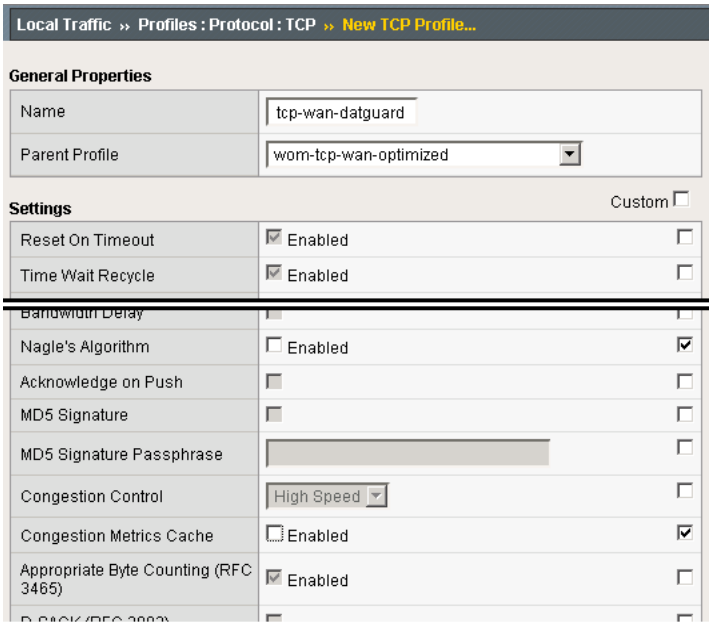

Figure 3 *General properties of the TCP profile (condensed)*

Creating the iSession Profile

The iSession Profile is used to configure the security, compression, and de-duplication parameters for the WOM tunnel.

The iSession profile configuration depends on which Oracle application you are using. Follow the procedure applicable for your application.

Creating the iSession profile for Streams and RMAN

Use the following procedure for the Streams or RMAN iSession profile.

To create the iSession profile

1. On the Main tab, expand Local Traffic, and then click Profiles
2. On the Menu bar, from the **Services** menu, click **iSession**.
3. Click the **Create** button.
4. In the **Name** box, give the profile a name. We recommend using the prefix *isession-* followed by the Oracle product, such as **isession-streams** or **isession-RMAN**.
5. Leave all of the other settings at the defaults.
6. Click the **Finished** button.

Creating the iSession profile for Data Guard

Use the following procedure for the Data Guard profile.

To create the iSession profile

1. On the Main tab, expand Local Traffic, and then click Profiles
2. On the Menu bar, from the **Services** menu, click **iSession**.
3. Click the **Create** button.
4. In the **Name** box, give the profile a name. We recommend using the prefix *isession-* followed by the Oracle product, such as **isession-dataguard**.
5. From the **Deduplication** row, click the **Custom** box, and then select **Disabled** from the list.
6. Leave all of the other settings at the defaults.
7. Click the **Finished** button.

Creating the iSession profile for GoldenGate

GoldenGate requires two iSession profiles: one for manager, and one for pump.

To create the iSession profile for manager

1. On the Main tab, expand Local Traffic, and then click Profiles
2. On the Menu bar, from the **Services** menu, click **iSession**.
3. Click the **Create** button.
4. In the **Name** box, give the profile a name. We recommend using the prefix *isession-* followed by the Oracle product, such as **isession-goldengate-manager**.
5. In the Compression Settings section, click the **Custom** boxes for **Deduplication**, **Adaptive**, **Deflate** and **LZO**. From the lists, select **Disabled**.
6. Leave all of the other settings at the defaults.
7. Click the **Finished** button.

To create the iSession profile for pump

1. On the Main tab, expand Local Traffic, and then click Profiles
2. On the Menu bar, from the **Services** menu, click **iSession**.
3. Click the **Create** button.
4. In the **Name** box, give the profile a name. We recommend using the prefix *isession-* followed by the Oracle product, such as **isession-goldengate-pump**.

5. From the **Deduplication** row, click the **Custom** box, and then select **Disabled** from the list.
6. Leave all of the other settings at the defaults.
7. Click the **Finished** button.

Run the WOM Quick Start Wizard

The WOM Quick Start Wizard is used to configure the initial parameters.

To run the WOM Quick Start Wizard

1. On the Main tab, expand **WAN Optimization**, and then click **Quick Start**.
2. In the **WAN Self IP Address** box, type the IP address you created in *Creating a new self IP address for the WOM tunnel endpoint*, on page 1-5. In our example, we type **10.10.10.10**.
3. Leave the **Discovery** list set to **Enabled**.
4. In the Select VLANs section, from the **LAN VLANs** row, select the VLAN for the Self IP you created, and click the Add (<<) button to move it **Selected** box.
5. From the **WAN VLANs** row, select the VLAN for the Self IP you created, and click the Add (<<) button to move it **Selected** box.
6. Leave **Outbound iSession to WAN** set to **serverssl**.
7. Leave **Inbound iSession from WAN** set to **wom-default-clientssl**.
8. Leave **Application Data Encryption** set to **Disabled** (see Figure 4, on page 10).
9. In the **Create Optimized Applications** section, do NOT check any applications. We create the application later in this guide.
10. ***Important:*** Click the **Apply** button at this step. If you do not, the WOM tunnel will not be set up properly.

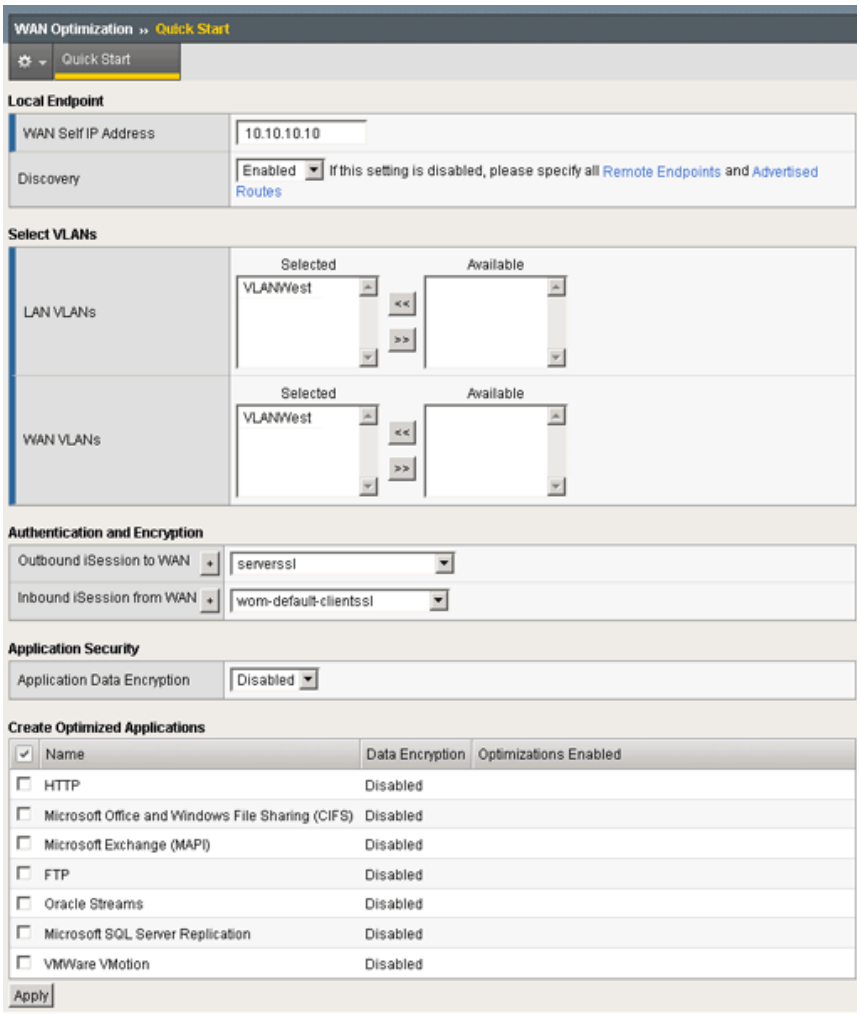

***Figure 4** BIG-IP WOM Quick Start*

Verifying the Local Endpoint

Check these setting as follows, to verify the Quick Start Wizard ran properly.

To configure the Local Endpoint

1. On the Main tab, expand **WAN Optimization**, and then click **Local Endpoint**.
2. In the WAN Self IP Address, you should see the address you entered in the Quick Start step. In our example, this is 10.10.10.10.
3. The **State** box should be checked **Enabled**.
4. The **Authentication and Encryption** box should be **serverssl**.

5. The **Tunnel Port** should be **443**.
6. The **Allow NAT** box should be checked **Enabled**.
7. The **SNAT** box should be set to **None**.

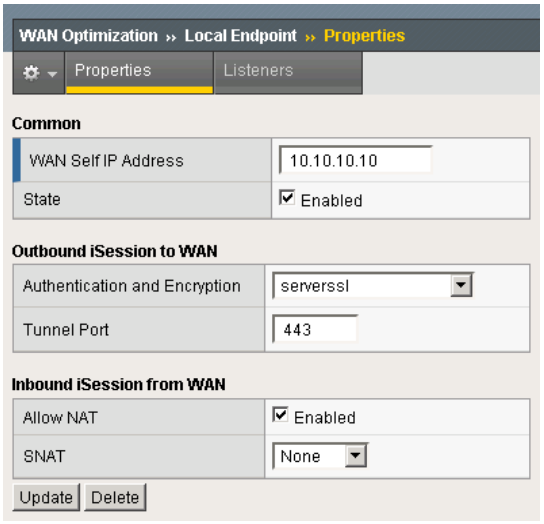

Figure 5 *Local Endpoint properties*

Configuring the Remote Endpoint

Next, we create the remote end of the WOM tunnel and point it to the BIG-IP in the other data center.

To configure the Remote Endpoint

1. On the Main tab, expand **WAN Optimization**, and then click **Remote Endpoints**.
2. Click the **Create** button.
3. In the **Remote Endpoint IP Address** box, type the address of the other BIG-IP's WAN Self-IP address. In our example, we type **20.20.20.20**.
4. Leave all the other settings at the defaults.
5. Click **Finished**.

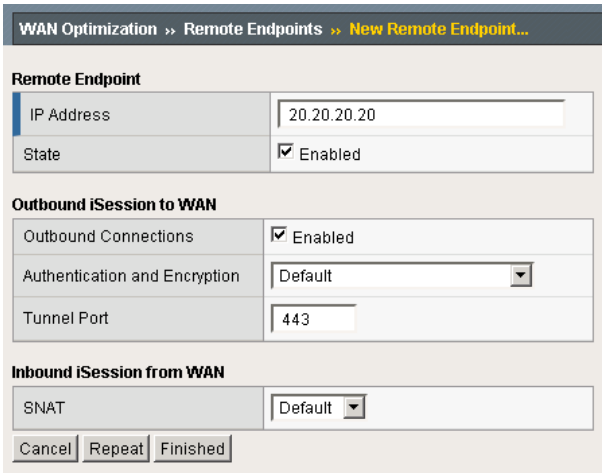

Figure 6 *Remote Endpoint configuration*

Advertise the local subnet

Next, the local IP subnets in each data center must be advertised across the tunnel. These are the subnets where the database servers are located. Each BIG-IP system needs to advertise the network for its directly connected database network. In our example, this is the 10.10.10.0/24 for the West BIG-IP network, and 20.20.20.0/24 for the East BIG-IP network.

To advertise the local subnet

1. On the Main tab, expand **WAN Optimization**, and then click **Advertised Routes**.
2. Click the **Create** button.
3. In the **Address** box, type the local subnet you want advertised. In our example, we type **10.10.10.0**.
4. In the **Netmask** box, type the mask. In our example, we type **255.255.255.0**.
5. In the **Label** box, give it a name. In our example, we type **West**.
6. Leave the **Mode** list set to **Included**.
7. Click **Finished**.

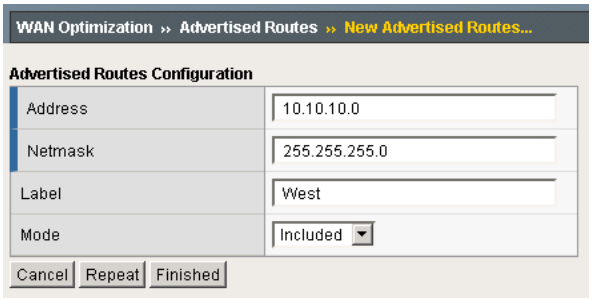

Figure 7 *Advertised Routes configuration*

Repeating all procedures for the BIG-IP WOM in the other data center

With the initial BIG-IP WOM system configuration complete, return to *Creating a new self IP address for the WOM tunnel endpoint*, on page 5 and repeat all of the procedures on the second BIG-IP in the other data center.

Verifying the WOM tunnel is ready

Once you have finished configuring the second BIG-IP WOM, use the following follow this procedure to ensure that the WOM tunnel endpoints are up and running properly.

Important

We strongly recommend that you complete this procedure, and verify that the WOM tunnel is operating properly before continuing with the rest of this guide.

For the procedure you will need SSH access to the BIG-IP.

To verify the WOM tunnel

1. Using an SSH client, like Putty, establish a connection to each BIG-IP.

2. After logging in, at the command prompt, type

   ```
   b endpoint remote show all
   ```

   You should see an output similar to the following:

```
b endpoint remote show all

ENDPOINT REMOTE 20.20.20.20
|   HOSTNAME bigip-west.oracle.com
|   MGMT ADDR 10.1.102.61   VERSION 10.2.0
```

```
|   UUID c1f3:68d6:f697:6834:108:5668:1e16:3fce
|   enable   STATE ready (incoming, outgoing)=(ready, ready)
|   BEHIND NAT disable
|   CONFIG STATUS "none"
|   DEDUP CACHE 62380   REFRESH (count) = (0)
|   ALLOW ROUTING enable
+-> ENDPOINT REMOTE 20.20.20.20 ROUTE 20.20.20.0/24
|   |   INCLUDE enable   LABEL West
```

3. SSH to the second BIG-IP and verify the tunnel status shows **ready/ready**.

Note

Only proceed with configuration after the status of the tunnel shows ready/ready.

Creating the Optimized Applications

The next task is to create an Optimized Application on the BIG-IP WOM.

This section contains two Optimized Applications, one for Streams, RMAN and Data Guard, and two for GoldenGate. Chose the one applicable for your configuration.

Create an Optimized Application for Streams, RMAN, and Data Guard

In this procedure, we create an application profile for Data Guard, and configure it to run across the tunnel.

To create an optimized application

1. On the Main tab, expand **WAN Optimization**, select **Optimized Applications**, and then click **Create Outbound**.
2. In the **Name** box, give it a name. In our example, we type **DataGuard-WOM**.
3. In the **Port** box, type **0** (zero).
4. Leave the **Enable LAN VLANs** at the defaults. In our example, the **West VLAN** is Selected.
5. From the iSession Profile list, select the appropriate iSession Profile you created in *Creating the iSession Profile*, on page 7. In our example, we select **isession-dataguard**.
6. Click **Finished**.

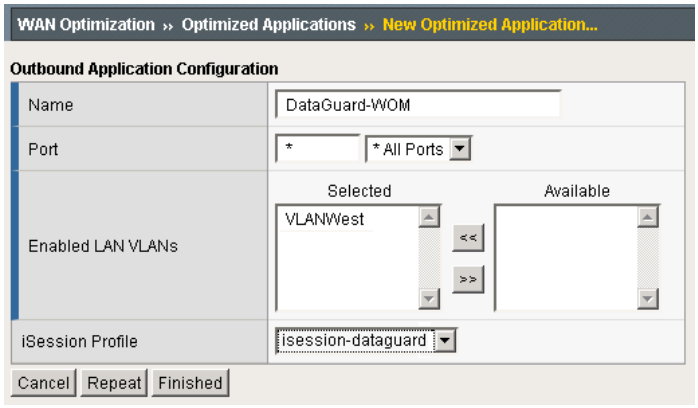

Figure 8 *Optimized Application configuration*

Create an Optimized Application for GoldenGate

In this procedure, we create two optimized applications for GoldenGate, one for pump and one for manager.

To create an optimized application for manager

1. On the Main tab, expand **WAN Optimization**, select **Optimized Applications**, and then click **Create Outbound**.
2. In the **Name** box, give it a name. In our example, we type **GoldenGate-manager-WOM**.
3. In the **Port** box, type **15000**.
4. Leave the Enable LAN VLANs at the defaults. In our example, the **West VLAN** is Selected.
5. From the iSession Profile list, select the iSession Profile you created in *To create the iSession profile for manager*, on page 8. In our example, we select **isession-goldengate-manager**.
6. Click **Finished**.

To create an optimized application for pump

1. On the Main tab, expand **WAN Optimization**, select **Optimized Applications**, and then click **Create Outbound**.
2. In the **Name** box, give it a name. In our example, we type **GoldenGate-pump-WOM**.
3. In the **Port** box, type **0** (zero).
4. Leave the Enable LAN VLANs at the defaults. In our example, the **West VLAN** is Selected.

5. From the iSession Profile list, select the iSession Profile you created in *To create the iSession profile for pump*, on page 8. In our example, we select **isession-goldengate-pump**.
6. Click **Finished**.

Modifying the Optimized Application

In this step, we change the destination network of the Optimized Application to point to the remote data center.

To modify the optimized application

1. On the Main tab, expand **WAN Optimization**, and then click **Optimized Applications**.
2. Click the application you created in the preceding procedure. In our example, we click the **DataGuard-WOM** link.
3. In the **Destination Address** box, type the destination subnet. In our example, we type **20.20.20.0**.
4. In the **Destination Mask** box, type the corresponding mask. In our example, we type **255.255.255.0**.
5. From the **Configuration** list, select **Advanced**.
6. Optional: If you created an optional TCP WAN optimized profile for Data Guard Synchronous Replication, from the **Protocol Profile (Server)** list, select the profile you created in *Creating the TCP WAN Profile*, on page 6. In our example, we select **tcp-wan-dataguard**.

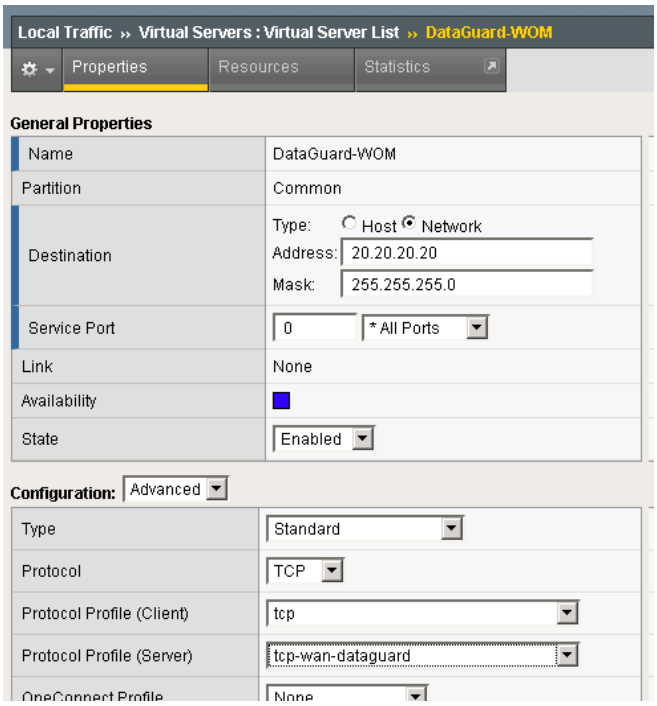

Figure 9 *Optimized Application modification (truncated)*

7. In the WAN Optimization section, from the **iSession Profile** list, make sure the profile you created in *Creating the iSession Profile*, on page 7 is selected. In our example, it is set to **isession-dataguard**.
8. Click **Update**.

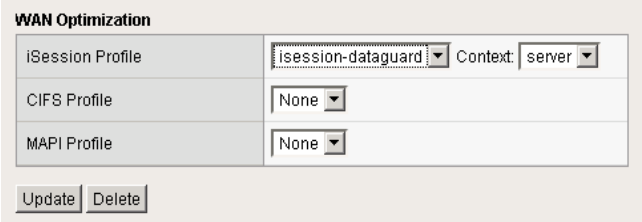

Figure 10 *Optimized Application modification complete*

Modifying the Oracle configuration

When running database applications across a Wide Area Network, it is important to configure the Oracle application TCP/IP stacks. For GoldenGate, this is performed in the GoldenGate parameters files. For Oracle Streams, RMAN, and Data Guard, the settings are stored in the SQLNET.ORA file.

Modifying the SQLNET.ora TCP settings for Streams, RMAN and Data Guard

The SQLNET.ORA file must be modified to change the TCP Send and Receive buffers in order to achieve optimal TCP/IP performance. There are two values that you need to know in order to calculate the TCP buffer values:

- *The WAN link speed between the Primary and Standby databases*
  Your network administrator should be able to provide this information.
- *The network latency between the Primary and Standby databases*
  We suggest using a Round Trip Time value taken from a series of PING packets done over 60 seconds, and then use the average millisecond value.

According to Oracle best practices, the optimal TCP socket buffer size is 3x (three times) the product of the link speed and latency value, expressed in bytes.

The value is calculated as follows:

```
Oracle Buffer Size = Link Speed * RTT / 8 * 3
```

Because of the BIG-IP WOM's acceleration technology, we take the Oracle Best Practice number and multiply it by 2.

So, we set the Oracle Net **RECV_BUF_SIZE** and **SEND_BUF_SIZE** parameters equal to this value. This will produce the largest increase in network throughput. Based on our network example (we have a T-3 45mb/s WAN link, with 50ms latency), the Oracle Best Practice value would be:

```
Oracle Buffer Size = 45,000,000 * .050 / 8 * 3 = 843,750
```

When using BIG-IP WOM, this value would be doubled:

```
Oracle Buffer Size with WOM = 843,750 * 2 = 1,687,500
```

So we modify the **SQLNET.ORA** file to add the following entries:

```
SEND_BUF_SIZE=1687500
RECV_BUF_SIZE=1687500
```

The following table includes examples of some common WAN networks.

Name	Link Speed	RTT (ms)	Bytes	3x BDP	WOM value
DS3/T3	45,000,000	50	281,250	843,750	1,687,500
100 mb/s	100,000,000	40	500,000	1,500,000	3,000,000
OC3	135,000,000	30	506,250	1,518,750	3,037,500

Calculate the value for your WAN network between the Primary and Standby servers, and record this value for future reference.

All of these TCP buffer calculations were based on the formulas above as an Oracle best practices, as documented in the Oracle whitepaper ***Data Guard Redo Transport & Network Best Practices***. The TCP/IP settings were changed on both the Primary and Standby database servers, this is also considered a best practice, in case there is a Data Guard role change.

Important

You must stop and re-start the Listeners and Database instances on both the Primary and Standby servers for these SQLNET.ORA tcp buffer changes to take effect. It is also important to know that increasing the TCP buffer settings will consume more memory on your database server. Each new TCP connection created by the database will use these new settings.

Modifying the GoldenGate parameters file TCP settings

For GoldenGate, all settings are stored in a parameters file. For example, a setting for setting up a remote host in GoldenGate would look something like:

```
rmthost 10.133.18.45, mgrport 15000
```

Which tells GoldenGate to:

- set up a Manager on port 150000 to the remote host
- use a GoldenGate default buffer size of 30KB
- flush the buffer at the default interval of 1 second.

Because of the BIG-IP WOM's acceleration technology, we are able to significantly increase the values from the default without encountering noticeable increases in the memory and CPU load of the GoldenGate servers. The resulting setting in the parameters file would be as follows:

```
rmthost 10.133.18.45, mgrport 15000, tcpbufsize 1000000, tcpflushbytes 1000000
```

Note

It is unnecessary to use GoldenGate's bundled compression and encryption, since both are built-in to BIG-IP WOM.

In our testing, we were able to set the TCP buffer and flush bytes size up to 2MB, but we found that the transfers were going so fast that the software stopped check-pointing until the end of the run. This is NOT RECOMMENDED, but may be a desired behavior in certain scenarios (an initial copy, for instance). Each deployment is different, so please test accordingly before putting into production.

Changing the host route to use the WOM tunnel

The next task is to log in with root level permissions to the database server's operation system, and change or add an IP route, to send the traffic to the local WOM Tunnel Endpoint.

Based on our example, the Primary database in the West data center, so we use the following command on the Primary:

```
Primary# route add -net 20.20.20.0/24 gw 10.10.10.10
```

And our standby database is in the East data center, so we use the following command on the standby:

```
Standby# route add -net 10.10.10.0/24 gw 20.20.20.20
```

Where 10.10.10.10 and 20.20.20.20 are the WOM Tunnel Endpoints.

Important

You need to stop and start the Listener and the Database to make the existing replication connection route properly over the WOM tunnel. It is important you do this on both the Primary and Standby databases.

Monitoring the deployment using the WOM dashboard

Using the WOM Dashboard, you can monitor the traffic flowing through the tunnel. To start the dashboard, on the Main tab, expand **WAN Optimization Module**, and then **Dashboard**. A new browser window will open.

In the top left, you see a summary of the bps traffic. The light blue is LAN traffic coming into the tunnel, the dark blue is WOM tunnel traffic after it has been Optimized.

In the lower left, you see the percentage of data that was able to be de-duplicated.

In the upper right, you see the percentage, Raw, and Optimized bytes that has passed through the tunnel.

In the lower right, you will see the Remote Endpoint configuration.

There are customization tools for the Dashboard, to configure the graphic display to suit your needs.

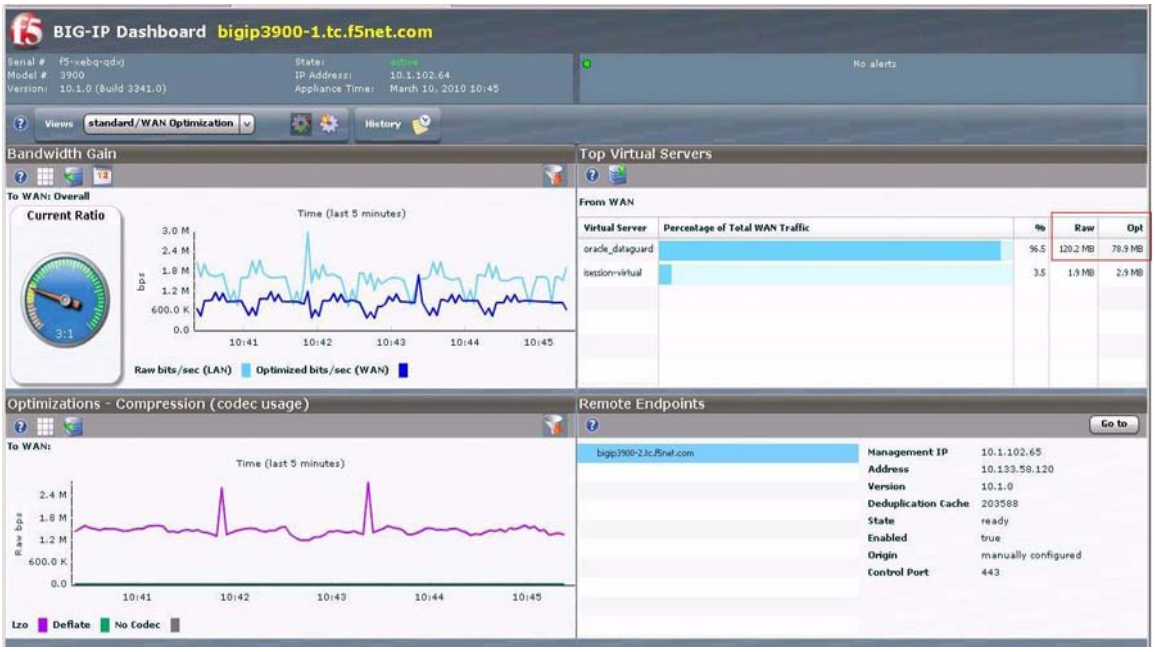

Figure 11 *BIG-IP Dashboard*

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration after you finish this configuration. When you save the BIG-IP configuration, it collects the following critical data and compresses it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving and restoring the BIG-IP configuration

The Configuration utility allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS).

To save the BIG-IP configuration using the Configuration utility

1. On the Main tab, expand **System**, and then click **Archive**.
2. Click the **Create** button.
3. In the **File Name** box, type a name for this archive file.
4. The other settings are optional.
5. Click the Finished button. The archive is created.

To restore a BIG-IP configuration

1. On the Main tab, expand **System**, and then click **Archive**.
2. Click the **Upload** button.
3. In the **File Name** box, type the file name, or click **Browse** to find it.
4. Click **Upload**.

References

F5 links

www.f5.com

www.f5.com/oracle

http://www.f5.com/products/big-ip/

http://www.f5.com/products/big-ip/product-modules/wan-optimization-module.html

Oracle links

www.oracle.com

http://www.oracle.com/us/products/database/index.html

http://www.oracle.com/technology/deploy/availability/htdocs/DataGuardOverview.html

http://www.oracle.com/technetwork/database/features/data-integration/index-094137.html

http://www.oracle.com/technetwork/database/features/availability/rman-overview-094650.html

http://www.oracle.com/technology/deploy/availability/pdf/MAA_WP_10gR2_DataGuardNetworkBestPractices.pdf