Tech Brief

Speeding Oracle Database Replication with F5 WAN Optimization Technologies

Efficient replication is vital to protect business data and maintain high network availability and responsiveness for users. By maximizing the resources of the Wide Area Network, F5 network optimization technologies can save time, reduce risks to mission-critical data, and accelerate the performance of Oracle Database Replication Services.

Chris Akker
Solution Architect, F5 Networks

Kollivakkam Raghavan
Senior Manager, Product Development, F5 Networks

Daniel Wright
Director, Product Management Engineering Solutions, F5 Networks

Contents

Introduction

Companies around the world recognize the importance of protecting business data from disaster, hardware failures, human error, or data corruption. Oracle provides a variety of strategic solutions to safeguard databases; manage backup, replication, and restoration; and ensure availability of mission-critical information. These Oracle 11*g* Database Replication Solutions include Oracle Data Guard, Oracle GoldenGate, Recovery Manager, and Oracle Streams.

- **Data Guard** is Oracle's management, monitoring, and automation software for creating and maintaining one or more standby databases that protect Oracle data while maintaining its high availability for applications and users.
- **GoldenGate** provides advanced replication services for best-in-class, real-time data integration and continuous data availability. By capturing updates of critical information as the changes occur, GoldenGate delivers continuous synchronization across heterogeneous environments.
- **Recovery Manager (RMAN)** is a fundamental component of every Oracle Database installation. Used to back up and restore databases, it also duplicates static production data as needed to instantiate a Data Guard standby database, create an initial GoldenGate replica, or clone databases for development and testing.
- **Streams** is a legacy replication product that Oracle continues to support, protecting customer investments in applications built using this technology with current and future versions of the Oracle database.

The Challenge of Efficient Replication

Since database replication requires the transmission of large amounts of data, the efficiency of Oracle Database Replication Services is often limited by the bandwidth, latency, and packet loss problems inherent in an organization's Wide Area Network (WAN). Whether databases are duplicated for business continuity and disaster recovery, compliance and reporting purposes, performance-enhancement strategies, or other business needs, the WAN handling all this data can become a bottleneck. Even with best-in-class replication solutions, WAN limitations can create delay nightmares and prevent administrators from meeting Recovery Point and Time Objectives (RPO/RTO). The effective capacity of the WAN simply may not be sufficient to replicate the volume of data in the time window needed. But upgrading bandwidth is very expensive, and the recurring costs can quickly consume IT budgets. Even if the network has enough bandwidth now, data loads only increase, and existing bandwidth must be used efficiently to maximize availability, postpone new investment, and prevent replication processes from impacting users.

Accelerating Replication With F5 WAN Optimization

Organizations using Oracle 11*g* Database Replication Services can solve WAN bandwidth challenges and manage costs with F5® BIG-IP® products, specifically BIG-IP® Local Traffic Manager™ (LTM) and BIG-IP® WAN Optimization Manager™ (WOM). BIG-IP LTM is an advanced Application Delivery Controller that helps to balance server utilization and improves administrators' ability to manage delivery of web applications and services. Using SSL acceleration, BIG-IP LTM creates a secure iSession™ tunnel between data centers and prioritizes traffic to provide LAN-like performance across the WAN.

Working in conjunction with BIG-IP LTM, BIG-IP WOM brings state-of-the-art networking to the Wide Area Network. BIG-IP WOM can optimize connections and accelerate Oracle database replication across the WAN, whether that replication takes place between data centers, to a disaster recovery site, or in the cloud. Together, BIG-IP LTM and BIG-IP WOM compress, deduplicate, and encrypt data while optimizing the underlying TCP connection using a variety of technologies:

- **TCP Express 2.0**—Built on the F5 TMOS® architecture, TCP Express™ 2.0 encompasses hundreds of TCP network improvements using both RFC-based and proprietary enhancements to the TCP/IP stack, which allow data to be moved more efficiently across the WAN. Advanced features such as adaptive congestion control, selective TCP window sizing, fast recovery algorithms, and other enhancements provide LAN-like performance characteristics across the WAN.
- **iSession secure tunnels**—The iSession tunnels created between two BIG-IP LTM devices can be protected with SSL encryption for the secure transport of sensitive data across any network.
- **Adaptive compression**—BIG-IP WOM can automatically select the best compression codec for given network conditions, CPU load, and different payload types.
- **Symmetric data deduplication**—Deduplication eliminates the transfer of redundant data to improve response times and throughput while using less bandwidth. BIG-IP WOM supports use of a deduplication cache from memory, disk, or both.

Deployed in pairs so compression, deduplication, and encryption can be reversed at the data's destination, BIG-IP WOM transmits more data while using less bandwidth and reducing susceptibility to latency and packet loss.

Working over a network optimized by BIG-IP WOM, Oracle's Data Guard, GoldenGate, Recovery Manager, and Streams solutions can run more efficiently while reducing network load and replication time. F5 BIG-IP platforms, including BIG-IP WOM, enable this efficiency by offloading CPU-intensive processes from the primary database server, performing network services like SSL encryption, data compression, deduplication, and TCP/IP network optimizations. This saves valuable computing power on the database server, freeing that resource for what it does best—processing the database needs of the organization. For the database administrator, this means increased availability for users with more easily achieved RPO/RTO targets for mission critical data—without spending money on expensive bandwidth upgrades.

Oracle and F5 technologies together provide a solid foundation for an Oracle database infrastructure, delivering greater data security and replication performance, faster recovery, increased network efficiency, and more dynamic data. As the cost of bandwidth and the need for data transmission increases, efficient network transport extends the capacity of the network to run timely applications while safeguarding data, enhancing administrator control, and prolonging the life of existing investments.

The benefits of combining Oracle Database Replication Services with F5 BIG-IP platforms are quantifiable. Tests across networks set to various parameters and for different Oracle products show replications completing up 33 times faster, for a performance improvement of up to 97 percent—and the "dirtier" the network, in terms of packet loss and latency, the more replication can be accelerated for huge leaps in performance. This technical brief outlines the test scenarios and results for extrapolation to real network situations. As the results show, the combination offers a solution for database administrators, network architects, and IT managers who are challenged to meet organizational needs for reliable and timely replication while controlling the costs of network enhancement.

Optimization Test Methodology

Proper testing of Oracle Database Replication Services with BIG-IP LTM and BIG-IP WOM required a test network with typical WAN link speeds, latency values, and packet loss. In addition, for the Data Guard tests, a test tool known as Swingbench generated a workload on the primary database server to provide the data for replication. Once the network was created and the primary database loaded, replication tests were conducted using each of the four Oracle replication services described above.

The results are representative only for a sample application on a test harness, using cases that were created in an engineering test facility. While every effort was made to ensure consistent and reproducible results, testing on production systems was outside the scope of this work.

Test Network Architecture and Configuration

The network was created with:

- One LANforge 500 WAN simulation appliance
- One primary and one standby Oracle 11*g*R1 Database Server as standalone devices. (Real Application Cluster [RAC]-enabled databases were beyond the scope of these tests.)
- Two F5 BIG-IP Model 3900 LTM devices, each running BIG-IP Version 10.2 RTM-build software and licensed to enable BIG-IP WOM. Two network scenarios were tested, one using only the iSessions tunnel and one using full BIG-IP WOM functionality.

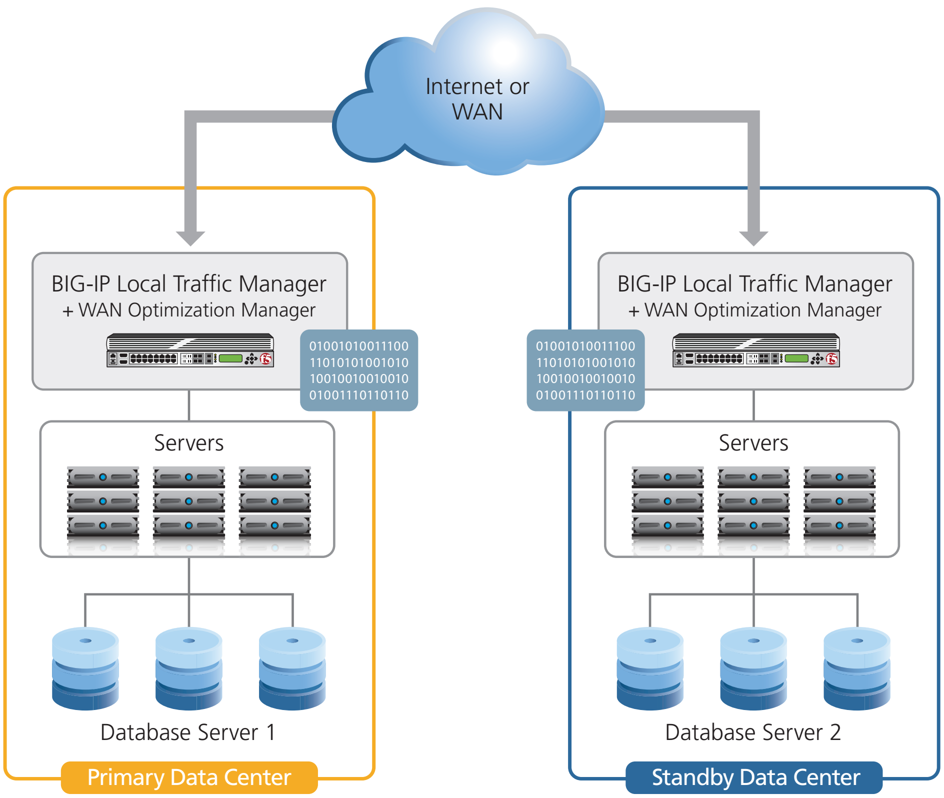


Figure 1: Oracle database replication with BIG-IP WOM

The Oracle Database Servers were configured as follows:

Hostname	Software	Hardware	OS	DB Role
Database Server 1	Oracle 11*g*R1	VMs	Oracle Ent Linux	Primary
Database Server 2	Oracle 11*g*R1	VMs	Oracle Ent Linux	Standby

The LANforge 500 WAN simulation device was configured as follows:

Bandwidth Network Link	RTT Delay	Packet Loss
45 Mb/s	100 ms (50 ms each direction)	0.5% (0.25% each direction)

Oracle Net Configuration

The tests also required setting the Oracle Net TCP/IP stack, also commonly called SQL.NET, for each TCP profile tested. Specifically, this configuration involved entering values for the size of the receive buffer, the send buffer, and the Session Data Unit (SDU). The SDU value used was 32767. All other TCP profile calculations were based on Oracle Best Practices documented in the Oracle white paper "Data Guard Redo Transport & Network Best Practices." The TCP/IP settings were changed on both the primary and standby database servers, which is also a best practice.

Buffer size settings require calculation of the Bandwidth Delay Product (BDP), which determines buffer sizes for optimal TCP/IP performance. For the largest increase in network throughput compared to the results with default settings, Oracle best practices previously identified the optimal socket buffer as three times BDP. For the Oracle Database 11*g*, the best practice has been updated to set the socket buffer at three times BDP or 10 Mbytes, whichever is larger (In the test scenarios, the calculated BDP was always the larger value.)

```
TCP BuffSize = 3 * BDP
```

Testing showed that when using BIG-IP WOM, the TCP buffer settings could be increased even further. Doubling the Oracle best-practice value—that is, using a value of 6 * BDP—sustained higher levels of throughput.

Finding BDP requires the bandwidth of the link, also known as link speed, and the network Round Trip Time (RTT)—the time required for a packet to travel from the primary database to the standby database and back, in milliseconds (ms).

```
BDP = Link Speed * RTT
```

The round trip time was determined from a series of PING packets done over 60 seconds and averaged for a millisecond value of 100 ms (as noted in the network configuration information above).

```
TCP BuffSize = (Link Speed * RTT / 8 bits) * 3
```

Or for higher throughput, as shown through the tests:

```
TCP BuffSize = (Link Speed * RTT / 8) * 6
```

Therefore the **`sqlnet.ora`** file for our test harness initially was configured with a default SDU size of 32767 and buffer values as shown in the following table for a variety of TCP/IP profiles, which were selected to establish baselines and to reflect differing BIG-IP WOM configurations. In each case, both the listeners and the databases were stopped and restarted after reconfiguration to allow the new settings to take effect.

Profile	Link Speed	Latency	BDP Bytes	Oracle Buffer Setting	BIG-IP WOM TCP Buffer Setting
LAN-GigE-BDP	1,000,000,000	0.0002	25,000	75,000	150,000
Oracle Tuned-BDP	45,000,000	0.1000	562,500	1,687,500	3,375,000
BIG-IP-WOM-2xBDP	90,000,000	0.1000	1,125,000	3,375,000	6,750,000

Swingbench Test Tool Configuration

As part of testing, the Swingbench database load generation tool created a workload on the primary database server, which caused the Data Guard process to send database redo records from the primary to the standby instances of the database. The test used Swingbench software version 2.3.0.422, and the primary database was populated using the Swingbench schema. Since the purpose of this testing was to determine performance using Data Guard synchronous mode, the Swingbench tool was configured for the worst case scenario—the maximum possible number of database record changes. The test profile made heavy use of the tool's "new order process" functions, which are designed to insert a maximum number of records into the order entry table. This created a large number of database transactions, which generated redo records that Data Guard had to replicate to the standby database.

Swingbench configuration required changing only a few parameters from their defaults. Final parameters included:

Parameter	Value
Number of Users	10
MinDelay	10
MaxDelay	20

To make the database create more log records, the Transaction Parameters were changed as follows:

Transaction Parameter	Value
NewCustomerProcess	False
BrowseProducts	False
NewOrderProcess	True
ProcessOrders	False
BrowseAndUpdateOrders	False

Oracle Data Guard Configuration

The Data Guard replication test exclusively used the product's "Zero Data Loss using Maximum Availability" protection mode and synchronous redo transport. Data Guard is the only Oracle replication technology that can guarantee zero data loss protection, and the Zero Data Loss mode (also known as the synchronous mode) was designed to ensure that any database changes—insert, delete, modify, commit transactions, DDL operations, etc.—are safely written to both the primary and standby databases before commit acknowledgements are returned to the application. Data Guard achieves this by synchronously transmitting database redo records (the information used to recover any Oracle database transaction) directly from the primary database log buffer to the standby database, where the change is applied. (See the figure below.) As network latency increases the round trip time (RTT) between the primary and standby servers, however, the acknowledgement response time from the Standby Redo Log Writer will also increase. This will increase the response time and reduce the throughput of any application or client connected to the primary database.

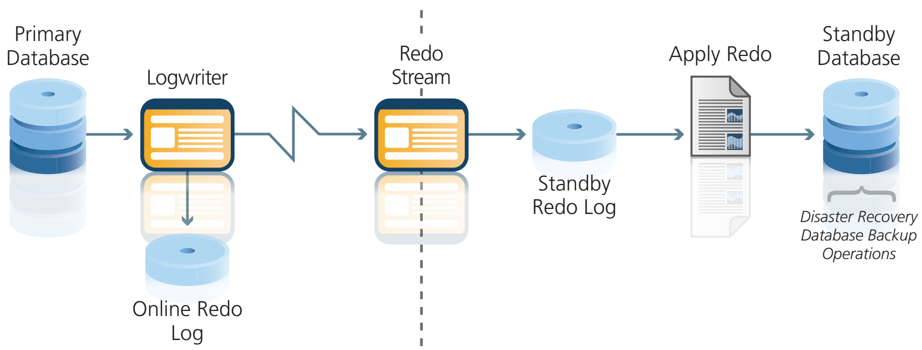


Figure 2: Typical Data Guard configuration

In most cases, an RTT of longer than 20 milliseconds between the primary and secondary databases is considered too excessive to deploy Data Guard in Zero Data Loss mode. When network latency is greater than 20 ms, most deployments must use the asynchronous mode, which is called Maximum Performance Mode. Replication tests using the F5 BIG-IP platform with asynchronous mode were not included in the testing described in this brief.

The goal of the Zero Data Loss mode test, however, was to determine if BIG-IP WAN Optimization Manager could provide sufficient network improvement for the synchronous mode to be used despite a network RTT longer than 20 ms. The test involved three cases with RTTs of 20 ms, 40 ms, and 100 ms, respectively. The 20 ms case represented the upper limit of expected RTTs on a metropolitan or regional network. The 40 ms case represented a short-haul WAN, and the 100 ms case represented a long-haul WAN, since 100 ms is a practical RTT for data center-to-data center replication using standard WAN transports. The larger RTT value is also five times the current tolerance level for Data Guard synchronous mode. Finally, it represents a realistic WAN RTT for replication from coast to coast across the U.S., from the U.S. to Europe, or from the U.S. to APAC using commercially available WAN carrier services.

In addition to the three test cases outlined above, replication was performed with the standby server connected via a local LAN under 0 ms RTT conditions to provide a baseline for Data Guard replication.

Oracle GoldenGate Configuration

The GoldenGate test measured the time required to move data from a GoldenGate source, populated with Swingbench data, to a target database. The objective was to determine how much BIG-IP LTM and BIG-IP WOM could speed up the "datapump" process of extracting data from the trail files and sending it over the network to the collector. The process would be tested multiple times using the same source data and the replication tools built into GoldenGate. The GoldenGate parameters were tuned for maximum network throughput on the test harness shown below.

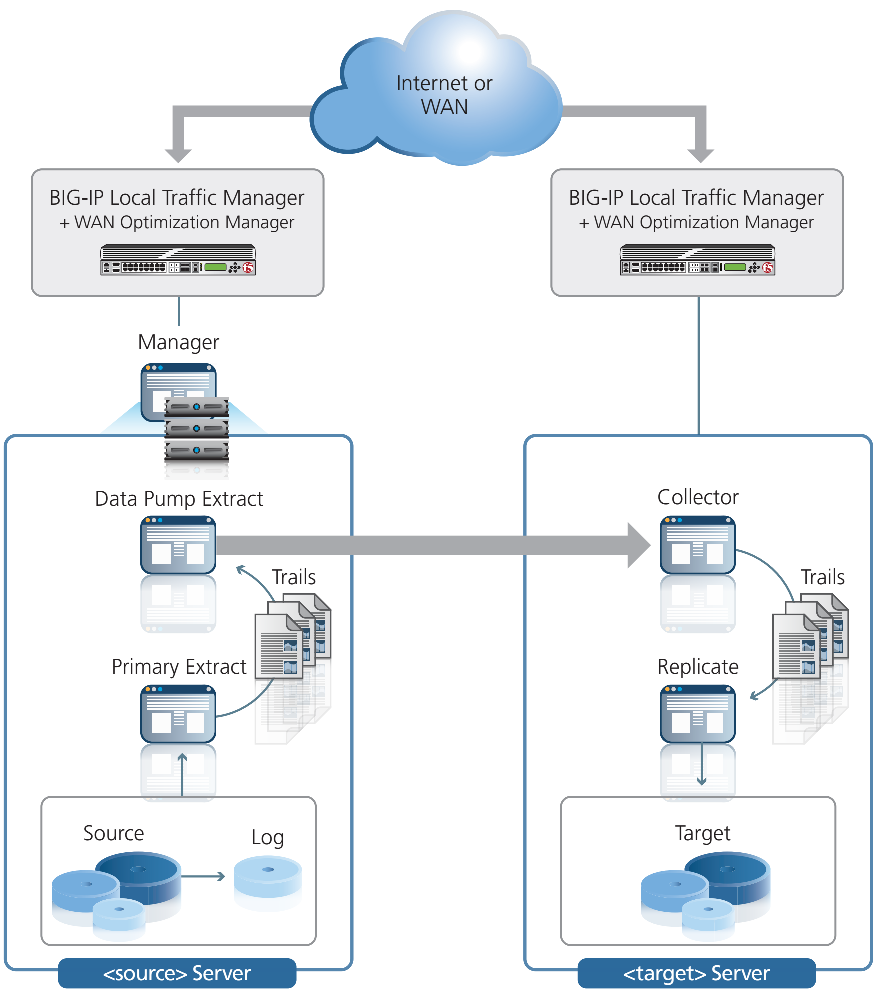


Figure 3: GoldenGate with BIG-IP WOM

Oracle Recovery Manager Configuration

This test identified the time required to instantiate a duplicate database across the WAN, creating a new Data Guard standby database while the primary was running. The test used a default installation of an empty Oracle 11*g*R1 Enterprise Edition database server of about 2.3 GB in size. Two scenarios were developed, one with the primary database connected directly to the standby target over the WAN, and a second case with the primary database connected to the standby target through the BIG-IP WOM iSessions tunnel. Both cases used a T3 45 Mb/s network with 100 ms RTT and no packet loss. This scenario is roughly the equivalent of a coast-to-coast WAN network in the United States.

The tests duplicated the database using the "RMAN Duplicate Database as Standby" script, which represents an Oracle best practice.

RMAN script example:

```
connect target /;

connect auxillary sys/oracle1@STANDBY_dgmgrl;

duplicate target database for standby from active
database

spfile

set db_unique_name='standby'

set control_files='/u01/app/oracle/oradata/standby/
control01.dbf'

set instance_number='1'

set audit_file_dest='/u01/app/oracle/admin/standby/
adump'

set remote_listener='LISTENERS STANDBY'

nofilenamecheck;
```

Oracle Streams Configuration

The Oracle Streams replication testing provided a "gap resolution test" that examined the time required for the standby target database to catch up with and synchronize to the source. The larger the gap and the longer the catch-up time, the more that data on the source database is exposed to the risk of loss.

This test explored scenarios based on two different LANforge WAN settings for the test network. One case simulated a T3 45 Mb/s WAN link with 100 ms RTT and packet losses of 1 percent, 0.5 percent, and 0 percent. The second case used a 135 Mb/s OC3 WAN link with 40 ms RTT and 1 percent packet loss.

Test data was provided by the TPC-E benchmark tool, which simulates the transactions of a financial trading company. First, the TPC-E schema was created on both the source and target database servers. Then Oracle Streams was configured to enable unidirectional replication from the source to the remote target database using Oracle stored procedures. Once the Capture, Propagate and Apply processes were successfully started on the test harness, the capture process was stopped on the source database server and the TPC-E tool populated the source database. The time required for the replication would be captured in the alert log files.

Test Results

After the tests, the results for each replication service and scenario were collected, calculated as needed, and charted. In every scenario and using every Oracle replication service, BIG-IP WOM optimization significantly improved replication speed, usually by many times over.

Results Using Oracle Data Guard

After the Data Guard tests, the results files from the Swingbench load generator machines were analyzed to determine the Average Response Time and, for the 100 ms case, the Transactions Per Minute. These results demonstrated that even when Data Guard was running on a WAN with high latency and packet loss, the combination of BIG-IP LTM and BIG-IP WOM could provide LAN-like response times while securely transporting the data within the encrypted iSession tunnel.

Replication performance over the networks with 0 ms and 20 ms latency was almost the same, with or without BIG-IP WOM optimization. As the latency and packet loss rates increased in the 40 ms and 100 ms latency cases, however, the performance improvement due to BIG-IP WOM was substantial. The F5 technologies were able to overcome the inefficiencies and provide greater performance and throughput than Data Guard alone, effectively increasing the latency tolerance of the network. *The higher the latency and packet loss, the more benefit the F5 WAN Optimization technology provided. Note that BIG-IP WOM improved performance at 40 ms latency to the levels of 20ms latency without BIG-IP WOM. This effectively increases the amount of latency the network can tolerate while still performing its tasks.*

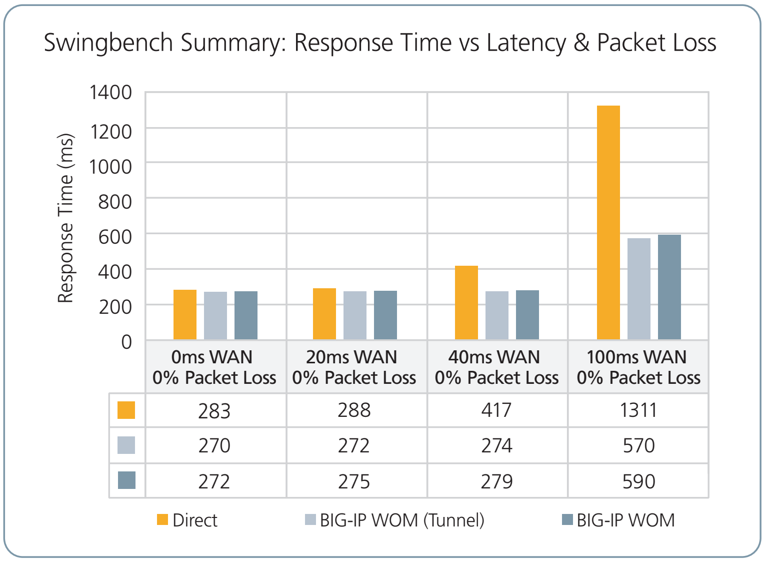


Figure 4: Data Guard replication with and without BIG-IP WOM

The BIG-IP WOM dashboard tracks data compression. During the Data Guard synchronous mode tests, the raw bytes from the Virtual Server called “oracle_Data Guard” were approximately 120 MB, with the optimized bytes reduced with the LZO codec to approximately 79 MB, nearly a 35 percent reduction. (Refer to the red square in upper right corner of the Figure5.) Consequently, the Bandwidth Gain metric in the upper left of the dashboard window shows approximately a 3:1 ratio.

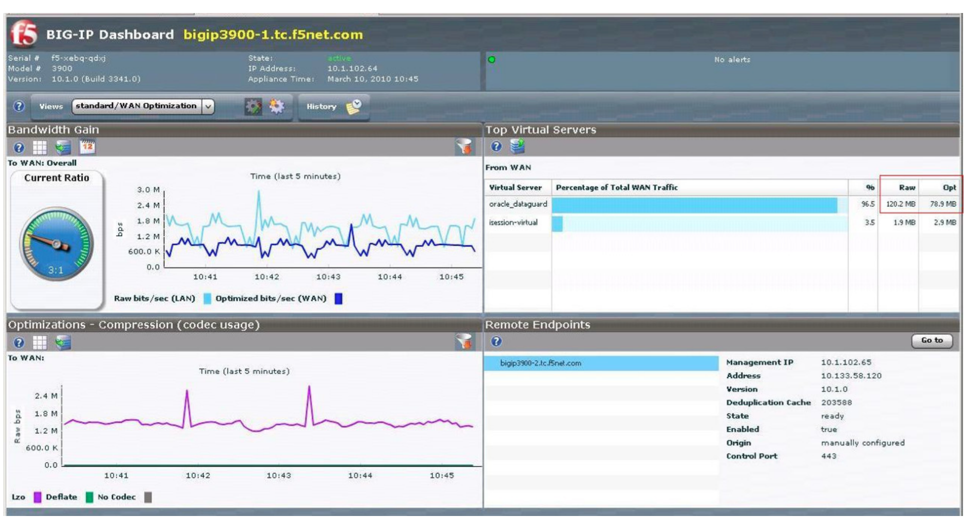


Figure 5: Compression tracking on the BIG-IP WOM dashboard

Results Using Oracle GoldenGate

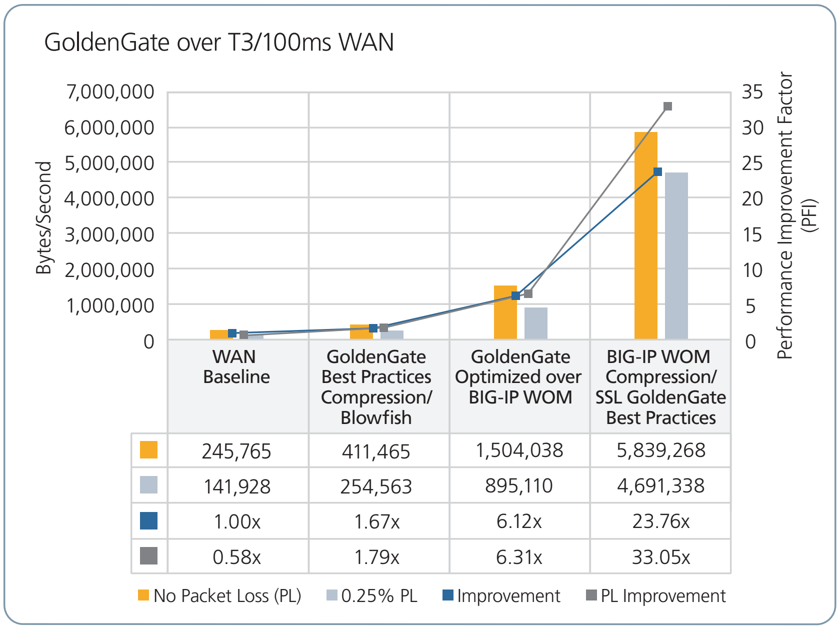
The GoldenGate datapump process was tested multiple times, using the same source data. The series included tests with compression, encryption, or both enabled. Baseline tests used the built-in GoldenGate zlib compression and Blowfish encryption. Tests involving the BIG-IP LTM and BIG-IP WOM optimization used LZO compression, SSL encryption, or both.

During the tests, the software displayed how much data had been sent and how long it took. Results in bytes per second were calculated from the average results of three 10-minute and three 15-minute test passes.

The performance improvement simply from tuning the GoldenGate software was minor, about 1.7 times faster than with the defaults. With the TCP optimizations, compression, and SSL encryption of the BIG-IP LTM and BIG-IP WOM products, however, replication took place over 23 times faster on a clean network and up to 33 times faster on a dirty network with significant packet loss.

BIG-IP platforms not only reduce the amount of data being transferred through compression and deduplication. Improving network performance with TCP optimization and offloading SSL encryption also allowed the database to send more data across the connection. One effect of this benefit is that CPU utilization on database servers went up because they were able to send more data in the same amount of time.

By contrast, throughput in the baseline WAN network was hampered by packet loss, with tests showing a 40 percent reduction in throughput from retransmit requests.



	WAN Baseline	GoldenGate Best Practices Compression/ Blowfish	GoldenGate Optimized over BIG-IP WOM	BIG-IP WOM Compression/ SSL GoldenGate Best Practices
No Packet Loss (PL)	245,765	411,465	1,504,038	5,839,268
0.25% PL	141,928	254,563	895,110	4,691,338
Improvement	1.00x	1.67x	6.12x	23.76x
PL Improvement	0.58x	1.79x	6.31x	33.05x

Figure 6: GoldenGate replication with and without BIG-IP WOM

Results Using Oracle Recovery Manager

The Linux shell command "time" measured how long the RMAN script took to execute and instantiate the duplicate database for each network scenario. The baseline RMAN script took 13 minutes and 49 seconds. The RMAN script running over the network optimized by BIG-IP WOM took 4 minutes and 21 seconds—approximately 3.2 times faster. Since there was no packet loss introduced in either scenario, most of the improvement can be attributed to the compression and deduplication provided by BIG-IP WOM.

Because every database is unique, is impossible to predict how any given database will benefit from compression. Still, these RMAN tests represented the worst-case scenario, since the default installation of the 11*g*R1 database contains very little user data. With a production source database, optimization would most likely achieve even better results.

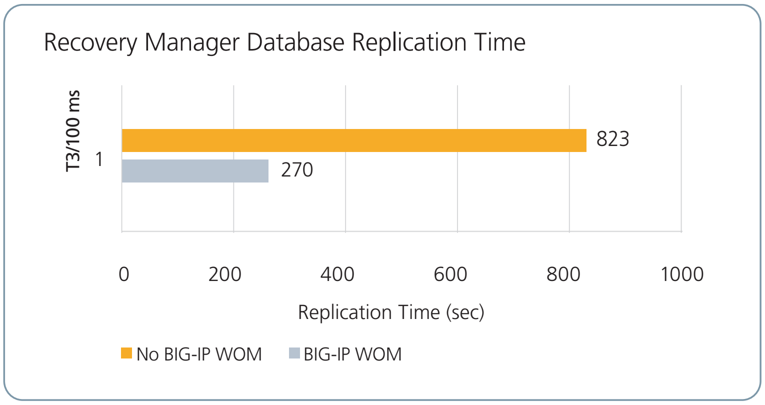
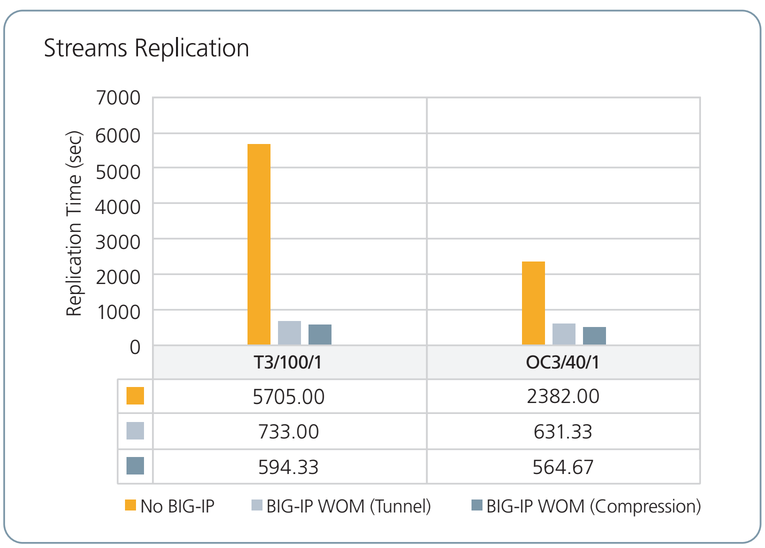


Figure 7: RMAN replication with and without BIG-IP WOM

Results Using Oracle Streams

Replication in the Oracle Streams test was verified by checking the contents of the TPC-E tables—about 2 GB of data—before and after replication. At both the T3 and OC3 link speeds, the BIG-IP WOM optimization significantly reduced the time required to replicate a day's worth of data from the source to the target database. In the T3 scenario, baseline replication took about 95 minutes, while replication over the BIG-IP platform took about 10 minutes—9.5 times faster. In the OC3 case, baseline replication took 40 minutes versus 9.4 minutes, which is a 75 percent reduction.



	T3/100/1	OC3/40/1
No BIG-IP	5705.00	2382.00
BIG-IP WOM (Tunnel)	733.00	631.33
BIG-IP WOM (Compression)	594.33	564.67

Figure 8: Streams replication with and without BIG-IP WOM

In addition, the off-host compression and TCP optimizations of BIG-IP WOM provided additional value by efficiently overcoming the detriments of packet loss. On the T-3 WAN at 40 ms RTT, packet loss rates were varied from 0 and 0.5 percent to 1 percent. As packet loss increased, so did the baseline gap resolution time (shown in orange). On the BIG-IP WOM platform, however, the gap resolution time (shown in gray) remained consistent, for a performance more than 9 times better than baseline when packet loss was at 1 percent. Even on a relatively clean network with minimal packet loss, the TCP/IP enhancements provided by BIG-IP WOM can increase throughput by as much as 50 percent, but the dirtier the network, the more BIG-IP WOM can streamline replication.

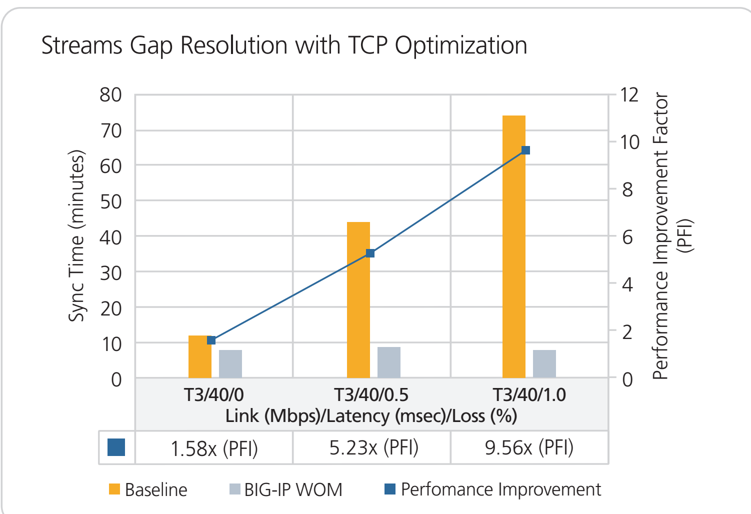


Figure 9: Streams gap resolution with and without BIG-IP WOM compression

BIG-IP WOM compression achieved even better results. Tests were performed on the same T3 45 Mb/s network with 40 ms RTT and 0.5% packet loss, first with BIG-IP WOM compression disabled and then with it enabled. As with TCP optimization, the compression helped resolve the replication gap faster. By compressing the data, BIG-IP WOM was in effect transmitting more data, sending the redo blocks faster.

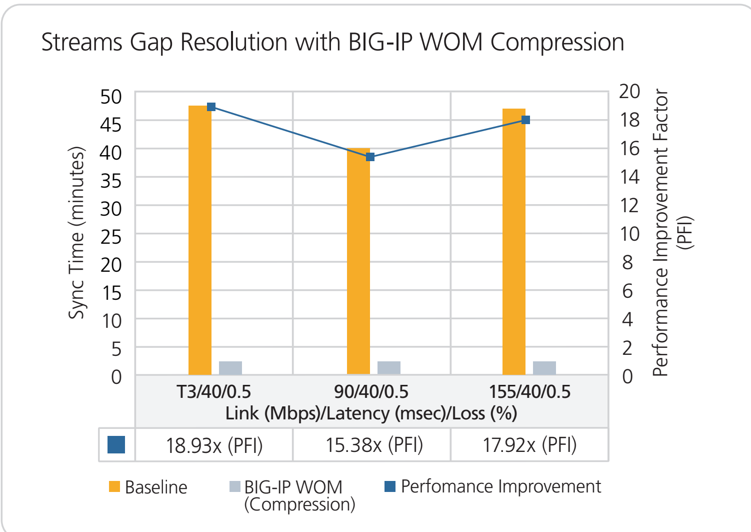


Figure 10: Streams gap resolution with and without BIG-IP WOM compression

The compression helped the target database remain consistently only a few minutes behind the source database. Without compression, it took at least 15 times longer for the gap to resolve. Overall, testing showed that the LZO algorithm provided the most consistent compression results for Oracle Database Replication Services.

Conclusion

Oracle Database Replication Services perform faster when they're run on an architecture that incorporates the optimization and acceleration provided by BIG-IP LTM and BIG-IP WOM. In tests using a variety of network configurations, BIG-IP WOM significantly improved the speed of replication, in some instances delivering performances that were 20 or 30 times faster.

Using Oracle Database Replication Services and F5 BIG-IP products together supports more efficient deployment and use of these database services over a WAN. The combination conserves resources, saves time, enables effective disaster recovery, and helps network and database administrators meet RPO/RTO objectives by providing off-host encryption, compression, deduplication, and network optimization. When replication takes place over less-than-ideal WAN networks, BIG-IP WOM helps minimize the effects of network latency and packet loss. Over time, the use of Oracle Database Replication Services with BIG-IP products can save money by eliminating or reducing the large expense of WAN upgrades while enabling timely replication to meet organizational needs.

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