the Availability Digest

www.availabilitydigest.com
@availabilitydig

Grocery Chain Achieves Continuous Availability with OmniReplicator

Yash Kapadia
CEO, Opsol Integrators Inc.
January 2015

A large, privately held grocery-store chain operates 300 supermarkets. It had been using a BASE24 financial-transaction switch from ACI on an HP NonStop server to route credit-card and debit-card payments from its point-of-sale (POS) terminals for authorization to the banks that issued the cards.[1]

Furthermore, its POS terminals provided additional customer services such as cell-phone topping, bank deposits, and bill payments. The chain's POS terminals were connected to the financial switch via in-store servers that provided this additional functionality.

The BASE24 financial-transaction switch ran on a single HP NonStop server. Should the switch fail, the grocery stores were limited to cash sales only and were basically out of business. Following ACI's announcement that it would no longer support BASE24 on HP NonStop servers, the grocery chain opted to move to the OmniPayments financial-transaction switch from Opsol Integrators Inc. Via its replication engine OmniReplicator, OmniPayments was able to provide an active/active system that guaranteed continuous availability for the chain's stores. This packaged solution saved the grocery chain a significant amount of money.

The Sunset

When ACI announced that it would no longer support BASE24 on the HP NonStop platform, the grocery chain was given an opportunity to review its approach to POS terminal support. The company decided on several additional features that it would like to have in a new system:

- It wanted to incorporate geographical redundancy so that it could implement a rapid failover response to a backup system in the event of a system outage. It wanted to avoid grocery store outages that occurred due to a financial-transaction switch outage.

- All communications between the grocery stores and its BASE24 financial-transaction switch were unencrypted. This is a violation of the PCI DSS (Payment Card Industry Data Security Standards) specifications. The chain wanted to be in compliance with PCI DSS.

- Additional customer services that the grocery chain wanted to offer via its POS terminals required modifications to the in-store servers. These modifications would have to be rolled out to all 300 in-store servers, a massive job.

[1] This article was originally published in the September/October 2014 issue of *The Connection*.

- The grocery chain wanted to be able to accept the new EMV (Europay, MasterCard, Visa) smart cards that prevent payment-card fraud via an embedded processor chip that offers encryption and risk management services.

After an evaluation of its various options, the grocery chain selected Opsol Integrator's OmniPayments financial-transaction authorization system that is resident on fault-tolerant HP NonStop servers. OmniPayments and its components met all of the chain's criteria. Continuous operation in its stores could be ensured by using OmniReplicator's bidirectional data-replication capabilities to architect an active/active switch. OmniCrypto supported PCI DSS-compliant in-flight and at-rest encryption. OmniPayments' Business Logic Modules could be easily implemented to supply the additional services provided by the in-store servers, thus eliminating the need for these servers. OmniPayments offered support for EMV POS terminals and the protocols used to communicate with the acquiring and issuing banks.

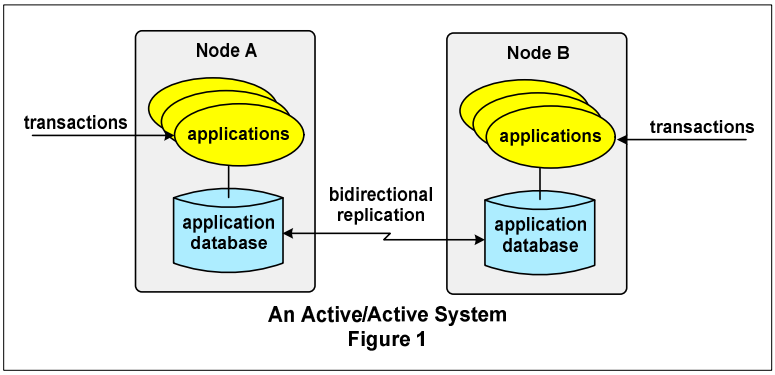
The OmniPayments Active/Active Financial Authorization System

The key immediate benefit that the grocery chain realized by moving to OmniPayments was achieving continuous availability for its store systems. The OmniPayments financial-transaction switch implements an optional active/active architecture via its OmniReplicator bidirectional data replication engine. With this architecture, two or more HP NonStop nodes share the processing load of the application.

The Active/Active Architecture

In order for an active/active architecture to be implemented, all of the nodes in the active/active application network need to have access to the application database. However, the nodes may be separated by thousands of miles for geographical redundancy. Performance issues preclude the use of a single database located at some central site with which all nodes can communicate. Furthermore, a common central database represents a single point of failure. As a result, continuous availability cannot be achieved with this approach. Each node needs its own local copy of the application database.

To address the challenge of a common, distributed application database, data replication is employed. As shown in Figure 1, two geographically distributed nodes each have its own copy of the application database. The databases are kept synchronized by bidirectional replication. Whenever an application makes a change to its local copy of the database, that change is replicated to the database of the other node. Thus, applications on both nodes see the same application state and will process transactions in the same way.



An Active/Active System
Figure 1

Consequently, a transaction can be sent to either node and be processed identically. Should a node fail, all that needs to be done is to route all transactions to the surviving node. Recovery time can be measured in seconds. In addition, failover faults are avoided (i.e., the surviving node does not come into service) because it is known that both nodes are functioning – they are both actively processing transactions.

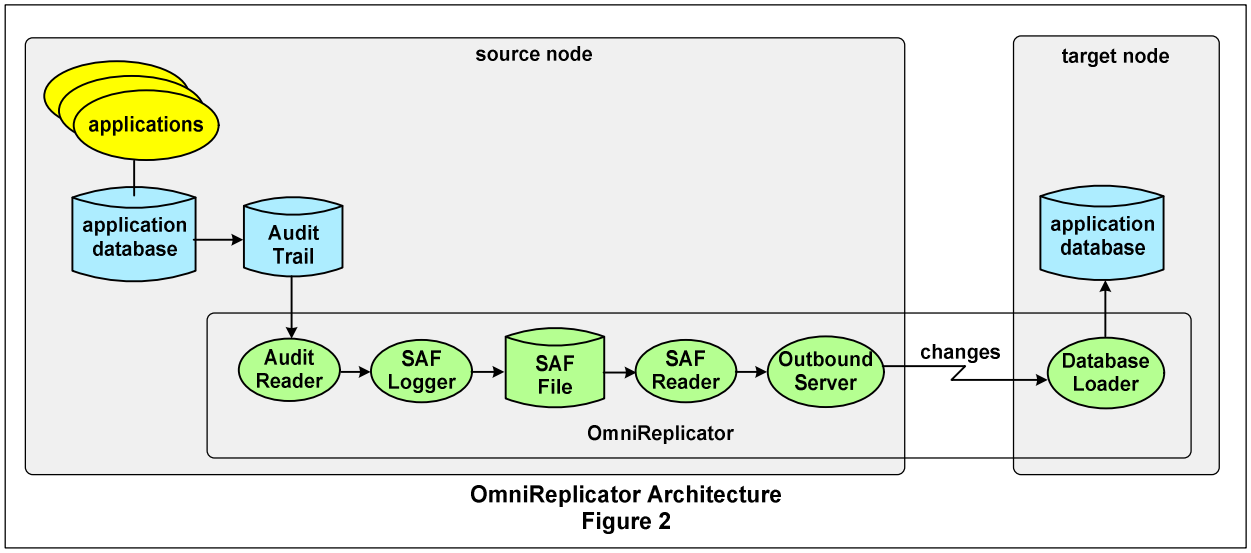
OmniReplicator Architecture

In the OmniPayments system, data replication is performed by the OmniReplicator. The architecture of the OmniReplicator is reflected in Figure 2, where the source node contains the database that is being updated by the application. The target node contains the database that is to be kept synchronized with the source database.

Within OmniReplicator, the Audit Reader process follows the NonStop Audit Trail logs. These are the logs that NonStop TMF maintains of all updates made to audited tables and files. The Audit Reader captures the application database changes as they are written to the Audit Trail and passes them to the SAF Logger process, which writes them to an intermediate SAF file. The purpose of the SAF file is to queue all database modifications in the event that the target system should fail. Upon recovery of the target system, changes that have occurred since its failure can be sent from the SAF file to the target database followed by the normal data-replication flow.

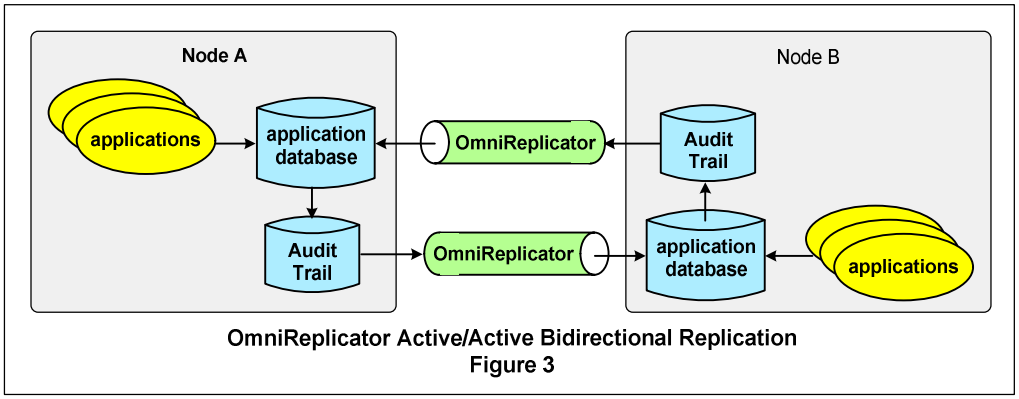
The SAF Reader reads changes from the SAF file and sends them to the Outbound Server. All of this activity takes place on the source node.

The Outbound server is tasked with sending the changes over a communication channel to the Database Loader on the target system, which then applies them to the target database.



OmniReplicator Architecture
Figure 2

Bidirectional Replication



OmniReplicator Active/Active Bidirectional Replication
Figure 3

In order to implement an active/active architecture, OmniReplicator is configured on each node to replicate changes made its node's database to the database on the other node, as shown in Figure 3. In this way, as application changes are made to either database, they are replicated to the other database. The two databases are therefore (nearly) kept in synchronism so that applications on either node can properly execute transactions sent to them.

Data Collisions

One problem with bidirectional replication is data collisions. A data collision occurs if an application on each node makes a change to the same row of the application database at substantially the same time. Each change will get replicated to the database on the other node and will overwrite the change made to the row in that database. Now the two databases are different, and each is wrong.

Many applications can be structured so that data collisions are avoided. As we shall see, the grocery chain was able to do this. However, if data collisions cannot be avoided, they must be detected and resolved to keep the databases properly synchronized.

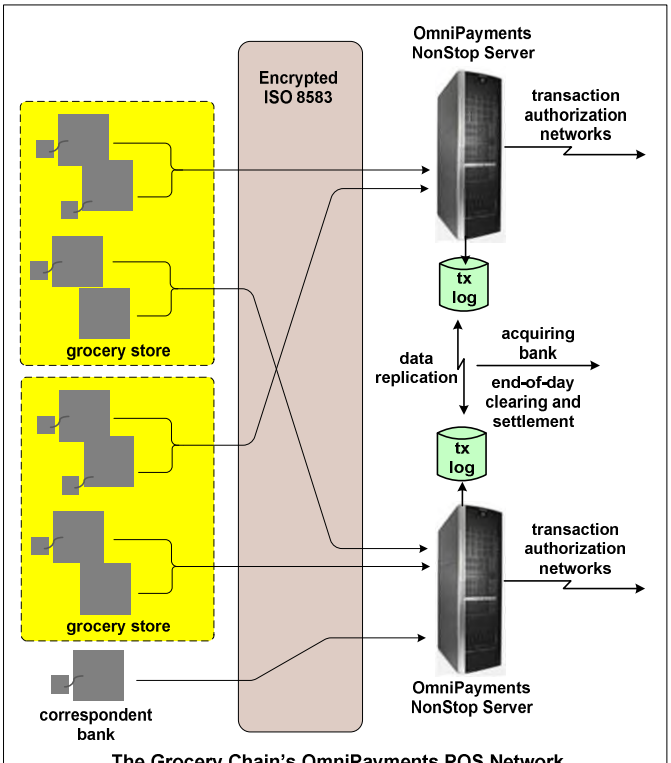
OmniPayments detects data collisions and automatically accepts the latest change.

The Use of Active/Active by the Grocery Chain

The grocery chain installed an active/active OmniPayments switch comprising two HP NonStop servers to manage its POS terminals. One server is located in the company's headquarters, and the other is located at a remote site 500 miles away.

POS Terminal Distribution

To split the load between the two NonStop servers, the POS terminals in each store are divided into two partitions, as shown in Figure 4. One set of POS terminals is connected to one of the HP NonStop servers in the active/active pair, and the other set is routed to the other NonStop server. The communication channels connecting the POS terminals to the NonStop servers use the standard ISO 8583 protocol utilized for transaction-switching networks. This in itself is an improvement over the earlier system, which incorporated the proprietary VISA 2 communication protocol.



The Grocery Chain's OmniPayments POS Network
Figure 4

Because communication between the POS terminals and the HP NonStop servers is encrypted and there are no in-store servers, the chain has no concern about being hacked and having data stolen, as happened to Target over the 2013 year-end holidays.

Since the POS terminals are split between the NonStop servers, should a NonStop server fail, half of the POS terminals in the store will still be operational. The failed terminals will auto-reconnect to the other HP NonStop server. Thus, the grocery stores can continue to serve their customers even in the presence of a NonStop server failure.

Transaction Authorization

As each payment-card transaction is processed by a POS terminal, it is sent to its HP NonStop server for preauthorization fraud checks.

The NonStop server sends the transaction over the appropriate transaction-switching network to the bank that issued the payment card. The issuing bank decides whether or not to authorize the transaction and returns an 'accept' or 'reject' response to the POS terminal.

Transaction Settlement Via OmniReplicator

Each server logs its own transaction activity. However, to ensure the durability of transactions in the event of a server failure, the transaction logs on each of the two servers are synchronized via OmniReplicator. Whenever a transaction is entered into the transaction log of one server, it is immediately replicated to the transaction log of the other server via OmniReplicator's bidirectional replication capability. Thus, each server has a record of all transactions made by both servers.

At the end of the day, either log may be used to send transaction information to the chain's acquiring bank for settlement and clearing. During this process, funds are transferred in settlement of the day's transactions from the issuing banks to the chain's account held by its acquiring bank.

Data Collisions

Data collisions in this active/active system are highly unlikely because there is only a very small probability that the same card will be used at two POS terminals simultaneously.

If a husband and wife should use their cards simultaneously to make purchases at two POS terminals connected to the same NonStop server, transaction locking will prevent data collisions. However, if they should use their cards simultaneously at POS terminals connected to different NonStop servers, there is still no problem. Each system will independently forward its transaction to the issuing bank, which will probably authorize both. Each system will then write the transaction to its log file. Each transaction will be replicated to the transaction log of the other system, and both transactions will be sent at the end of the day to the acquiring bank for settlement. The grocery chain will be reimbursed for each transaction.

Correspondent Banks

In addition to the supermarket stores, the new OmniPayments system also supports what is known as correspondent banks. In the country served by the grocery chain, small, rural villages often have no supermarkets, no banks, and, in some case, no Internet service. In many of these communities, the grocery chain has set up one or more local merchants with POS terminals. A merchant can then sell goods via credit cards and debit cards and can execute other transactions such as the cell-phone topping and banking services provided by the chain's grocery stores. These merchants are called *correspondent banks* because they extend banking services to the small villages.

The correspondent bank POS terminals are connected to the active/active NonStop servers just as are the in-store POS terminals so that their transactions can be authorized by the issuing banks.

OmniReplicator Management

The OmniReplicator replication channel is managed by OmniConsole, a component of OmniPayments. OmniConsole integrates all of the functions that are delivered by OmniPayments, such as replication-channel monitoring; selecting files for replication; starting, stopping and restarting OmniReplicator; defining master keys; sending encryption keys to POS terminals; and creating batch schedules for OmniScheduler. OmniConsole is a web service, so the management of OmniPayments can be undertaken from any location.

OmniConsole includes two major facilities necessary for system management – OmniOffender and OmniDash. OmniOffender is an interactive performance monitor for NonStop systems. It displays parameters such as NonStop server CPU time utilization, CPU resource usage, process utilization, disk utilization, and file activity.

OmniDash is a real-time dashboard. It displays many statistics, such as the total number and amount of purchases and other transactions for all POS terminals, the volume of usage for each POS terminal, the volume of transaction denials, and the status of each POS terminal. This information is vital to the chain's ability to manage its POS terminal network.

OmniScheduler is the OmniPayments component that schedules batch jobs. It performs similar functions to HP NonStop NetBatch. For instance, it is OmniScheduler that controls the end-of-day batch processing of the log files for settlement of transactions.

Other Benefits Achieved by the Grocery Chain

Achieving continuous availability via OmniReplicator is only one of the many benefits that the chain obtained by moving to OmniPayments.

Encryption

The new system now provides encryption for data in-flight and at-rest via OmniPayments' OmniCrypto facility. OmniCrypto supports POS transaction security, key management, Public Key Infrastructure (PKI), encryption, and tamper-proofing of database files. It manages passwords and credentials for user authentication and role-based Access Control Lists for user authorization.

With OmniCrypto in place, the grocery chain is now PCI DSS compliant.

Elimination of In-Store Servers

The 300 in-store servers are no longer needed in the grocery stores. All functions that had been carried out by these servers are now performed via the OmniPayments Business Logic Modules. These functions include cell-phone topping, customer bank account management, and bill payments.

POS Expanded Functions

The chain now can easily add functions to its POS terminals without having to roll out upgrades to 300 store servers. Rather, the functions are simply added to the OmniPayments switch.

One such new function is loyalty cards. As customers make purchases at the chain's grocery stores, points are added to their loyalty cards. The customer can use these points to purchase additional products at the chain's stores. Loyalty-card processing is one of the new functions to be supported by OmniPayments. OmniPayments will maintain loyalty-card balances in its database and will furnish loyalty credits to customers on demand. The loyalty balances will be replicated between the NonStop systems via OmniReplicator so that both systems will have access to customer loyalty accounts. Replication also will protect the loyalty account balances in the event of a NonStop server failure.

Smart Card Processing

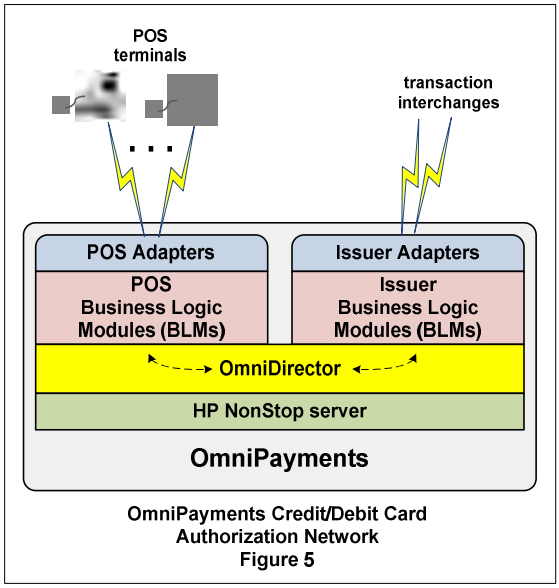
OmniPayments supports all aspects of EMV smart-card processing. EMV POS terminals are supported as are the communication protocols required to pass EMV transactions to the issuing banks and EMV settlement data to the chain's acquiring bank.

Reduced Licensing Costs

OmniPayments substantially reduced the grocery chain's licensing costs. This is because the OmniPayments license fee is based on the size of the NonStop systems rather than on the previous year's transaction volume, as is the case with many other financial transaction switches.

The OmniPayments Financial Transaction Switch

Opsol's OmniPayments financial-transaction switch is shown in Figure 5. The core layer of OmniPayments is Opsol's OmniDirector Enterprise Service Bus. OmniDirector services include data transformation, encryption, intelligent routing, and communication-failure recovery. It also implements adapters to support those protocols required to communicate with the chain's POS terminals as well as with the international financial switching networks.



OmniPayments Credit/Debit Card Authorization Network
Figure 5

Business logic modules, or BLMs, provide the business functions of OmniPayments. These functions include credit-card and debit-card authorization services. The BLMs are extensible to supply the other services that the chain offers or plans to offer its customers via its POS terminals.

OmniPayments supports complete logging of all transactions via its OmniLogger module. The logs contain the transaction information needed at the end of each day for clearing and settlement. It is this processing function that transfers funds from the card-issuing banks to the chain's merchant account held by its acquiring bank to reflect the day's sales activities.

Summary

The grocery chain was faced with a tough decision when ACI announced its termination of support for its BASE24 financial-transaction switch on HP NonStop systems. It either had to make a major investment to convert its applications to run on an alternate platform or it had to move to another transaction switch on the HP NonStop. After a great deal of study and analysis, it chose the latter and decided to go with OmniPayments from Opsol Integrators.

As a result, the grocery chain recognized several improvements in the functionality of its financial-transaction system:

- It achieved continuous availability for its grocery stores via OmniReplicator's active/active architecture.
- It became PCI DSS compliant with encryption of data in-flight and at-rest.
- It moved to an improved, industry-standard communication protocol for its POS terminals.
- It supports EMV smart cards, the payment cards of the future.
- It eliminated its 300 in-store servers that managed its POS terminals.
- It is now able to add new functionality in the OmniPayments switch rather than having to roll upgrades to 300 in-store servers.
- It significantly reduced its license fees for the transaction switch.

OmniPayments includes several stand-alone modules, most of which are bundled into OmniPayments and are not sold separately. These modules include OmniReplicator, OmniConsole, OmniDash, and OmniLogger. However, OmniCrypto and OmniOffender are sold as separate products.

Opsol Integrators

With successful implementations at many customer sites, OmniPayments is just one member of the Opsol family of solutions for the financial industry. Opsol Integrators Inc. specializes in HP NonStop mission-critical applications and is HP NonStop's largest system integrator.