F5 ARX Disaster Recovery with BIG-IP Global Traffic Manager (GTM)

Michael Fabiano, 2011-25-10

Introduction

This article highlights the F5 ARX Disaster Recovery process via the configuration-replication feature (DMOS 5.2 and above) and Big-IP (v10.2.1) Global Traffic Manager (GTM). A new ARX global-config mode option enables as well as facilitates simple Disaster Recovery fail-over of all or part of a file virtualization environment from one ARX cluster to another assuming that files are being replicated using file server replication technology (i.e SnapMirror; VNX Replication; etc…). When an administrator wishes to fail-over to the other ARX cluster, they can load and enable all (or parts of) the replicated and shared global-config. This is important to note as the administrator has the ability to fail-over the entire site or down to a single Virtual IP (VIP) if needed. Having the ability and granularity of virtual server fail-over allows Active/Active configurations where some VIPs are active on SiteA and others are active on SiteB. In parallel, GTM pools can be configured and synchronized with ARX global-servers in order to fail-over to a DR data center. This ARX/GTM solution facilitates minimal end-user traffic disruption and/or down-time and a complete enterprise Disaster Recovery strategy, which minimizes Recovery Time and respective Recovery Point objectives.

Problem/Challenge

Prior to ARX DMOS 5.02.000, two-site Disaster Recovery solutions with storage based replication required manual scripts to keep ARX configurations in sync. These were Expect and Perl scripts used within production environments to perform ARX Disaster Recovery from one data center to another. Due to the complex nature of coordinating DR services across multiple devices, having to manually run additional scripts on ARX made the DR fail-over process more time consuming. Continual ARX CLI changes among all the various releases resulted in tedious script updates in order to accommodate CLI deltas among releases.

With respect to DNS changes, once failed over to the DR site, administrators would need to manually change the ARX virtual-server IPs in the local DNS. In some instances, customers can have hundreds of virtual servers that would require manual local DNS changes before enabling the fail-over data center. Again, this proved tedious.

Solution

The ARX DMOS 5.2 configuration-replication feature accomplishes simple failover by configuring a global-config replication between ARX clusters. The replication is based on a schedule and is configured in global-mode and occurs directly from the active node on the active ARX cluster to the active and backup node on the backup ARX cluster. The target storage device for the replicated global-config is the system disk. Big-IP Global Traffic Managers (GTMs) are configured and synchronized, in conjunction with ARX configuration-replication, with ARX global-server DNS information redirecting end-users to the DR data center upon successful DR fail-over. In other words, once SiteB DR data center has been correctly provisioned and enabled with the ARX replication configuration, then the SiteB Global Traffic Manager is subsequently provisioned and made active as well as authoritative for the respective delegation domain name for the ARX global-config and respective active global-server at the DR site. See Figure 1 below illustrating a high-level F5 ARX/BIG-IP Global Traffic Manager Disaster Recovery fail-over design:

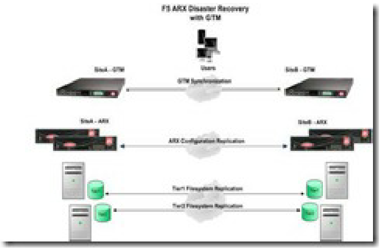
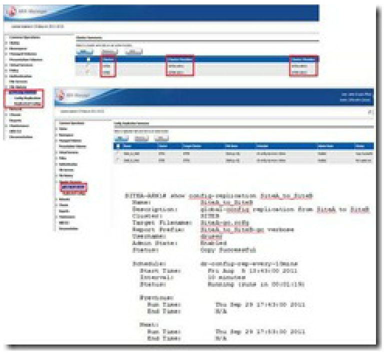

F5 ARX Disaster Recovery with GTM
Users
SiteA - GTM
SiteB - GTM
GTM Synchronization
SiteA - ARX
SiteB - ARX
ARX Configuration Replication
Tier1 Filesystem Replication
Tier2 Filesystem Replication

Figure 1 – Disaster Recovery with F5 ARX and Big-IP Global Traffic Manager (GTM)

Setup 1: ARX configuration-replication

Below are the ARX GUI & CLI screen-shots for the F5 ARX configuration-replication feature:



```
SITEA-ARX1# show config-replication SiteA_to_SiteB
  Name:            SiteA_to_SiteB
  Description:     global-config replication from SiteA to SiteB
  Cluster:         SITEB
  Target Filename: SiteB-gc.rcfg
  Report Prefix:   SiteA_to_SiteB-gc verbose
  Username:        druser
  Admin State:     Enabled
  Status:          Copy Successful

  Schedule:        dr-config-rep-every-10mins
    Start Time:      Fri Aug  5 13:43:00 2011
    Interval:        10 minutes
    Status:          Running (runs in 00:01:19)

    Previous:
      Run Time:        Thu Sep 29 17:43:00 2011
      End Time:        N/A

    Next:
      Run Time:        Thu Sep 29 17:53:00 2011
      End Time:        N/A
```

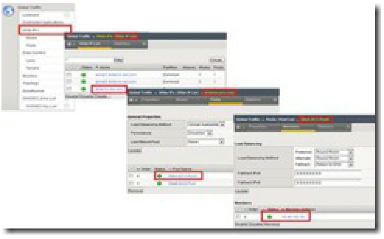
Setup 2: Global Traffic Manager (GTM) Wide-IPs for ARX

Below is the GTM GUI screenshot representing 3 GTM Wide-IPs for ARX:

1. drdemo.arx.com = delegation domain that GTM is authoritative

2. arxvip1.drdemo.arx.com = SiteA ARX global-server

3. arxvip2.drdemo.arx.com = SiteB ARX global-server



F5 ARX & GTM DNS Considerations

A typical GTM deployment involves the creation of a DNS delegation domain under the current DNS domain. This allows the GTM to be the authoritative source for all records in the delegation domain. Server names that need to be converted to Wide-IP's have their IP addresses moved to this delegation domain. When this is done the FQDN of the server being converted to a Wide-IP changes. The original server name is preserved using a CNAME alias.

Most ARX deployments involve what is called a name-based takeover. In this situation the original filer server name is moved to the ARX and the file server is renamed. This allows the ARX to virtualize the existing file sever without requiring any changes to the clients that access this file server.

In combined ARX/GTM deployments involving the use of Wide-IP's, an additional step is required in order to preserve Kerberos authentication. Since the use of a Wide-IP involves changing the FQDN of the original file server, a Service Principle Name (SPN) alias also needs to be created in addition to a CNAME alias. The creation of the SPN alias allows the client to authenticate using Kerberos to the ARX virtual server using the original file server name.

Example

- **Original File Server**: nas.arx.com
- **File Server is renamed to**: old-nas.arx.com
- **WideIP File Server Name**: nas.wideip.arx.com
- **ARX VIP name becomes**: nas.wideip.arx.com
- **ARX VIP is joined to**: arx.com
- **ARX VIP AD machine account**: nas in arx.com
- **CNAME is created in arx.com DNS**: nas.arx.com -> nas.wideip.arx.com
- **SPN alias is created on *nas.arx.com* SPN**:

```
setspn –a HOST/nas.wideip.arx.com nas
setspn –a CIFS/nas.wideip.arx.com nas
```

Adding GTMs to an existing DNS environment

There are two deployment methods for GTM. The first involves GTM becoming the primary DNS server for all of your clients. In the second case, GTM is only responsible for a sub-domain of the existing DNS environment. The second case is easier to deploy as it requires very few changes to the existing DNS environment. When using the second method, servers that host applications at multiple data centers are added to this new DNS subdomain. To preserve the original server name, CNAME aliases (See Figure 2 below) are created that point the original name to the new name that is part of the DNS subdomain. The existing DNS servers are then configured to delegate requests associated with the new DNS subdomain to the GTM devices. With this approach, no client changes are necessary and the GTM can be used to decide which IP address to return based on the defined health checks.

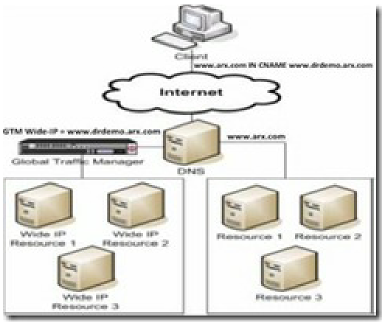


Figure 2 - GTM configured as authoritative for a new ARX delegation domain

Example

If your domain is .arx.com and your website is www.arx.com the GTM becomes authoritative for a new delegation domain drdemo.arx.com. The DNS servers in ARX.COM are configured to delegate DNS requests for anything in drdemo.arx.com to the GTM devices. The GTM is configured with a Wide-IP www.drdemo.arx.com. The original DNS A record for www.arx.com is deleted and a CNAME is created in arx.com that points to www.drdemo.arx.com.

Summary

In summary, corporations that define and subsequently design their enterprise architecture, specific to storage management, while paying close attention to disaster recovery and how it relates to all components within the design (i.e. ARX config-replication/GTM synchronization/Storage replication) are essentially investing in a long-term cost-effective disaster recovery strategy. Corporations that have a well-defined disaster recovery plan in place and deployed ahead of time ensures minimal end-user downtime dramatically reducing recovery time and recovery point objective mandates. With the F5 ARX configuration-replication feature along with the Big IP Global Traffic Manager (GTM), F5 Networks provides IT administrators data center peace of mind ensuring simple site fail-over in the event of a primary site disaster and/or outage.

Notes

In the next installment of the F5 ARX /BIG-IP Global Traffic Manager (GTM) solution tech-tip, we will expand upon and highlight BIG-IP v11 and the DNSSEC & DNS Express feature sets as well as how they are applied and benefit an ARX/BIG-IP disaster recovery strategy. More information on these feature sets can be found at the links below:

http://devcentral.f5.com/weblogs/macvittie/archive/2011/08/05/f5-friday-dns-express-ddos-protection.aspx

http://www.f5.com/pdf/white-papers/dns-services-big-ip-v11-wp.pdf

For additional information on F5 ARX and GTM please refer to the following links:

http://www.f5.com/products/arx-series/

http://www.f5.com/products/big-ip/global-traffic-manager.html

Author Bio

Michael J. Fabiano is a pre-sales Sr. Corporate Systems Engineer for the F5 Data Solutions (ARX/Data Manager/ARX-CE) Sales business unit. Michael has been with F5 Networks just under 7 years and was also a Principal Test Engineer in the Product Development engineering organization. Prior to F5, Michael worked as a Sr. Interoperability Engineer at Pillar Data Systems (An Oracle Company) in San Jose, CA and was an Infrastructure Engineer at Genuity (formerly BBN/GTE Internetworking). Michael has a Master of Engineering degree from Northeastern University in SOA Governance & Enterprise Architecture.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | 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