

VMware App Volumes

Business Continuity / Disaster Recovery Plan

Contents

Engagement Overview	3
App Volumes Summary	3
App Volumes Business Continuity and Disaster Recovery (BCDR) Summary	3
SMP App Volumes Environment for Business Continuity Testing	4
Business Continuity Installation Steps	4
Business Continuity Installing App Volumes Manager Server	7
Business Continuity Configuring App Volumes Manager Server	11
Business Continuity Installing the Second App Volumes Manager Server in BCP Pair	16
Configuring F5 Load Balancing for the BCP Pair of App Volumes Manager Servers	17
Business Continuity Validation	23
Business Continuity Conclusion	27
SMP App Volumes Environment for Disaster Recovery Testing	28
Disaster Recovery Installation Steps	29
Disaster Recovery Validation	32
Disaster Recovery Variations	38
Disaster Recovery Conclusion	38

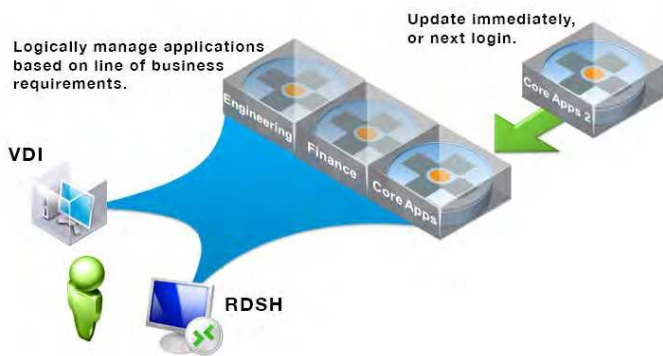
Engagement Overview

VMware engaged SMP to deliver an End-User Computing (EUC) reference study to evaluate, test, validate, and document VMware EUC technology solutions that provide their customers with a robust platform for EUC strategies. VMware has engaged SMP, pursuing experienced EUC subject matter experts to recommend how to protect App Volumes with regard to Business Continuity and Disaster Recovery Plans. SMP will also document how these solutions can help VMware's customers understand the benefits of protecting layering applications in a virtualized desktop infrastructure.

App Volumes Summary

VMware App Volumes provides real-time application delivery with lifecycle management. IT can use App Volumes to instantly deliver applications and data to users without compromising the user experience. Infrastructure and management costs are reduced by utilizing managed volumes. Unlike traditional application management solutions, App Volumes allows IT to deliver a desktop with no trade-off between user experience and costs. App Volumes allows IT to deliver applications and data to users or desktops in seconds, and at scale. Applications are stored in shared, read-only virtual disks that instantly attach to desktops by users, groups, or devices. These applications perform like natively installed applications for end-users providing a seamless desktop experience.

When App Volumes is installed on a desktop, the desktop is assigned applications from the App Volumes Manager. IT creates application stacks that are stored in shared volumes across virtual disks. With the click of a button, the App Volumes Manager delivers these application stacks to the desktop, or to the user or group they choose.



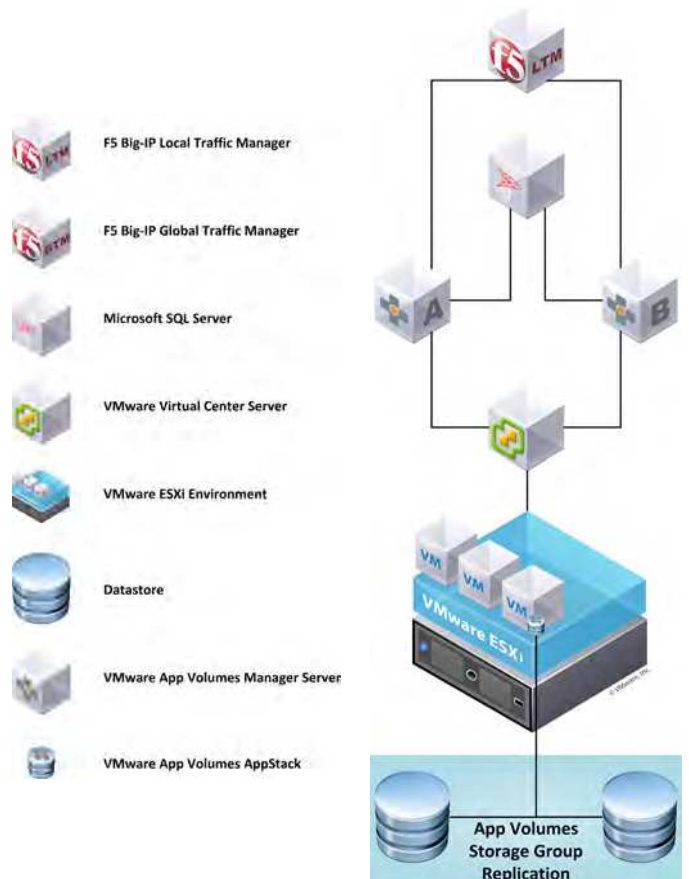
For end-users, applications delivered by App Volumes appear and perform as if they are natively installed. Applications seamlessly follow end-users across sessions and devices. Data can also optionally follow that end-user as well. IT can update, or replace applications in real time and IT can remove any assigned application in seconds. App Volumes is tightly

integrated with VMware's hypervisor / virtual infrastructure and the storage that the virtual disks span. This ensures that customers can easily scale out this solution to support end-users at scale.

App Volumes Business Continuity and Disaster Recovery (BCDR) Summary

Business continuity planning for App Volumes includes multiple App Volumes Manager servers using a shared database and App Volumes replicated storage groups. Disaster recovery planning for App Volumes includes multiple App Volumes environments using a replicated database and datastore replication for datastores containing App Volumes AppStacks. It is possible to leverage both business continuity and disaster recovery configurations together to form a resilient and highly available App Volumes environment; however this joint configuration is not necessary to operate in an environment where disaster recovery is desired apart from business continuity or vice versa.

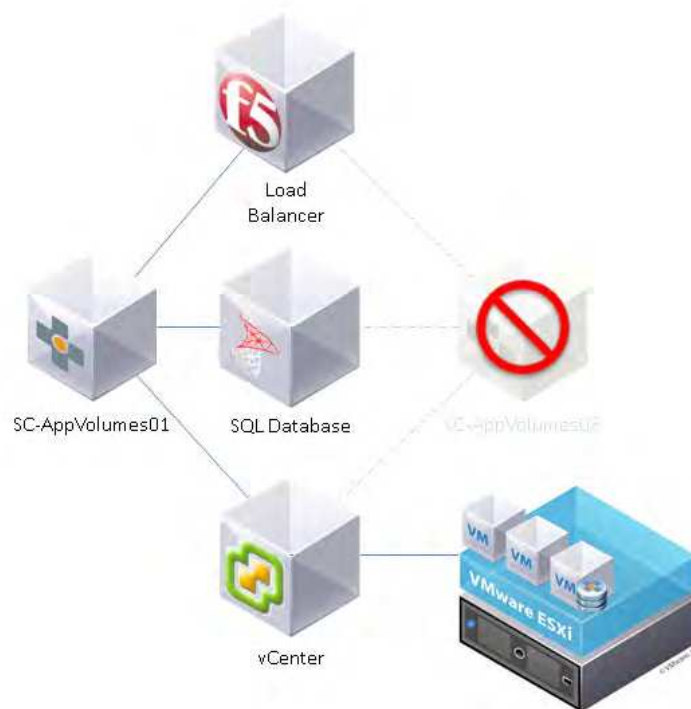
The purpose of this document is not to illustrate database or datastore replication technologies, and therefore these topics will be relegated to whichever methodology or mechanism is presently in use within the environment. This document will focus on the initial configuration of each App Volumes environment, and the methods used in each scenario.



SMP App Volumes Environment for Business Continuity Testing

The SMP environment for business continuity testing consisted of two (2), F5 load balanced VMware App Volumes 2.6 Manager servers leveraging a shared Microsoft SQL 2012 database in an AlwaysOn availability group. The AlwaysOn configuration within Microsoft SQL 2012 ensures availability of database resources, further reducing potential single points of failure within the business continuity configuration of VMware App Volumes. The F5 load balancing was configured

to balance traffic based on least number of connections, and included basic HTTP health monitoring for each of the App Volumes Manager servers. The App Volumes Managers were configured to communicate with vCenter for attaching App Volumes AppStacks to virtual machines used in conjunction with VMware Horizon View. Configured in this fashion, the App Volumes Managers can sustain a failure, and the subsequent management traffic will continue to function in a normal manner. Previously attached App Volumes AppStacks will remain, as they are not dependent on the App Volumes Management servers after assigned attachments have completed.



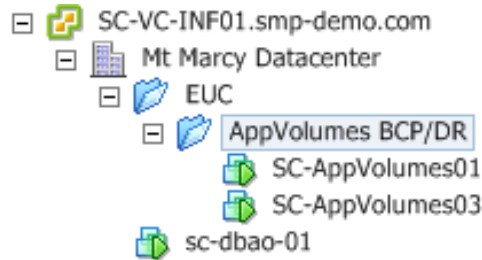
Business Continuity Installation Steps

During the course of validating the App Volumes business continuity plan detailed above, the following actions were taken to install the App Volumes environment.

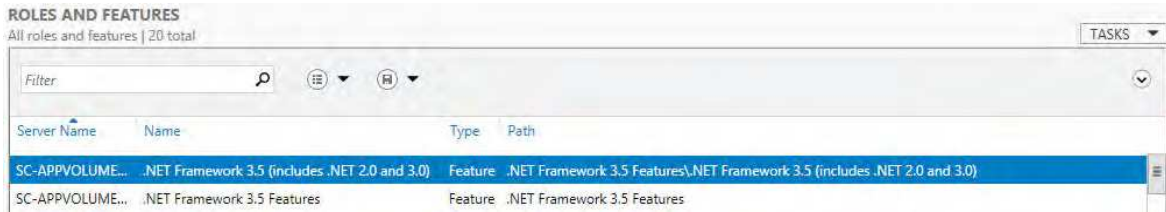
1. Business Continuity Pre-Configuration

- Determined names and IP addresses of two (2) App Volumes Manager servers and one (1) load balanced namespace. This encompassed three (3) IP addresses
- Created a DNS entry for the load balanced namespace

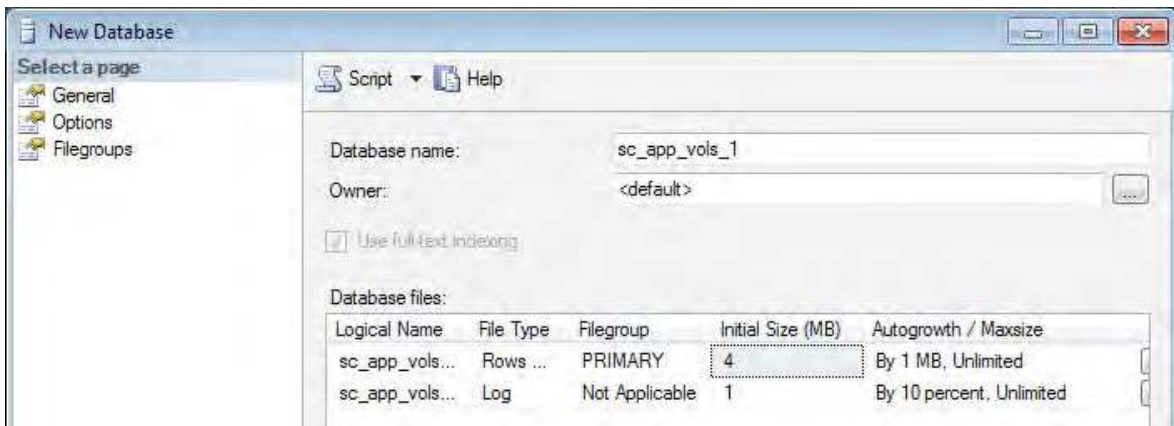
- c. Two (2) Windows Server 2012 r2 virtual machines were deployed to act as App Volumes Manager servers and added to the domain. For future reference, in the illustration below, SC-AppVolumes01 and SC-AppVolumes03 were paired together as a BCP pair which was ultimately given a load balanced namespace, monitored and controlled by an F5 Local Traffic Manager,



- d. The .NET Framework 3.5 feature was added to each Windows Server 2012 r2 virtual machine

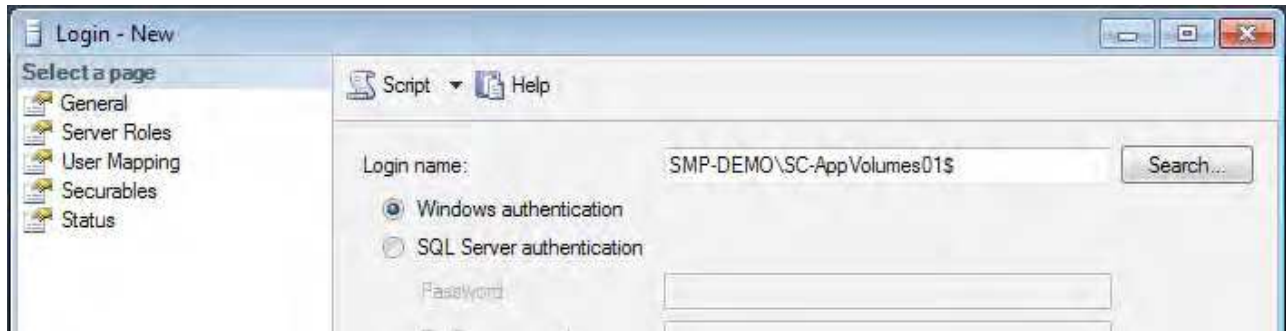


- e. An empty Microsoft SQL database in an AlwaysOn availability group was created



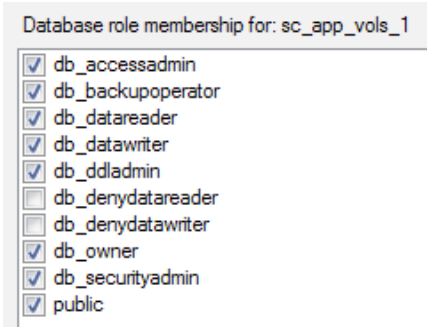
Note: More information on configuring AlwaysOn availability groups can be found at <https://msdn.microsoft.com/en-us/library/gg509118.aspx>

- f. Microsoft SQL users were created for each server's service account using Windows authentication, consisting of the domain, then the App Volumes Manager server name followed by a dollar sign



g. Each of the created Microsoft SQL users was granted the following roles to the database under each user's User Mapping attribute

- db_accessadmin ■ db_ddladmin
- db_backupoperator ■ db_owner
- db_datareader ■ db_securityadmin
- db_datawriter ■ public



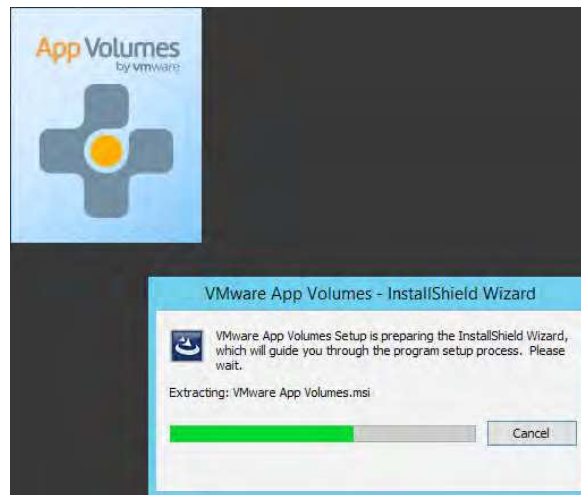
- h. Created an Active Directory service account for App Volumes
- i. Created an Active Directory security group for App Volumes administrators and added the service account for App Volumes as a member of the newly created security group
- j. Presented two (2) datastores for App Volumes AppStacks and templates which were later configured for storage group replication via the App Volumes Manager web interface.
- k. Provided the App Volumes service account with the following permissions within vCenter:

Datastore	Resource	Virtual Machine	Virtual Machine
Allocate Space	Assign Virtual Machine to Resource Pool	Configuration	Provisioning
Browse Datastore		Add Existing Disk	Clone Template
Low Level File Operations	Sessions	Add New Disk	Clone Virtual Machine
Remove File	View and Stop Session	Add or Remove Device	Create Template from Virtual Machine
Update Virtual Machine Files	Tasks	Change Resource	Customize
	Create Task	Remove Disk	Deploy Template
Folder		Settings	Mark as Template
Create Folder		Interaction	Mark as Virtual Machine
Add Existing Disk		Power Off	Modify Customization Specification
		Power On	Promote Disks
Global		Suspend	Read Customization Specifications
Cancel Task		Inventory	
		Create form Existing	
Host		Create New	
Local Operations		Move	
Create Virtual Machine		Register	
Delete Virtual Machine		Remove	
Reconfigure Virtual Machine		Unregister	

Installing App Volumes Manager Server

This section covers how to install a single App Volumes Manager or the first App Volumes Manager in a BCP pair

2. Installed the first App Volumes Manager server
 - a. Opened the App Volumes Setup application



- b. Proceeded through the VMware App Volumes installation wizard by clicking next



- c. Read through the VMware App Volumes License Agreement to ensure that it hadn't changed since the first installation before accepting and clicking next



- d. Selected "Install App Volumes Manager" on the App Volumes Install Screen, then clicked the install button



- e. Proceeded through the App Volumes Manager installation wizard by clicking next



- f. Selected "Connect to an existing SQL Server Database" and clicked next



- g. Entered information for the MS SQL AlwaysOn Availability Group Listener as the database server, connecting with Windows Integrated Authentication, browsed for the database, and ensured that the checkbox to “Overwrite existing database” was selected*



* Selecting the option to overwrite the existing database is only to be chosen when installing the first instance of App Volumes Manager. Selecting this in the second instance will result in loss of configuration information!

- h. Left the HTTP and HTTPS ports at their default values of 80 and 443



- i. Left the destination location and feature installation selection at default values



- j. Began installation by clicking the Install button



- k. App Volumes Manager began installation routine



- l. App Volumes Manager installation wizard completed



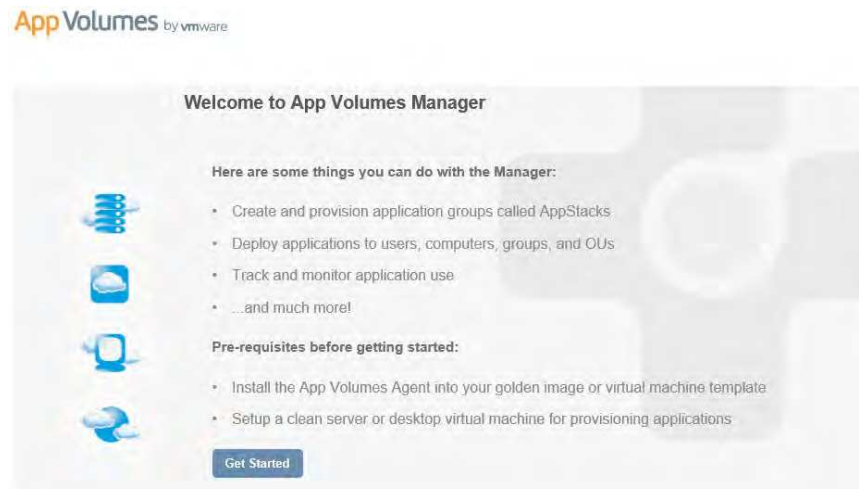
Configuring App Volumes Manager Server

This section covers how to configure a single App Volumes Manager or the first App Volumes Manager in a BCP pair

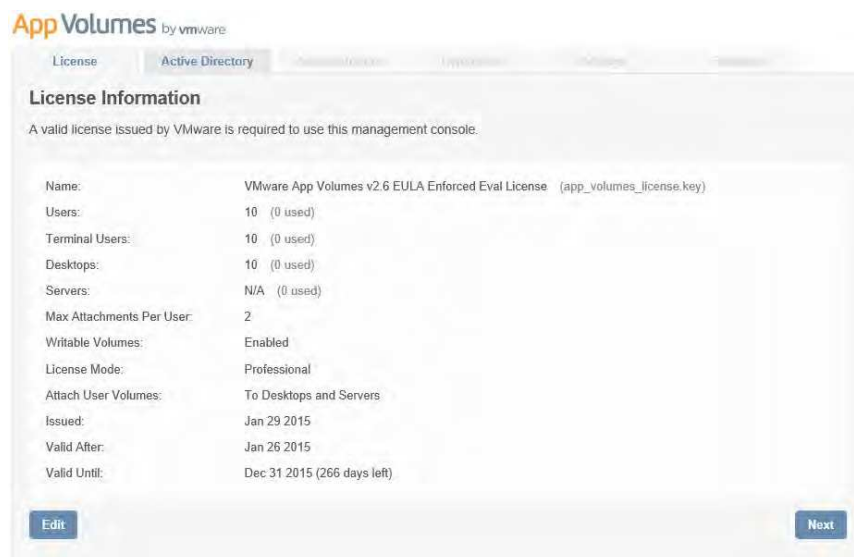
3. Configure the first App Volumes Manager server
 - a. Launched the App Volumes Manager web interface from desktop shortcut



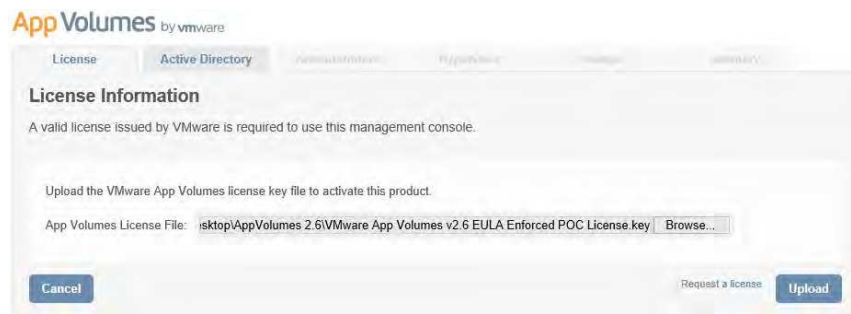
- b. Clicked the "Get Started" button on the Welcome to App Volumes Manager page



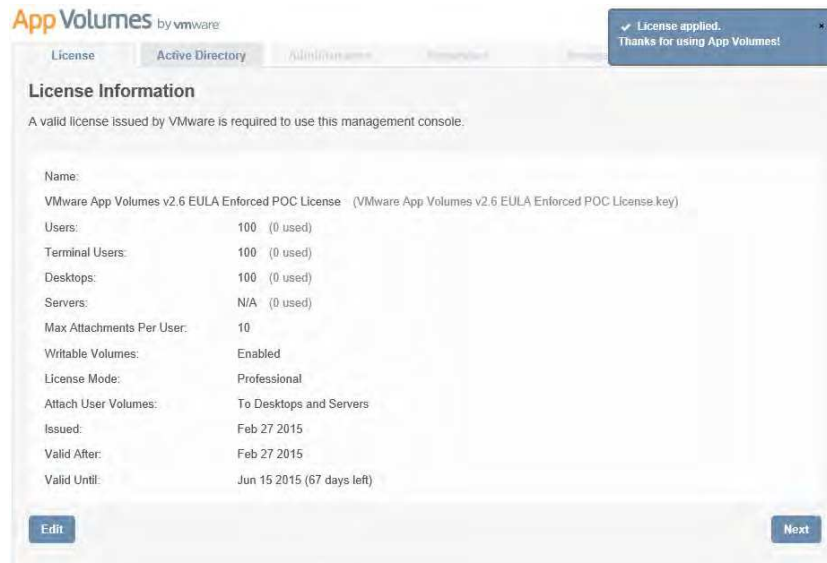
- c. Clicked the "Edit" button on the License Information page to provide a more applicable license



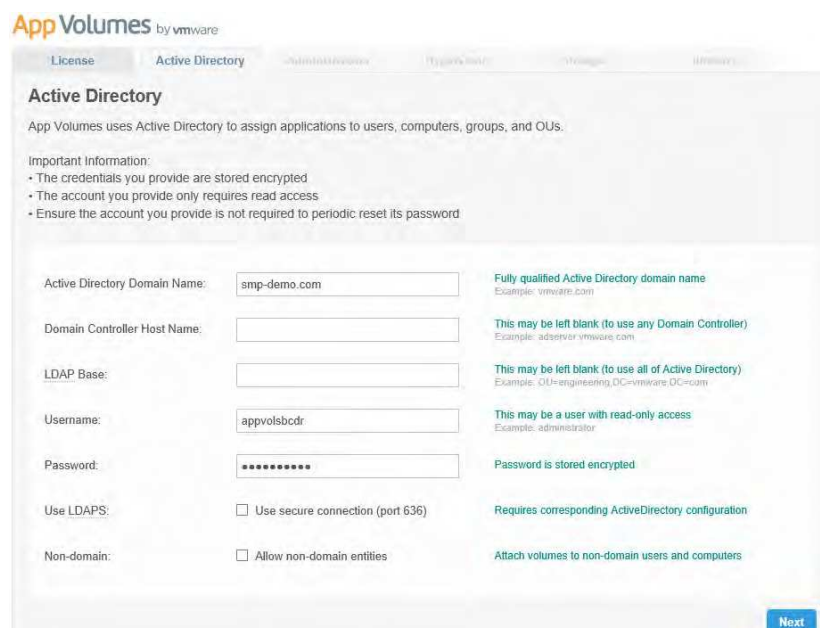
- d. Browsed for the appropriate license file and clicked the “Upload” button



- e. Verified the license information before clicking the “Next” button



- f. Provided Active Directory information and clicked the “Next” button



- g. Searched for and selected the Active Directory security group for App Volumes administrators within the domain before clicking the “Next” button

The screenshot shows the 'App Volumes Administrators Group' configuration page. The 'Current Group' is 'Not configured'. The 'Search Groups' field contains 'AppVol' and the 'Contains' dropdown is set to 'Contains'. A 'Search!' button is visible. Below this, there is a checkbox for 'Search all domains in the Active Directory forest' which is unchecked. The 'Choose Group' dropdown is set to 'SMP-DEMOAppVolumesAdministrators'. A 'Next' button is located at the bottom right.

- h. Entered vCenter information, providing the App Volumes service account information for accessing vCenter per the permissions noted in the bottom corner of the page (as detailed in the Pre-Configuration section above)

The screenshot shows the 'Hypervisor Credentials' configuration page. The 'Hypervisor' dropdown is set to 'vCenter Server'. The 'Host Name' field contains 'sc-vc-euc01.smp-demo.com'. The 'Username' field contains 'SMP-DEMO\appvolsbcdr'. The 'Password' field is masked with dots. There are two checkboxes: 'Mount Local' (unchecked) and 'Mount On Host' (unchecked). A 'Next' button is at the bottom right. Below the form, there is a note: 'Required vCenter Permissions'.

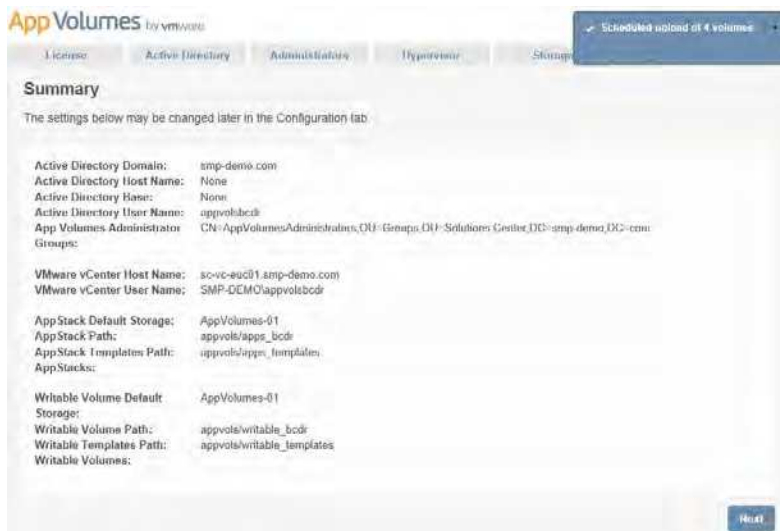
- i. Selected datastore locations and specified desired storage paths for AppStacks and templates before clicking the “Next” button

The screenshot shows the 'Storage' configuration page. The 'Default Storage Location' for both 'AppStacks' and 'Writable Volumes' is set to '[Mt Marcy Datacenter] AppVolumes-01 (NFS)'. The 'Default Storage Path' for AppStacks is 'appvol/apps_bcd' and for Writable Volumes is 'appvol/writable_bcd'. The 'Template Path' for both is 'appvol/apps_templates'. A 'Next' button is at the bottom right.

- j. Provided ESXi host information and selected templates to upload onto the desired storage paths for template locations before clicking the "Upload" button



- k. Verified configuration information before clicking the "Next" button



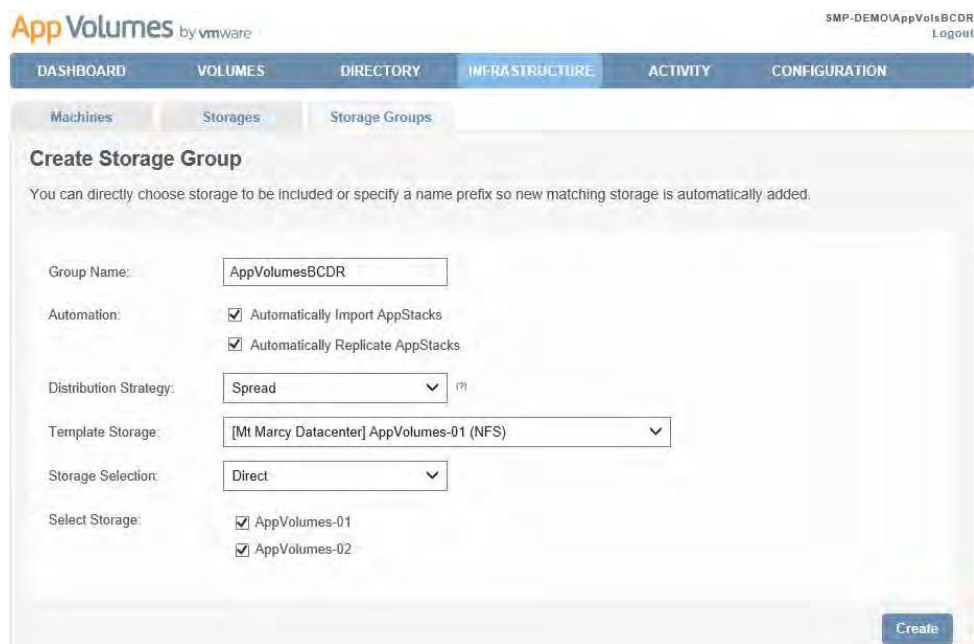
- l. Arrived at the Volumes > AppStacks page, automatically logged in as the previously specified Active Directory User Name



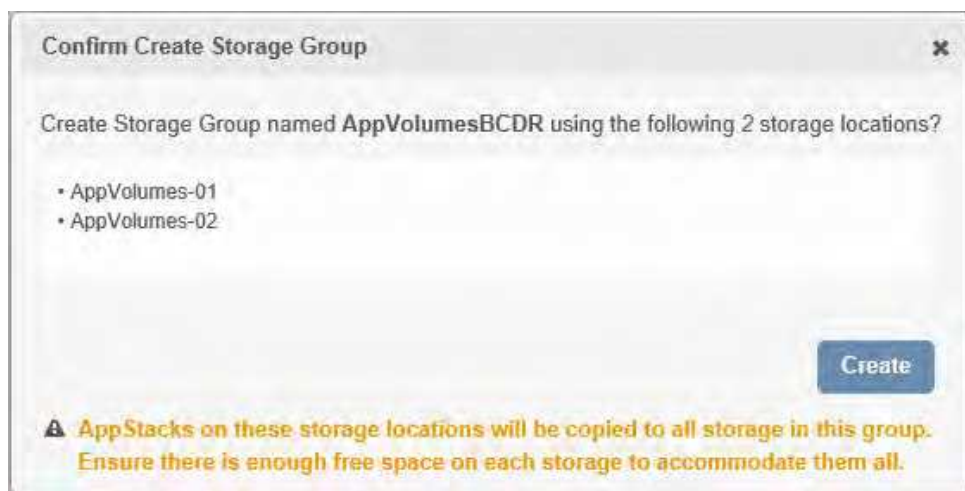
- m. Navigated to Infrastructure > Storage Groups to begin configuration of storage groups for App Volumes, and clicked the “Create Storage Group” button



- n. Provided a name for the new storage group, elected to automatically import and replicate AppStacks with a spread distribution strategy, and selected the two (2) datastores designated for AppVolumes, then clicked the “Create” button



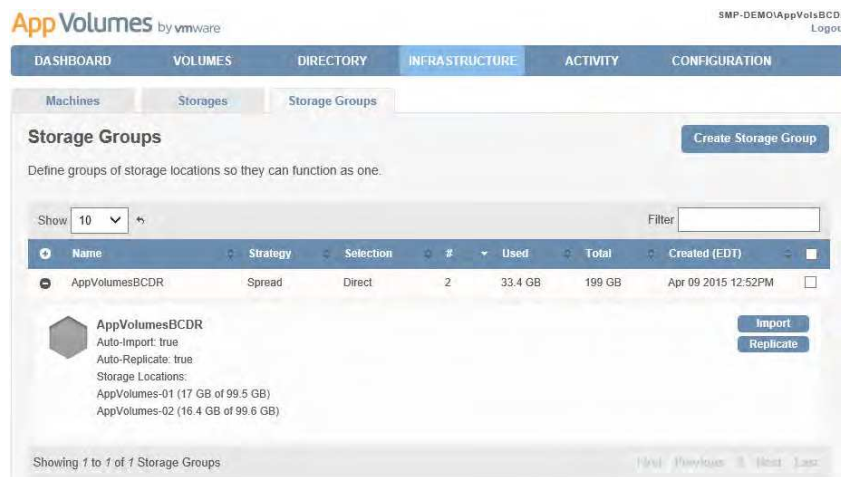
- o. Reviewed the storage group confirmation window, and clicked the “Create” button



- p. The storage group was created successfully, and now appears within the Storage Groups tab



- q. Clicked the plus sign to the left of the storage group to view and confirm further details surrounding the storage group. This concludes the initial configuration of the first App Volumes Manager server



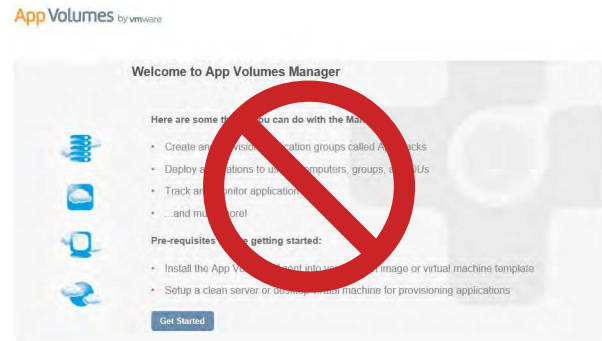
Installing the Second App Volumes Manager Server in a BCP Pair

This section covers how to install the second App Volumes manager in a BCP pair. The installation of the second App Volumes manager is very similar to the installation of the first App Volumes manager node. In fact, the same steps can be followed, with the following exceptions:

- 4. The same database should be specified for the second node in the BCP pair, however the checkbox to “overwrite the existing database” at the bottom of the installation screen where the database server is defined 2g MUST be left unchecked. If this checkbox is checked, it will be necessary to reconfigure App Volumes.



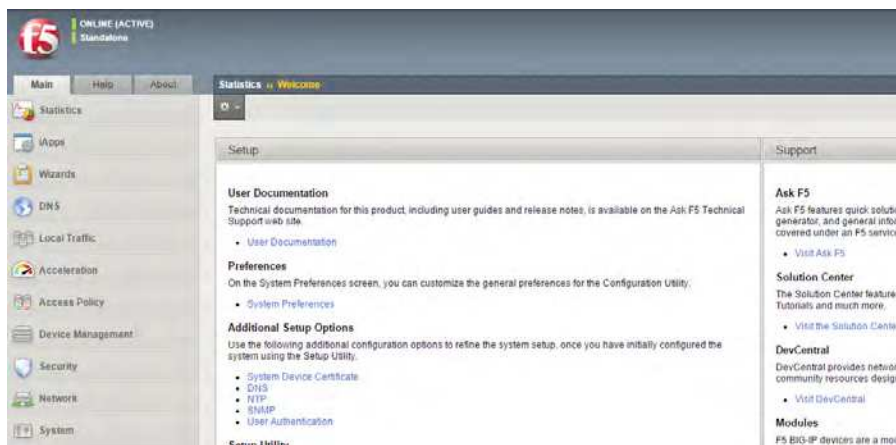
5. Verification of proper second node installation can be accomplished by launching the App Volumes Manager web interface from desktop shortcut. If a login screen appears, the second node was installed successfully. If a welcome screen appears, the database has been overwritten, and App Volumes will need to be reconfigured per the section pertaining to configuring App Volumes above.



Configuring F5 load balancing for the BCP pair of App Volumes Manager Servers

This section covers how to configure load balancing for the BCP pair of App Volumes Manager servers

6. Configure F5 load balancing
- a. Logged into the production F5 Big-IP Local Traffic Manager



- b. Navigated to Local Traffic > Monitors and clicked the plus sign to add a new monitor



- c. Created a new health monitor with the following non-default properties Type: HTTP

Parent Monitor: http_80 Interval: 20 seconds

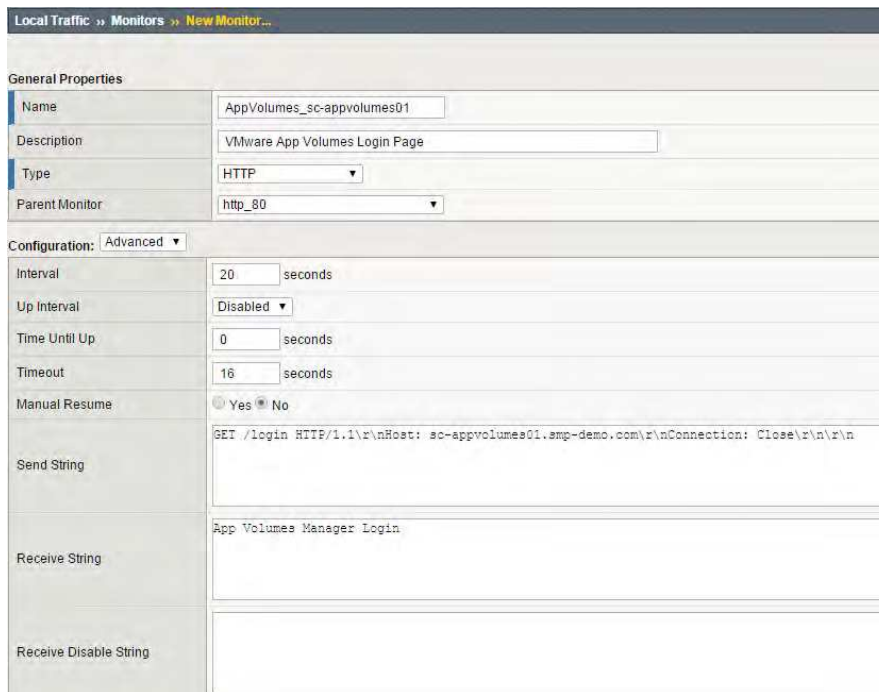
Send String (without actual line breaks):

GET /login HTTP/1.1\r\n

Host: sc-appvolumes01.smp-demo.com\r\n

Connection: Close\r\n\r\n

Receive String: App Volumes Manager Login



Local Traffic >> Monitors >> New Monitor...

General Properties

Name: AppVolumes_sc-appvolumes01
Description: VMware App Volumes Login Page
Type: HTTP
Parent Monitor: http_80

Configuration: Advanced

Interval: 20 seconds
Up Interval: Disabled
Time Until Up: 0 seconds
Timeout: 16 seconds
Manual Resume: Yes

Send String: GET /login HTTP/1.1\r\nHost: sc-appvolumes01.smp-demo.com\r\nConnection: Close\r\n\r\n

Receive String: App Volumes Manager Login

Receive Disable String:

Note: Click the "Repeat" button when submitting the new health monitor to create another similar health monitor for the other App Volumes Manager server

- d. Created another health monitor similar to the first, but with the second App Volumes Manager server name in the Name and Send String fields



Local Traffic >> Monitors

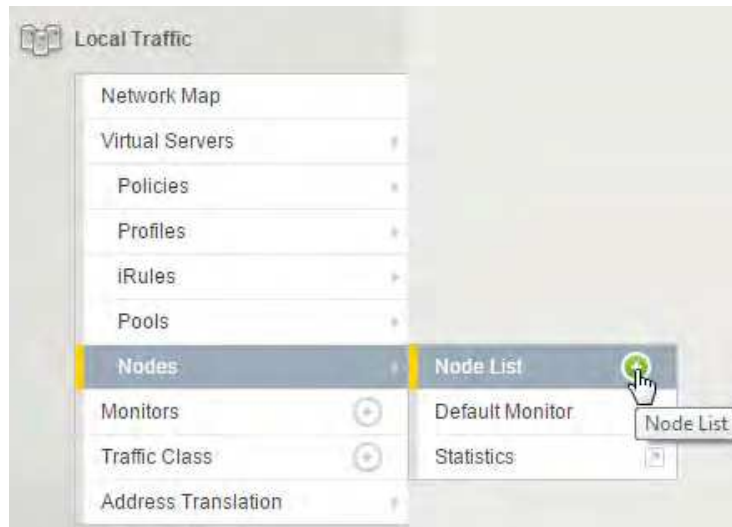
Monitor List

Search Reset Search Create...

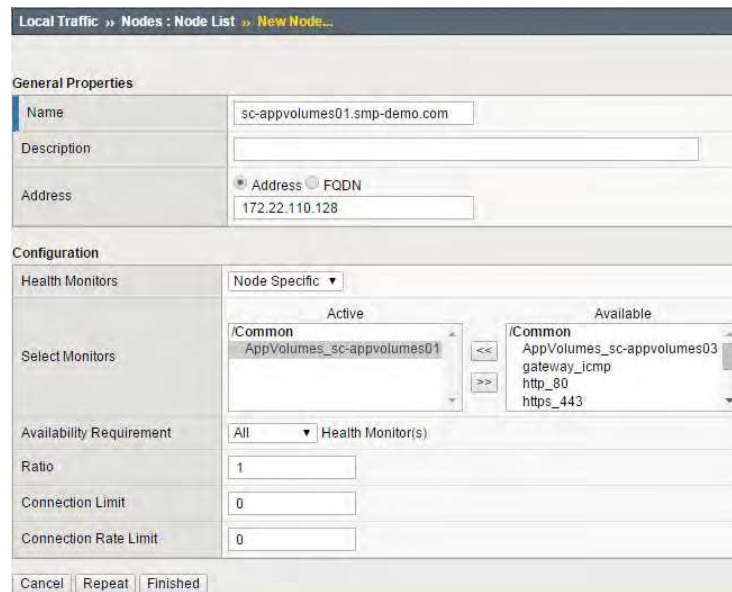
Name	Application	Type	Partition / Path
AppVolumes_sc-appvolumes01		HTTP	Common
AppVolumes_sc-appvolumes03		HTTP	Common

Delete...

- e. Navigated to Local Traffic > Nodes > Node List and clicked the plus sign to add a new node

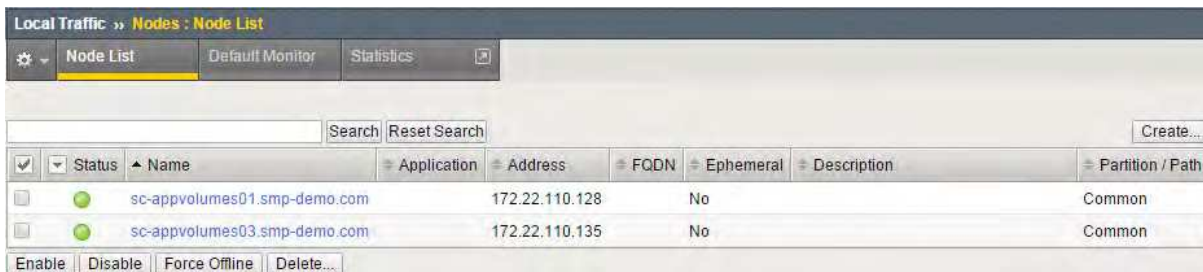


- f. Created a new node, specifying an identifiable name, the IP address, and the corresponding Node Specific health monitor



Note: Click the “Repeat” button when submitting the new node to create another similar node

- g. Created another node similar to the first, but with the second App Volumes Manager information and health monitor



Note: The green status indicators let us know that the health monitors are detecting that the login page is accessible for each App Volumes Manager server

- h. Navigated to Local Traffic > Pools > Pool List and clicked the plus sign to add a new pool



- i. Created a new pool with the load balanced namespace as the name, the http_80 health monitor, “Least Connections (member)” load balancing method, and selected each of the previously identified nodes on service port 80 as pool members

A screenshot of the 'New Pool' configuration dialog in the VMware Local Traffic Manager. The dialog is titled 'Local Traffic >> Pools : Pool List >> New Pool...'. It has a 'Configuration: Advanced' dropdown at the top left. The configuration is divided into several sections:

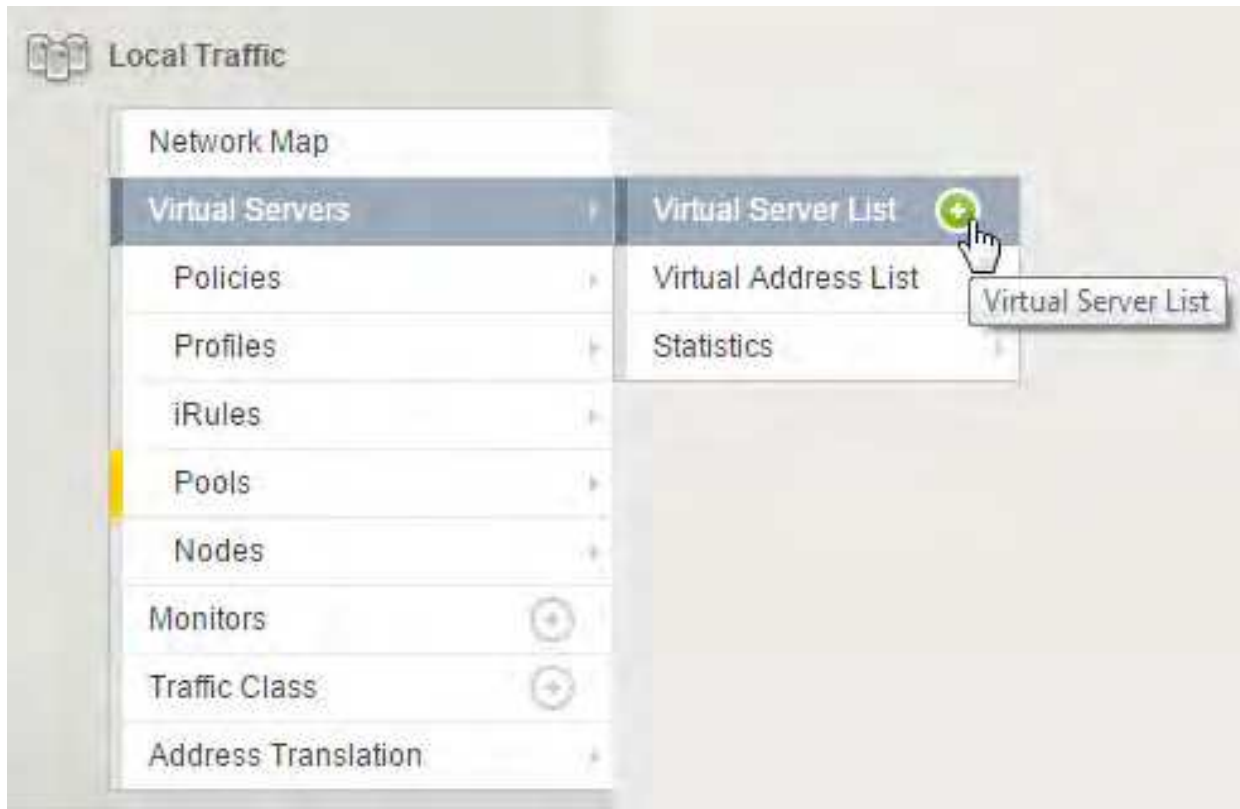
- Name:** MM-AppVolumes.smp-demo.com
- Description:** (empty text field)
- Health Monitors:** A list of health monitors is shown. Under the 'Active' column, 'http_80' is selected. Under the 'Available' column, 'AppVolumes_sc-appvolumes01', 'AppVolumes_sc-appvolumes03', 'gateway_icmp', and 'http' are listed.
- Availability Requirement:** All Health Monitor(s)
- Allow SNAT:** Yes
- Allow NAT:** Yes
- Action On Service Down:** None
- Slow Ramp Time:** 10 seconds
- IP ToS to Client:** Pass Through
- IP ToS to Server:** Pass Through
- Link QoS to Client:** Pass Through
- Link QoS to Server:** Pass Through
- Reselect Tries:** 0
- Enable Request Queueing:** No
- Request Queue Depth:** 0
- Request Queue Timeout:** 0 ms
- IP Encapsulation:** None

The **Resources** section is expanded to show:

- Load Balancing Method:** Least Connections (member)
- Priority Group Activation:** Disabled
- New Members:** A list of nodes is shown. The 'Node List' radio button is selected. The list contains two entries: 'R:1 P:0 C:0 sc-appvolumes01.smp-demo.com 172.22.110.128:80' and 'R:1 P:0 C:0 sc-appvolumes03.smp-demo.com 172.22.110.135:80'. There are 'Add', 'Edit', and 'Delete' buttons for the members.

At the bottom of the dialog are 'Cancel', 'Repeat', and 'Finished' buttons.

- j. Navigated to Local Traffic > Virtual Servers > Virtual Server List and clicked the plus sign to create a new virtual server, which will leverage our DNS registered load balanced IP address



- k. Created a new virtual server with the following non-default properties (see diagram 1)

Name and Destination Address (load balanced IP address)

Service Port: 80 (HTTP)

Protocol Profile (Client): tcp-lan-optimized HTTP Profile: http

Source Address Translation: Auto Map Port

Translation: unchecked OneConnect

Profile: oneconnect

Default Pool: previously created pool of App Volumes Manager servers Default

Persistence Profile: source_addr

Diagram 1

Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server...

General Properties

Name	MM-AppVolumes.smp-demo.com
Description	
Type	Standard
Source Address	
Destination Address	172.22.110.143
Service Port	80 HTTP
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp-lan-optimized
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
FTP Profile	None
RTSP Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map
Bandwidth Controller	None
Connection Rate Limit Mode	Per Virtual Server
Address Translation	<input checked="" type="checkbox"/> Enabled
Port Translation	<input checked="" type="checkbox"/> Enabled
Source Port	Preserve
Clone Pool (Client)	None

Acceleration: Advanced

Rate Class	None
OneConnect Profile	oneconnect
NTLM Conn Pool	None
HTTP Compression Profile	None

Policies

Default Pool	MM-AppVolumes.smp-demo.com
Default Persistence Profile	source_addr
Fallback Persistence Profile	None

Cancel Repeat Finished

- I. Verified health status of the new virtual server by viewing the status column within the virtual server list



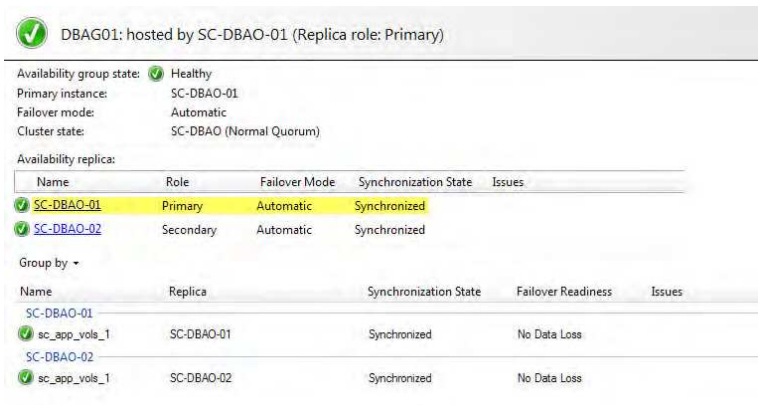
Business Continuity Validation

SMP tested the above scenario, and determined that the App Volumes Managers operated in the expected manner. Details of the validation can be found below.

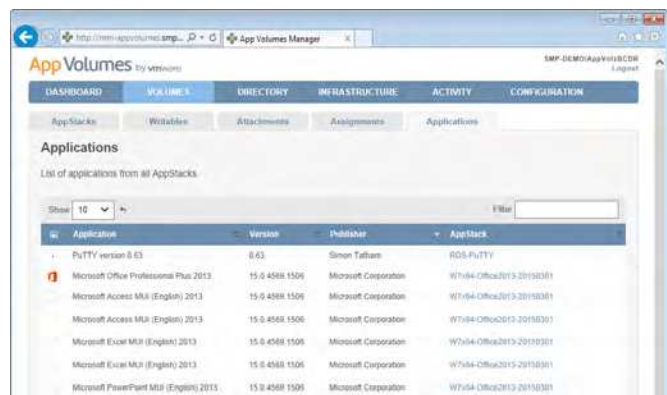
Business Continuity Validation Steps

During the course of validating the App Volumes business continuity plan detailed above, the following actions were taken.

1. Configuration
 - a. App Volumes Manager servers were installed and configured to use an external Microsoft SQL database in an AlwaysOn availability group
 - b. App Volumes AppStacks were created to include AppStacks assigned and attached to Microsoft Remote Desktop Services Hosts (RDSH) via Active Directory Organizational Unit, and pools of VMware Horizon View desktops via Active Directory Organizational Unit
 - c. Load balancing was configured via F5's Big-IP Local Traffic Manager including health monitors and a DNS entry
 - d. App Volumes Agents were installed using the load balanced DNS name
2. Environmental Verification



- a. MS SQL AlwaysOn availability group was verified, with primary replica identified



- b. App Volumes AppStack assignments and attachments were verified
- c. Validated F5 health monitors, and identified which App Volumes Management server was being used out of the load balanced pool

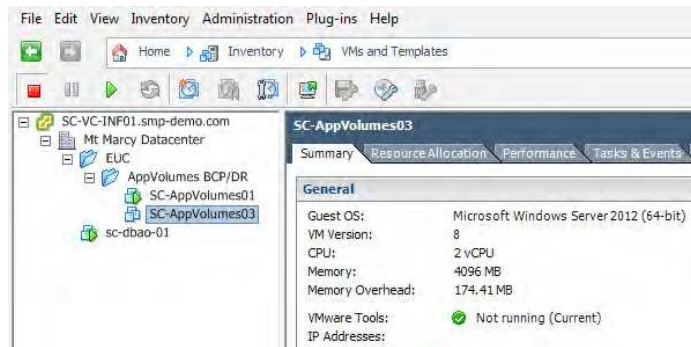
		Bits		Packets		Connections		
		In	Out	In	Out	Current	Maximum	Total
<input type="checkbox"/>	MM-AppVolumes.smp-demo.com	1.9M	8.4M	1.1K	1.1K	1	13	90
<input type="checkbox"/>	→ sc-appvolumes01.smp-demo.com:80	911.8K	5.3M	617	673	0	6	43
<input type="checkbox"/>	→ sc-appvolumes03.smp-demo.com:80	1.0M	3.0M	566	521	1	7	47

- d. App Volumes AppStacks were verified within a virtual desktop

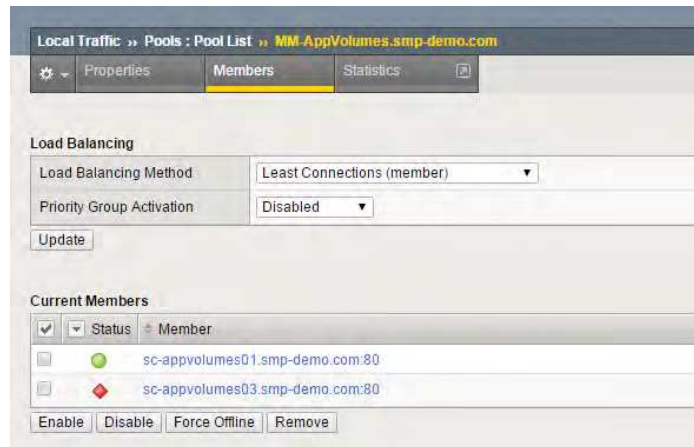


3. Disruption of App Volumes Management Server

- a. Powered down the active App Volumes Management server (03)

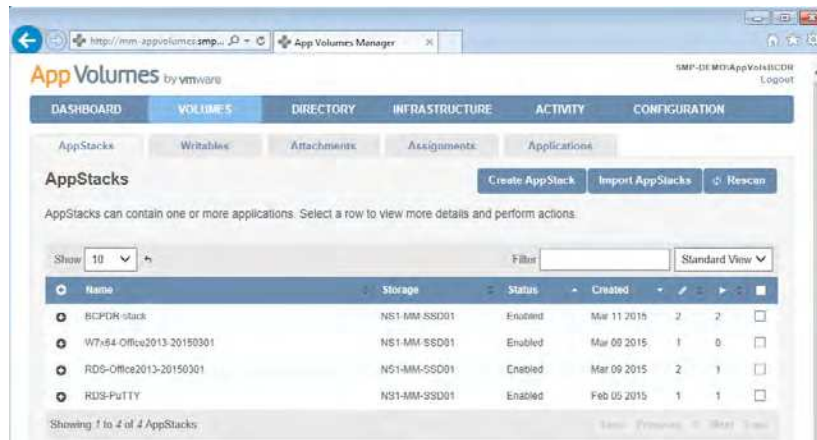


- b. F5 health monitor status was verified as detecting the App Volumes Management server offline, routing new traffic to the healthy server



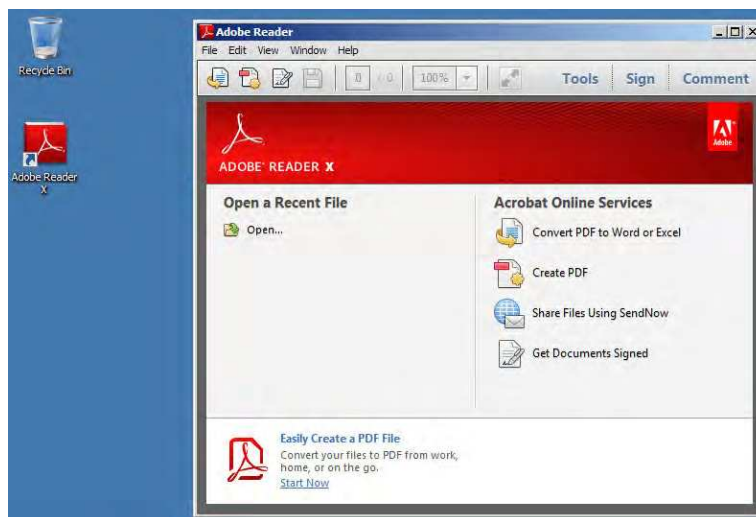
4. Verification of App Volumes State After Disrupting the App Volumes Manager

a. Navigated to the Volumes > Applications page within App Volumes Manager

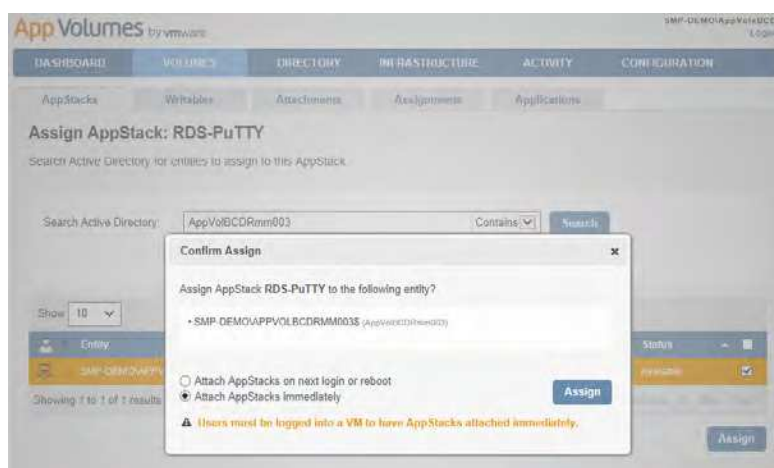


Note: The expectation was some sort of session expiration, or login page as a result of the failover – but this was not the case, the interface remained fully functional

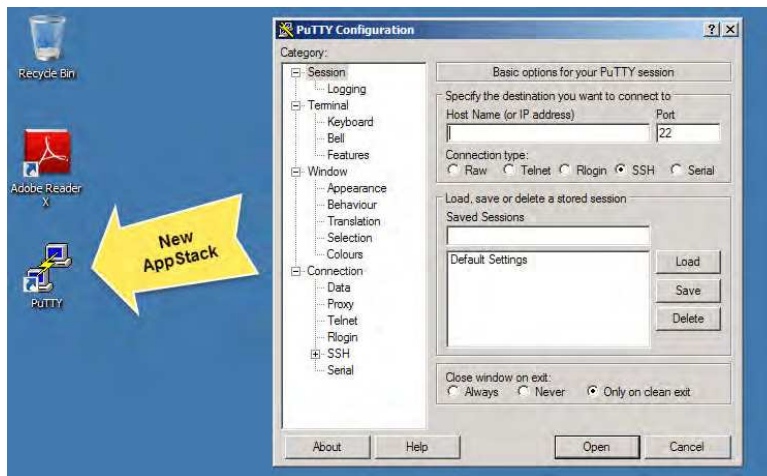
b. Verified that the previously verified AppStack was still functional



c. Assigned a different AppStack to the same machine

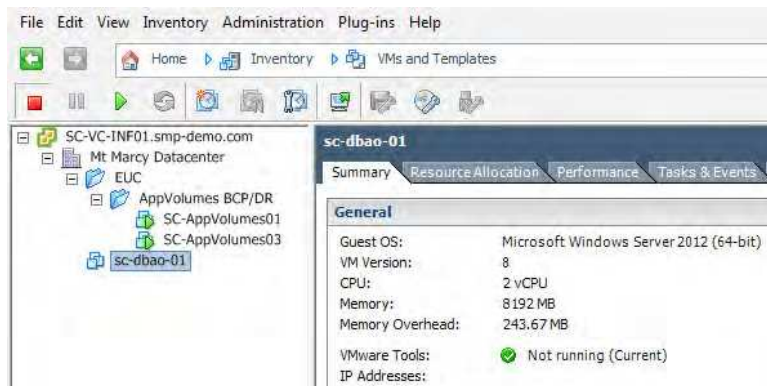


d. Verified the appearance and function of the newly assigned AppStack

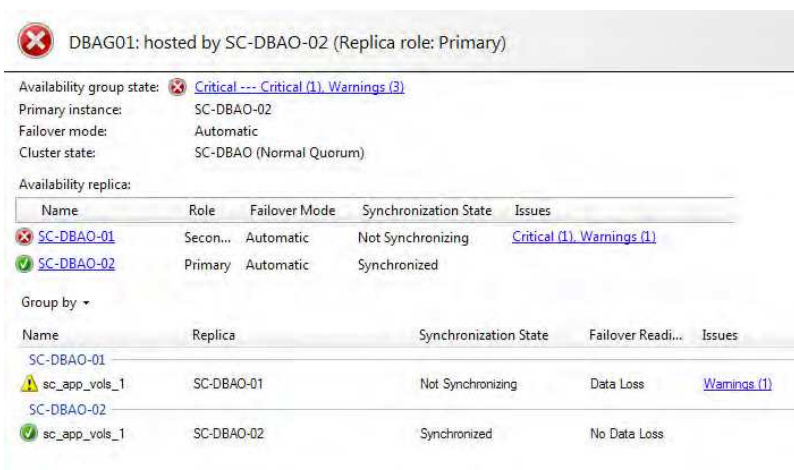


5. Disruption of AlwaysOn SQL Database

a. Powered down the primary MS SQL server (sc-dbao-01)

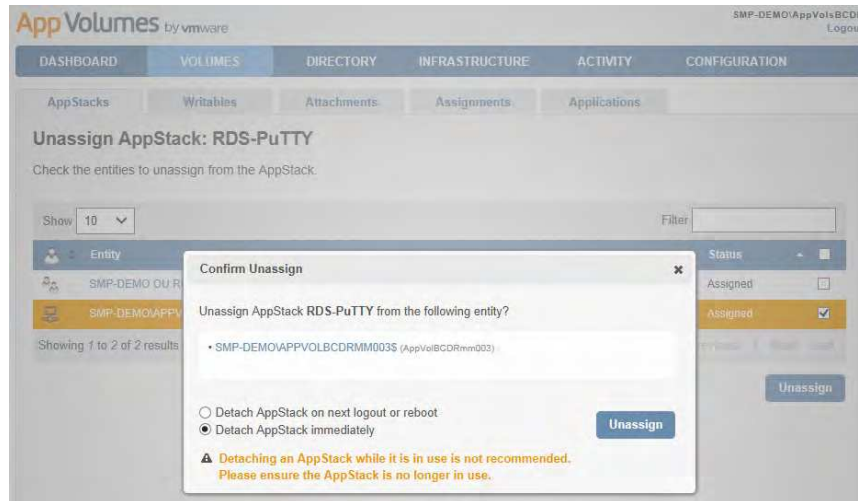


b. MS SQL AlwaysOn availability group was verified as detecting the failed MS SQL server



6. Verification of App Volumes State After Disrupting the AlwaysOn SQL Database

- a. Unassigned the previously assigned AppStack from the test machine



- b. Verified that the AppStack was detached as evidence by the disappearance of the application shortcut



Business Continuity Conclusion

SMP validated that a configuration including multiple App Volumes Manager servers using a shared database functions very well to ensure high availability of VMware’s App Volumes Manager server. SMP also validated that high availability of the underlying SQL database in an AlwaysOn configuration is beneficial in ensuring high availability of the App Volumes Management servers in the event that the server containing the SQL database sustains a failure.

SMP App Volumes Environment for Disaster Recovery Testing

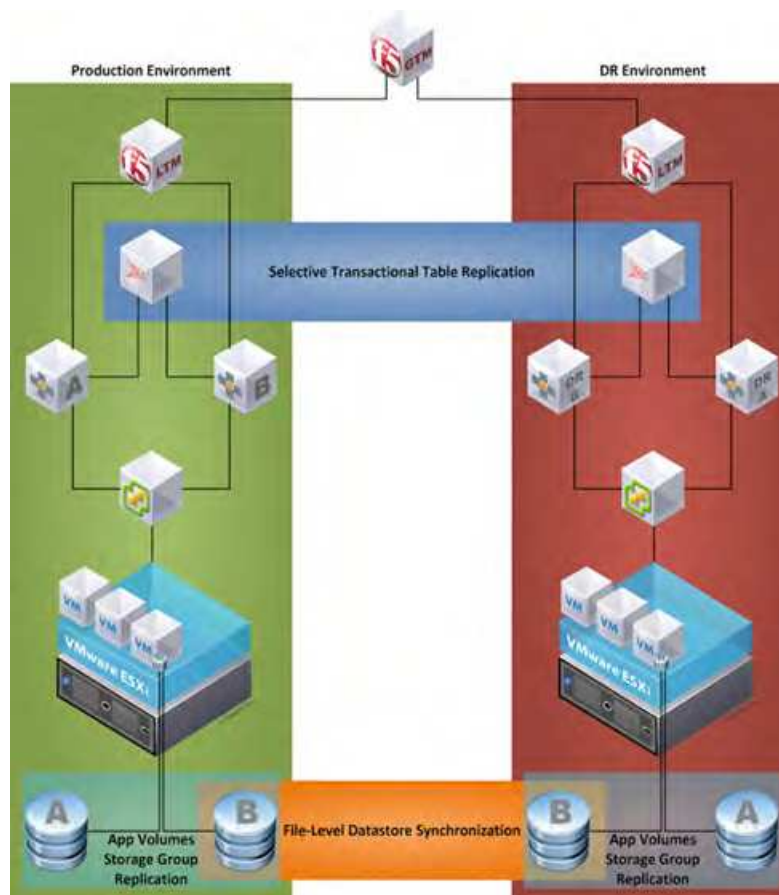
The SMP environment for disaster recovery testing consisted of two distinct VMware App Volumes 2.6 BCP-ready environments in distinct VMware Virtual Center environments, each using distinct storage resources configured with App Volumes Storage Groups. These App Volumes Storage Groups allow for the automatic replication of AppStacks between the Storage Group members, and also the automatic import of AppStacks from Storage Group members. Special consideration was made in the individual datastore naming convention, as App Volumes only leverages the datastore name when ascertaining the health of its known AppStacks. With this in mind, AppStack datastores in each environment had the same name, though the underlying storage was distinct between environments.

The two App Volumes environments shared access to the same Active Directory domain, the same VMware Horizon View environment (using different desktop and application pools), and an F5 Global Traffic Manager (GTM) was employed for geolocation based load balancing of a single DNS namespace amongst each BCP-ready App Volumes environment F5 Local Traffic Manager (LTM). The addition of the F5 GTM allows for IT administrators managing the solution to be common across the production and DR environments. When the DR event occurs, the F5 GTM's health monitor of the F5 LTM virtual server pool status triggers the change in traffic from the production environment to the DR environment. Since SMP is not using a stretched layer 2 network for the App Volumes environments, no special considerations needed to be made in the geolocation scheme.

In addition to the F5 components, select database tables were configured for transactional replication from the production database to the DR database, and AppStack datastore contents were copied from the production environment to the DR environment via SCP whenever there was a change in AppStack data (such as the creation of a new AppStack or update of an existing AppStack).

User-based assignments continued to function in the DR environment, however the specific strategy employed for assigning AppStacks became important concerning machine-based assignments. Virtual machine names in the production environment were not the same as their equivalent virtual machines in the DR environment. As a result, it was necessary to make machine-based AppStack assignments such as those used for Remote Desktop Services hosts for Horizon View

Application Pools by Active Directory Organizational Unit instead of individual machines in order for assignments to properly apply in the DR environment.



Disaster-Recovery Installation Steps

During the course of validating the App Volumes disaster recovery plan detailed above, the following actions were taken to install the App Volumes environments. While it is possible to first deploy with business continuity and then add disaster recovery to the solution, a BCP configuration is not required to deploy the disaster recovery solution.

1. Pre-Configuration

The same pre-configuration steps were performed for disaster recovery as were performed for business continuity with the following exceptions

- a. Determined names and IP addresses of four (4) App Volumes Manager servers and two (2) load balanced namespaces, one (1) in production, and the other in the DR environment. This encompassed six (6) IP addresses
- b. Four (4) Windows Server 2012 r2 virtual machines were deployed to act as App Volumes Manager servers and added to the domain. Two (2) of these servers were deployed in the production datacenter, and the other two (2) servers were deployed in the DR datacenter. App Volumes Manager servers were paired by the datacenter where they reside. For future reference, in the illustration below, SC-AppVolumes01 and SC-AppVolumes03 were paired together as a BCP pair, and SC-AppVolumes02 and SC-AppVolumes04 were paired together. Each pair was ultimately given a load balanced namespace, monitored and controlled by a F5 Local Traffic Manager, local to the datacenter where the servers resided



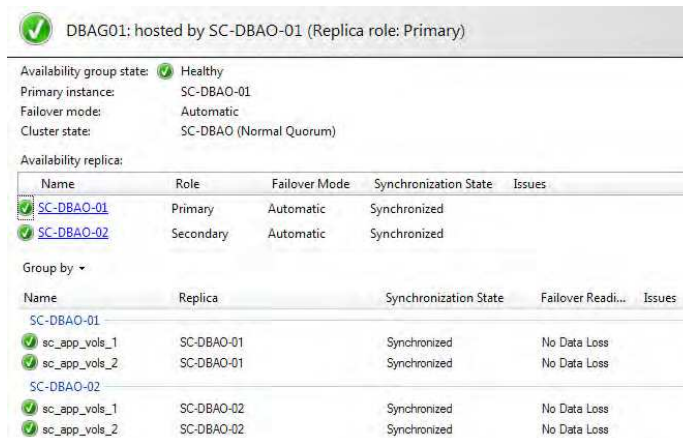
- c. An empty Microsoft SQL database was created for each environment. In this instance, sc_app_vols_1 was used for the production environment, and sc_app_vols_2 was used for the DR environment.
- d. Presented two (2) datastores in each vCenter environment for App Volumes AppStacks and templates which were later configured for storage group replication via the App Volumes Manager web interface.



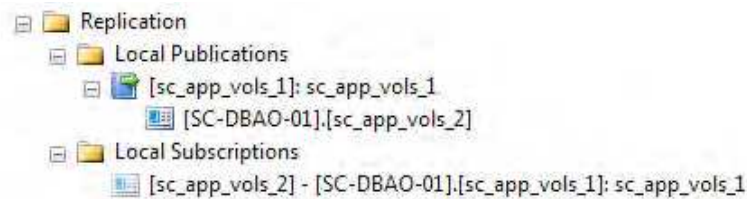
2. Installation of the App Volumes Environments

Each App Volumes environment was deployed for business continuity as detailed in the business continuity section of this document with the following exceptions

- a. Two (2) sets of App Volumes Manager servers were installed and configured to use their own external Microsoft SQL database in an AlwaysOn availability group. Individual namespaces “mm-appvolumes” and “wf-appvolumes” were selected for eventual load balancing for each environment.



- b. Transactional database replication was configured from select tables (see below) of the production App Volumes Manager server’s database as the publisher to the DR App Volumes server’s database as a subscriber.

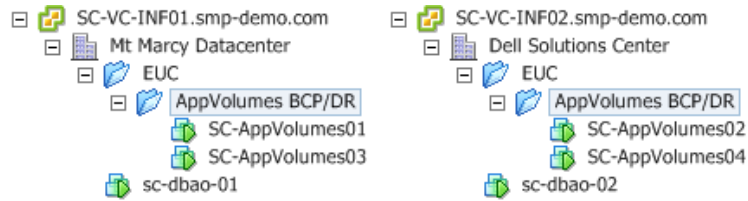


- available_locations
- binary_files
- groups
- keyword_assignments
- operating_systems
- org_units
- snapvol_apps
- snapvol_files
- snapvol_members
- snapvol_operating_systems
- snapvol_updates
- snapvol_versions
- snapvols
- storage_group_snapvols
- storage_groups
- storage_locations
- storage_members
- users
- zip_update_snapvols
- zip_updates

Notes:

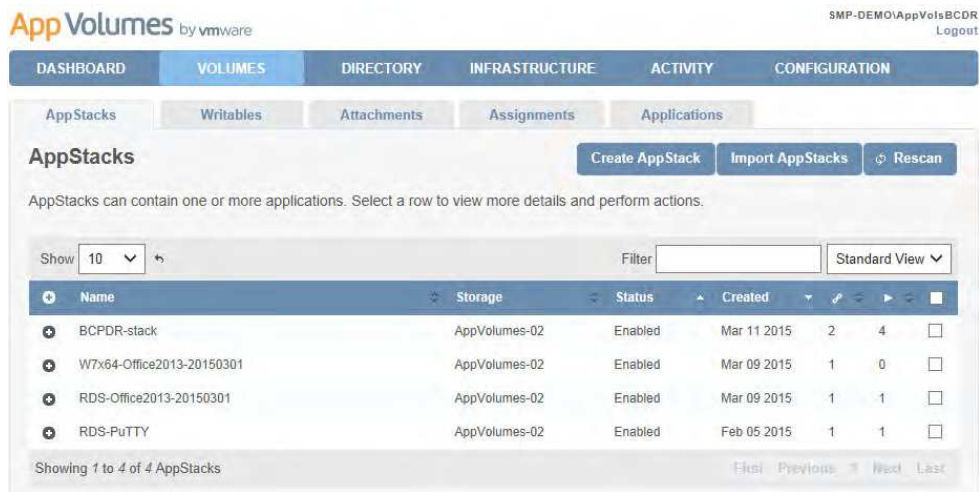
- More information surrounding the configuration of transactional database replication can be found here: <https://technet.microsoft.com/en-us/library/aa337437.aspx>
- The “Copy default value specification” must be set to true within the publisher’s articles for all tables
- While it is technically possible to log into a secondary App Volumes Manager and make changes such as adding assignments or AppStacks, this may cause the two SQL databases to become out of sync. Modifications to the secondary manager are strongly discouraged. It is best to simply consider the secondary manager as a subscriber of the primary. In the event that the primary manager is compromised and will not be returning to service, the secondary could be considered primary, database replication halted, and a new secondary could be created and configured.

- c. Multiple datastores of similar names were created for the use of AppStacks within each App Volumes environment. In our environment, these were named AppVolumes-01, and AppVolumes-02. Each environment was configured with these datastores, though the underlying storage for each environment was distinct.



NOTE: Datastores in App Volumes storage groups are referenced by name, therefore the datastores must have the same name in both vCenters

- d. App Volumes AppStacks were created in the production environment to include AppStacks assigned and attached to Microsoft Remote Desktop Services Hosts via Active Directory Organizational Unit, Users, and pools of VMware Horizon View desktops via Active Directory Organizational Unit where the production and DR pools share the same Active Directory Organizational Unit for their virtual machines



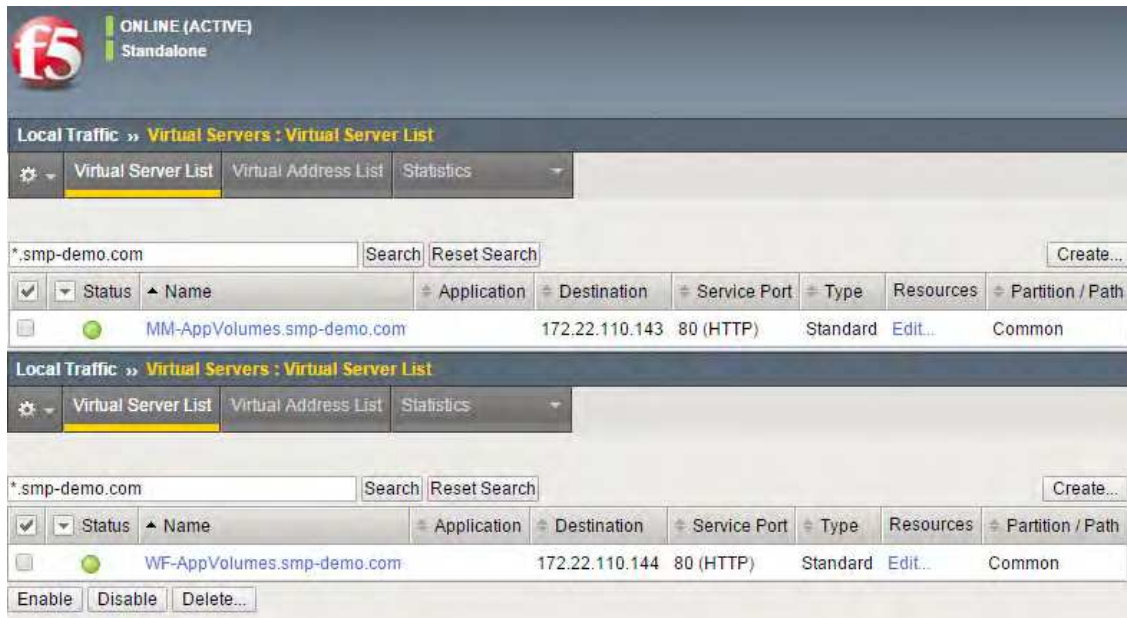
- e. App Volumes AppStacks were copied from one of the App Volumes replicated datastores in the production environment to one of the App Volumes replicated datastores in the DR environment using SCP from the ESXi command line interface, which took approximately 1 hour (Time was for 4, 20 GB AppStacks and 3 AppStacks and 3 AppStack Templates- effectively 140 GB)

```

/vmfs/volumes/8d01c809-d78fb906 # scp -r -C -o CompressionLevel=6 /vmfs/volumes/8d01c809-d78fb906/ap
pvols root@esx-r720a.smp-demo.com:/vmfs/volumes/75f35225-29cc38a1/
Password:
BCPDR-stack-flat.vmdk          100% 20GB 15.5MB/s 22:02
BCPDR-stack.vmdk              100% 528 0.5KB/s 00:00
RDS-PuTTY-flat.vmdk           100% 20GB 31.7MB/s 10:46
RDS-PuTTY.vmdk                100% 526 0.5KB/s 00:00
RDS-Office2013-20150301-flat.vmdk 100% 20GB 32.3MB/s 10:34
RDS-Office2013-20150301.vmdk 100% 540 0.5KB/s 00:00
W7x64-Office2013-20150301-flat.vmdk 100% 20GB 17.0MB/s 20:02
W7x64-Office2013-20150301.vmdk 100% 542 0.5KB/s 00:00
RDS-PuTTY.vmdk.metadata       100% 11KB 10.9KB/s 00:00
RDS-Office2013-20150301.vmdk.metadata 100% 10KB 10.1KB/s 00:00
W7x64-Office2013-20150301.vmdk.metadata 100% 11KB 11.2KB/s 00:00
BCPDR-stack.vmdk.metadata     100% 646 0.6KB/s 00:00

```


- f. Network topology based load balancing was configured between the two (2) App Volumes environments via F5's Big-IP Global Traffic Manager so that connections from different client networks will arrive at their respective App Volumes Management server



Notes:

- Geolocation based on topology will not work if using a stretched layer 2 network. In those instances, global availability may be the best option, as it will use the order specified in the member list based on status.
- Without the F5 Global Traffic Manager, it would be necessary to configure the App Volumes Agents with their own distinct App Volumes namespaces, and use multiple namespaces to access the App Volumes Manager interface.

Disaster Recovery Validation

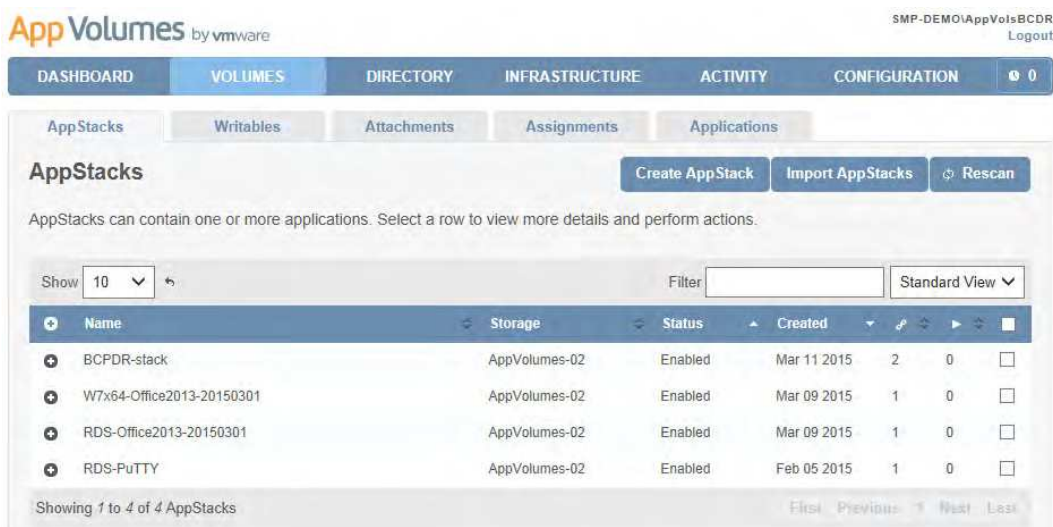
SMP tested the above configuration, and determined that App Volumes operated in the expected manner in a disaster recovery scenario. Details of the validation can be found below.

Disaster Recovery Validation Steps

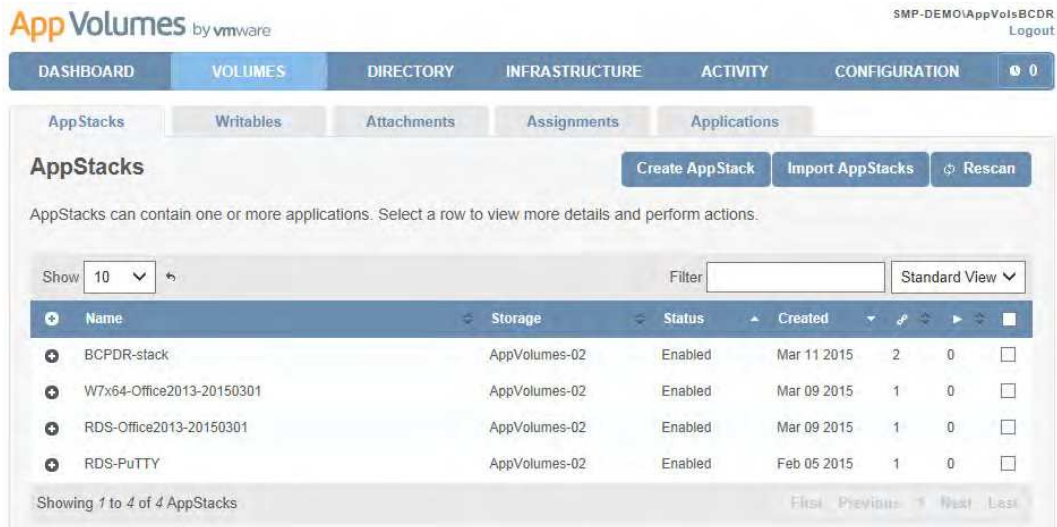
During the course of validating the App Volumes disaster recovery plan detailed above, the following actions were taken.

1. Environmental Verification

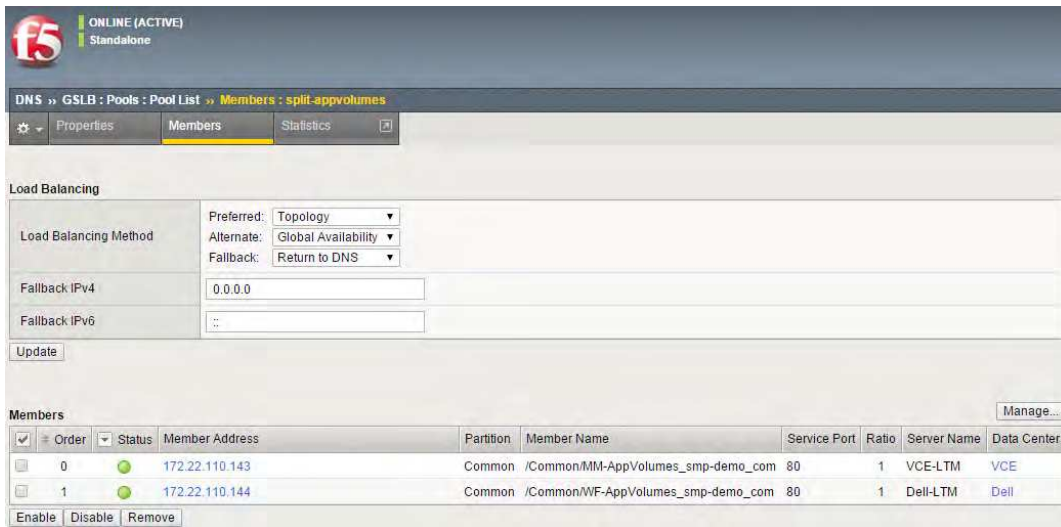
- a. App Volumes AppStack assignments and attachments were verified within the production environment



- b. App Volumes AppStacks were verified as being visible within the DR environment's App Volumes Management console



- c. Validated F5 Global Traffic Monitor health monitors



- d. Verified that the AppStack datastore contents are the same in both environments via the md5sum command in the ESXi command line interface

```

/vmfs/volumes/75f35225-29cc38a1/appvols/apps_bcdr/appstacks # find . -exec md5sum {} \;
60ac4ca68b7f72595377d2eb52ec4ab4 ./BCPDR-stack-flat.vmdk
b1ef075d956d9199df5eed405617225f ./BCPDR-stack.vmdk

/vmfs/volumes/8d01c809-d78fb906/appvols/apps_bcdr/appstacks # find . -exec md5sum {} \;
60ac4ca68b7f72595377d2eb52ec4ab4 ./BCPDR-stack-flat.vmdk
b1ef075d956d9199df5eed405617225f ./BCPDR-stack.vmdk

```

e. App Volumes AppStacks were verified within virtual desktops in the production App Volumes environment



2. Disruption of App Volumes production environment

a. Powered down the production App Volumes Management servers and Microsoft SQL server



b. The F5 Global Traffic Manager health monitor status was verified as detecting the production App Volumes environment offline, routing new management traffic to the DR environment

Members										Manage...
<input checked="" type="checkbox"/>	Order	Status	Member Address	Partition	Member Name	Service Port	Ratio	Server Name	Data Center	
<input type="checkbox"/>	0	❖	172.22.110.143	Common	/Common/MM-AppVolumes_smp-demo_com	80	1	VCE-LTM	VCE	
<input type="checkbox"/>	1	●	172.22.110.144	Common	/Common/WF-AppVolumes_smp-demo_com	80	1	Dell-LTM	Dell	

Enable Disable Remove

- c. Verified that the AlwaysOn Microsoft SQL availability group status detected the down state of the primary replica server, and failed over to the secondary

DBAG01: hosted by SC-DBAO-02 (Replica role: Primary) Last updated: 3/24/2015 4:29:36 PM

Availability group state: ✘ Critical --- Critical (1), Warnings (3) [Start Failover Wizard](#)

Primary instance: SC-DBAO-02 [View AlwaysOn Health Events](#)

Failover mode: Automatic [View Cluster Quorum Information](#)

Cluster state: SC-DBAO (Normal Quorum)

Availability replica:

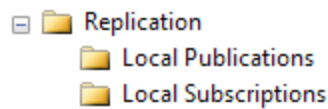
Name	Role	Failover Mode	Synchronization State	Issues
✘ SC-DBAO-01	Secondary	Automatic	Not Synchronizing	Critical (1), Warnings (1)
✔ SC-DBAO-02	Primary	Automatic	Synchronized	

Group by ▾

Name	Replica	Synchronization State	Failover Read...	Issues
SC-DBAO-01				
⚠ sc_app_vols_1	SC-DBAO-01	Not Synchronizing	Data Loss	Warnings (1)
⚠ sc_app_vols_2	SC-DBAO-01	Not Synchronizing	Data Loss	Warnings (1)
SC-DBAO-02				
✔ sc_app_vols_1	SC-DBAO-02	Synchronized	No Data Loss	
✔ sc_app_vols_2	SC-DBAO-02	Synchronized	No Data Loss	

3. Manual Actions Performed Upon Failover to App Volumes DR Environment

- a. Terminated transactional database replication from the production database to the DR database to ensure individuality of database data



- b. Initiated a Rescan operation within App Volumes to ensure that all necessary datastore and database functions were working properly

AppVolumes by VMware SMP-DEMO|AppVolsBCDR Logout

DASHBOARD VOLUMES DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

AppStacks Writables Attachments Assignments Applications

AppStacks [Create AppStack](#) [Import AppStacks](#) [Refresh](#)

AppStacks can contain one or more applications. Select a row to view more details and perform actions.

Show 10 ▾ Filter Standard View ▾

Name	Storage	Status	Created	...
BCPDR-stack	AppVolumes-02	Enabled	Mar 11 2015	2 0
W7x64-Office2013-2015				1 0
RDS-Office2013-2015				1 0
RDS-PuTTY				1 0

Showing 1 to 4 of 4 AppStacks

Confirm Rescan ✘

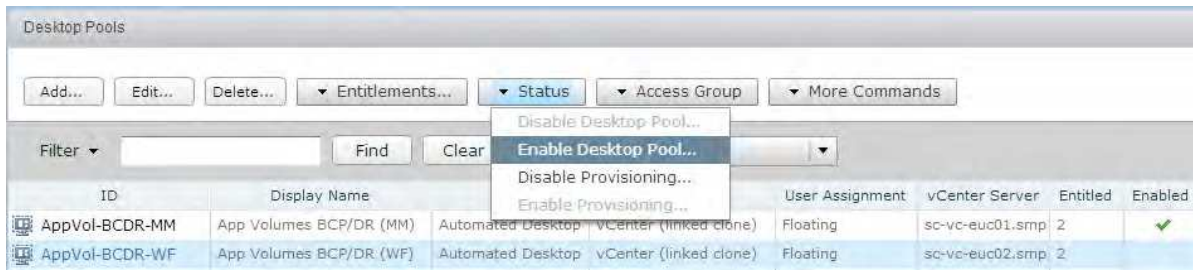
Rescanning will verify the existence and current state of each AppStack on the datastore. The scan only affects known AppStacks. Use the Import option when adding AppStacks.

Perform in the background

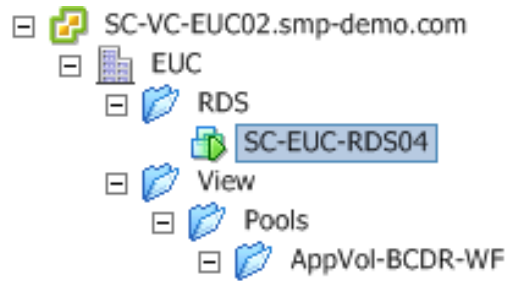
Wait for completion [Rescan](#)

⚠ Warning: The UI will issue an error after 10 minutes even if the task is still processing.

- c. Enabled the VMware Horizon View Pool to allow View to power up the DR environment's virtual desktops so that users can use them

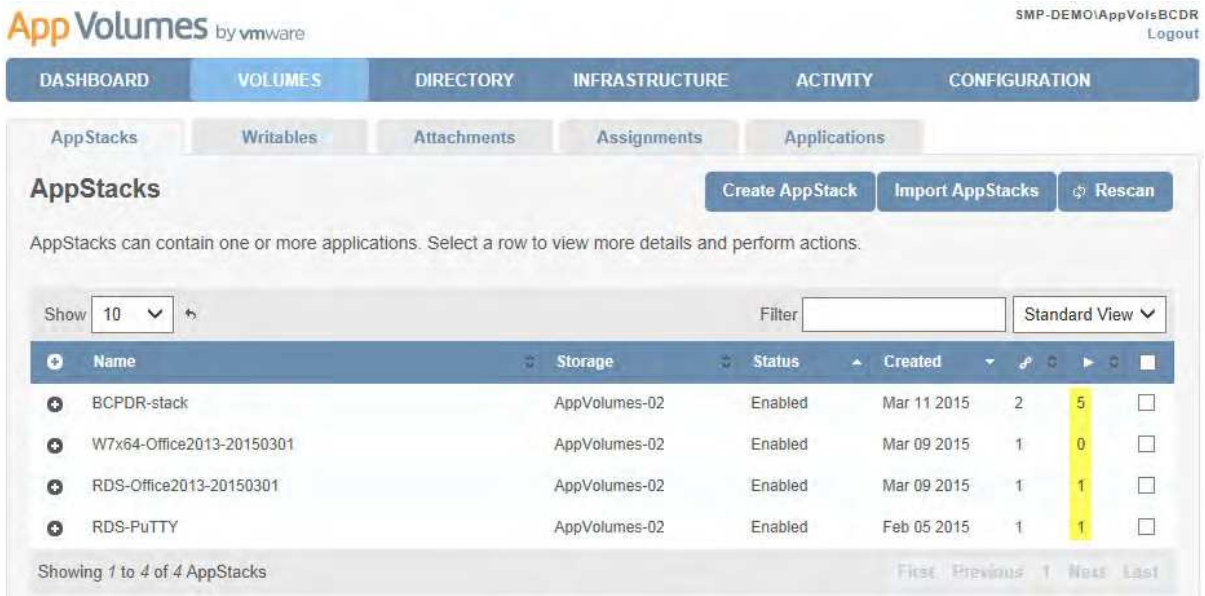


- d. Powered up the DR environment's RDS server

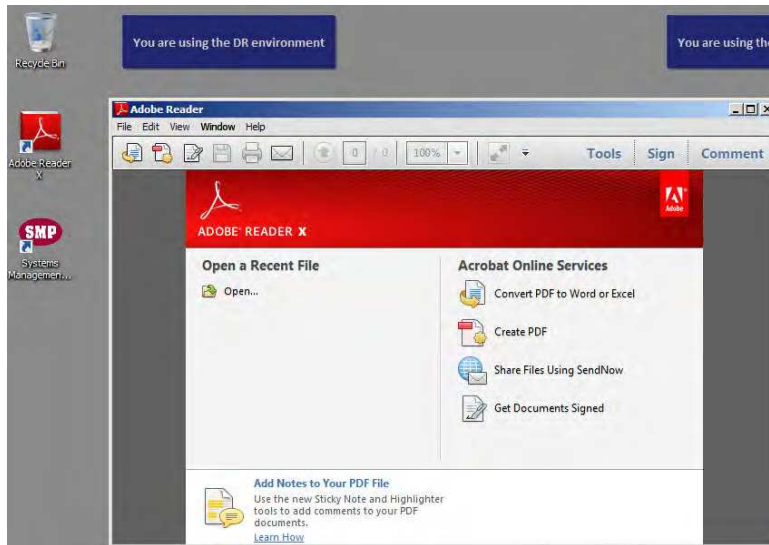


4. Verification of App Volumes After Failover to the DR Environment

- a. Refreshed the Volumes > AppStacks page to check AppStack attachment status



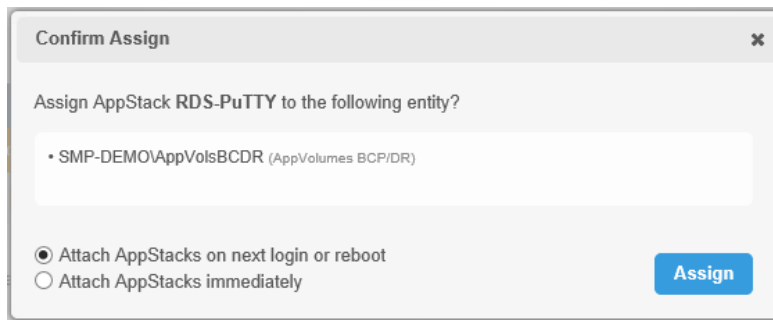
- b. Verified that the previously verified AppStack from the production environment was functional within the DR environment



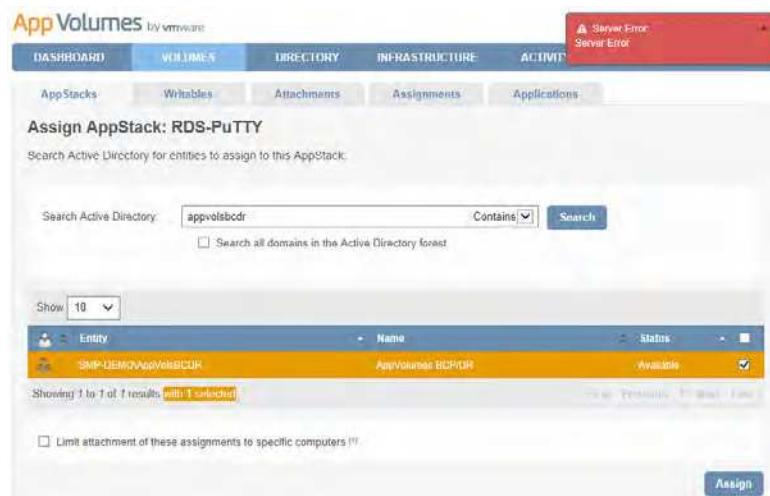
Note: The local policy of the DR pool's parent image included a mandatory tiled background notifying the user that they were using the DR environment

5. Verification of Read-Only App Volumes DR Environment

- a. Attempted to assign an existing AppStack to a user



- b. Received a red "Server Error" notification, and attempted change was not saved



Note: This error is to be expected when attempting to make changes within the DR environment, as it is a read-only environment

Disaster Recovery Variations

SMP also tested the following scenarios, and experienced the same level of success.

- The use of distinct namespaces for each App Volumes environment without the use of the F5 Global Traffic Manager. This method required the App Volumes Agents to be pointed at their individual App Volumes Manager namespace, and the use of multiple App Volumes Manager namespaces for administrative functions.
- The use of array-based storage replication between the production and DR environment instead of using an SCP file transfer. This method required similar storage in the production and DR environments, and the additional step of triggering a storage failover in order for the replicated datastores to be presented to Virtual Center within the DR environment.

Note: Array-based storage replication is the method that must be employed for writable volumes. Writable volumes should reside on distinct datastores apart from AppStack datastores. SQL transactional replication as detailed in this document will also replicate assignment information for writable volumes.

- The use of two (2) EMC VNXe storage arrays afforded the ability to leverage array based replication instead of the SCP file transfer. The configuration used for the testing included two (2) NFS volumes per location. The VNXe array replication was used to replicate one (1) of the volumes and leveraged the AppVolumes Storage group to ensure consistency between the two (2) datastores in each location. Lastly, we scripted the failure of a single site and the “bring online” of the volumes in the DR location.

Disaster Recovery Conclusion

SMP validated that a configuration including multiple BCP-ready App Volumes “pods” with datastore content synchronization, App Volumes Storage Groups, selective transactional database replication, and F5 load balancing and traffic management functions very well to ensure high availability of VMware’s App Volumes AppStacks in the event of a disaster recovery situation. Manual processes included in this configuration are datastore synchronization, and termination of the selective transactional database replication to ensure that the DR environment cannot be affected by any changes in the production environment.

Thought leadership,
wellness, excellence,
and creativity in
everything we do.
We're not your
typical IT company

This is an IT company?

Yes. One that looks at problems differently than most.

Yes, we provide IT solutions. Our engineers are the best and they have tremendous competence in virtualization and data center transformation, networking, unified communications, storage, security, and just about anything you need to make a difference in the way you run your business. With additional offices in Albany, NY, Pittsburgh, PA, and Pompano Beach, FL, we partner with the best in the business: Cisco, Dell, EMC, and VMware to name a few.

We take a fresh look at how we deliver IT solutions. How we serve you. How we come up with new ideas. How we do our work - and how to be the best at what we do. How we think. How we act. How we create success for ourselves and, more importantly, for you. At the end of the day, it's not just what we do; it's how we do it that really matters.

At SMP, we believe in two core philosophies: adventure and wellness. We think these are the key to doing amazing things for you: creating IT solutions that drive growth, innovation and efficiency.

We're well aware that these aren't the typical philosophies that drive IT companies. But then again, we're not the typical IT company. If we sound like someone you'd like to work with, we can't wait to talk to you.

WE CAN'T WAIT TO TALK TO YOU. Contact us today and discover even more about us at www.smp-corp.com.

ROCHESTER, NEW YORK
1020 John Street
W. Henrietta, NY 14586
585.475.0670
800.934.4790
Fax: **585.475.0909**

ALBANY, NEW YORK
125 Wolf Rd
Suite 401
Albany, NY 12205
518.435.0800
Fax: **518.435.0808**

PITTSBURGH, PENNSYLVANIA
2009 Mackenzie Way
Cranberry Crossroads Suite 100
Cranberry Twp, PA 16066
585.475.0670

POMPANO BEACH, FLORIDA
PO Box 10427
Pompano Beach, FL 33061
954.298.2937

BURLINGTON, VERMONT
47 Maple Street, Suite 202
Burlington, Vermont 05401
800.934.4790