vCloud Networking and Security – High Availability Primer

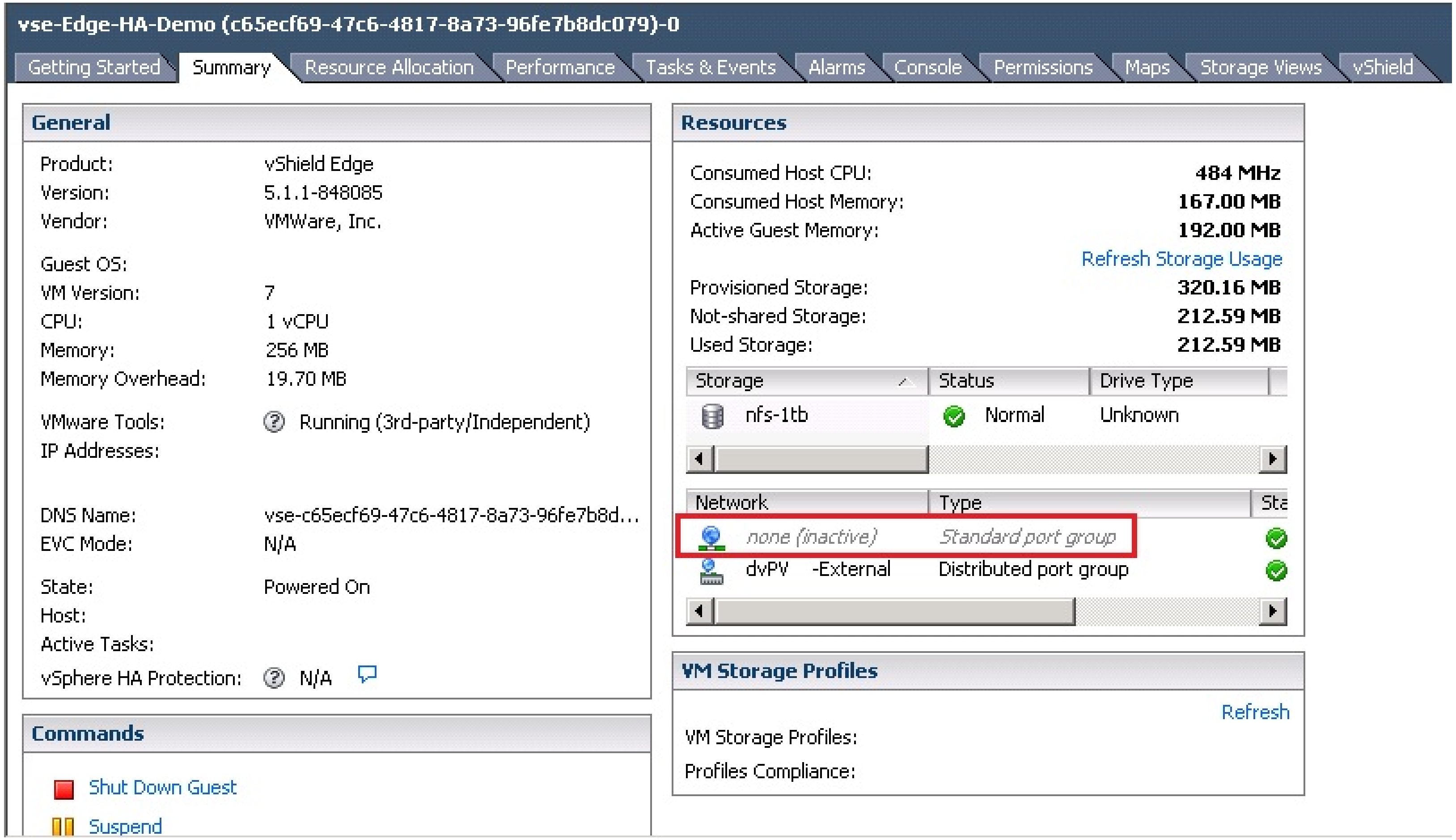
With vShield 5.1, we have seen that High Availability of vSM Service Virtual Machine has been introduced.

Today I am going to talk about how HA in Edge device works and shortly what it takes to configure it.

HA feature in Edge deploys 2 Edge Appliances per cluster, which runs in Active-Standby mode. Now, you may ask how about the configuration synchronization? Does it automatically do or need manual intervention?

vCenter Networking and Security Manager manages the life cycle of both peer’s and will push user configurations to both Edges simultaneously. The Active Edge device will push run-time state information to the Standby as well.

Edge HA peers talk to each other using an Internal IP Address and cannot be used for any other purpose except purely for HA purpose. This IP address gets allocated on one of the internal interfaces of the Edge.



vse-Edge-HA-Demo (c65ecf69-47c6-4817-8a73-96fe7b8dc079)-0

General

Product:	vShield Edge
Version:	5.1.1-848085
Vendor:	VMWare, Inc.
Guest OS:	
VM Version:	7
CPU:	1 vCPU
Memory:	256 MB
Memory Overhead:	19.70 MB
VMware Tools:	Running (3rd-party/Independent)
IP Addresses:	
DNS Name:	vse-c65ecf69-47c6-4817-8a73-96fe7b8d...
EVC Mode:	N/A
State:	Powered On
Host:	
Active Tasks:	
vSphere HA Protection:	N/A

Resources

Consumed Host CPU:	484 MHz
Consumed Host Memory:	167.00 MB
Active Guest Memory:	192.00 MB
Provisioned Storage:	320.16 MB
Not-shared Storage:	212.59 MB
Used Storage:	212.59 MB

Storage	Status	Drive Type
nfs-1tb	✓ Normal	Unknown

Network	Type	Sta
none (inactive)	*Standard port group*	✓
dvPV -External	Distributed port group	✓

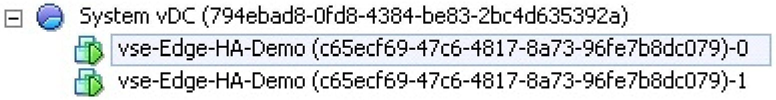
VM Storage Profiles

VM Storage Profiles:

Profiles Compliance:

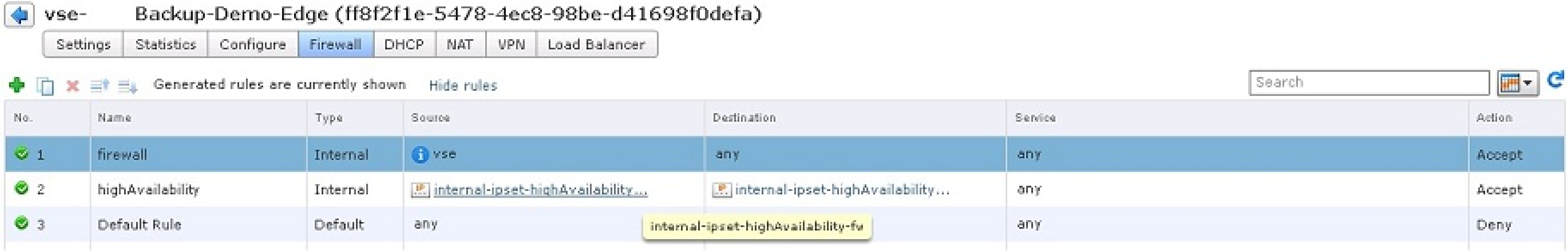
Commands

Below is a sample screen shot of how it looks when you deploy an Edge device in HA mode.



System vDC (794ebad8-0fd8-4384-be83-2bc4d635392a)
vse-Edge-HA-Demo (c65ecf69-47c6-4817-8a73-96fe7b8dc079)-0
vse-Edge-HA-Demo (c65ecf69-47c6-4817-8a73-96fe7b8dc079)-1

Also Edges must be allowed to communicate without L2 restrictions, that means there should be a Auto Firewall Rule generator which should allow the communication in between then. Yes, it is indeed there. Auto Rule generation automatically generates service rules to allow flow of control traffic in between peers.



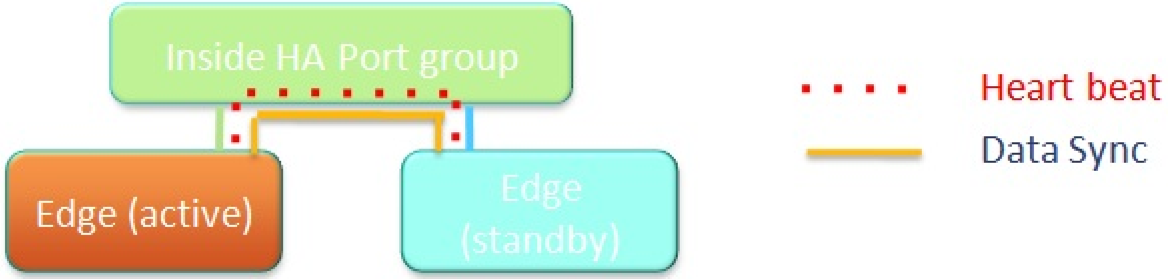
vse- Backup-Demo-Edge (ff8f2f1e-5478-4ec8-98be-d41698f0defa)

Generated rules are currently shown Hide rules

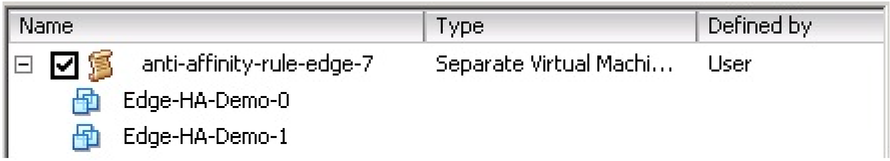
No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	highAvailability	Internal	internal-ipset-highAvailability...	internal-ipset-highAvailability...	any	Accept
3	Default Rule	Default	any		any	Deny

internal-ipset-highAvailability-fw

Now you may ask what are the types of traffic it carry out in between, it does exchange two types of Network traffic. They are Heartbeat and Data Sync.



So, when you deploy an Edge appliance in HA mode what it does in vSphere Level. It creates a anti affinity rule in the DRS cluster and places then separately in two different hosts within that cluster. A sample output is as below.



Name	Type	Defined by
⊟ ☑ anti-affinity-rule-edge-7	Separate Virtual Machi...	User
Edge-HA-Demo-0		
Edge-HA-Demo-1		

Now, you may wonder what or how should it behave when it does experience a failure. That means how should the Passive Edge behave when the active Edge fails over.

1. It should failover to the Passive Edge statefully for the firewall connections.
2. Load Balancer should synced to the passive and then fail over to the Passive node.
3. SSL VPN Client should reconnect automatically when it does a failover.
4. IPSec VPN tunnel should reconnect automatically when it does a failover.
5. After the failover Edge retains the DHCP allocation table state.