Technical Brief

Adding Zadara Storage to VMware Cloud on AWS

zadara

Revision History

Row	Version	Date	Description
1	1.0	26 Nov 2018	Initial release
2	1.1	15 Jan 2019	Updates for VMware style guide compliance, plus trademark acknowledgements

Introduction

VMware Cloud on AWS

Amazon describes VMware Cloud® on Amazon Web Services (AWS®) as an "integrated cloud offering jointly developed by AWS and VMware delivering a highly scalable, secure and innovative service that allows organizations to seamlessly migrate and extend their on-premises VMware vSphere®-based environments to the AWS Cloud running on next-generation Amazon Elastic Compute Cloud® (Amazon EC2®) bare metal infrastructure."

Problem

Unfortunately, the architecture of VMware Cloud on AWS (VMC-AWS) has, until now, made it impossible to present third-party storage located outside of Amazon's data centers to software-defined data center (SDDC) compute elements via AWS Direct Connect (DX). This restriction limited users' ability to present storage with full enterprise functionality to SDDCs hosted within AWS and forced users to scale storage and compute capacities in lock-step.

Purpose

This document describes a new method of leveraging VMware's network virtualization and security platform, VMware NSX®, to enable users to take full advantage of Zadara's data centric, location agnostic storage solution. In this example implementation, we will present Zadara iSCSI Block, SMB and NFS NAS to guest VM's running in a new SDDC within VMware Cloud for AWS.

Sample Use Cases

- Present the same Zadara file, block, and object storage to all compute elements, whether located on-premises, within one or more SDDCs, across multiple Virtual Private Clouds (VPCs), across multiple data centers, or across multiple cloud providers
- Scale storage capacity and compute elements independently
- Enhance availability with remote replication across regions, continents, or cloud providers
- Maximize application data security with user-managed encryption keys

- Ensure consistent high storage performance with 100% dedicated resources (i.e., no “noisy neighbors”)
- Match storage performance to application requirements when one size does not fit all

Requirements

- SDDC v1.5 or later (NSX-T functionality enabled)
- AWS permissions to launch Cloud Formation script
- Zadara Virtual Private Storage Array (VPSA) in the same region as the SDDC in use

Configuration Tested

- VMware Cloud on AWS using NSX-T (required)
- Single Host SDDC “starter configuration”[1]
    - 10 TB usable SSD capacity split between VSAN datastore to support management virtual machines (VMs - vCenter, NSX, etc.) and Workload data store to host application VMs
- VMware SDDC v1.5.0.29
- NSX flags
    - enableNsxtDeployment
    - enableNsxtCspAuth
    - reverseProxyUrl
    - installNsxtCert
    - enableNsxtTransitiveRouting
    - dxForMgmtApplianceAndWorkload
- Zadara 1000 engine, v18.07-104 (any appropriately sized engine may be used)
- Zadara VPSA configured with (any valid VPSA configuration may be used)
    - 8 x 10 TB SATA HDDs
    - Extended mirrored SSD cache (480 GB)

[1] https://cloud.vmware.com/vmc-aws/get-started

Overview

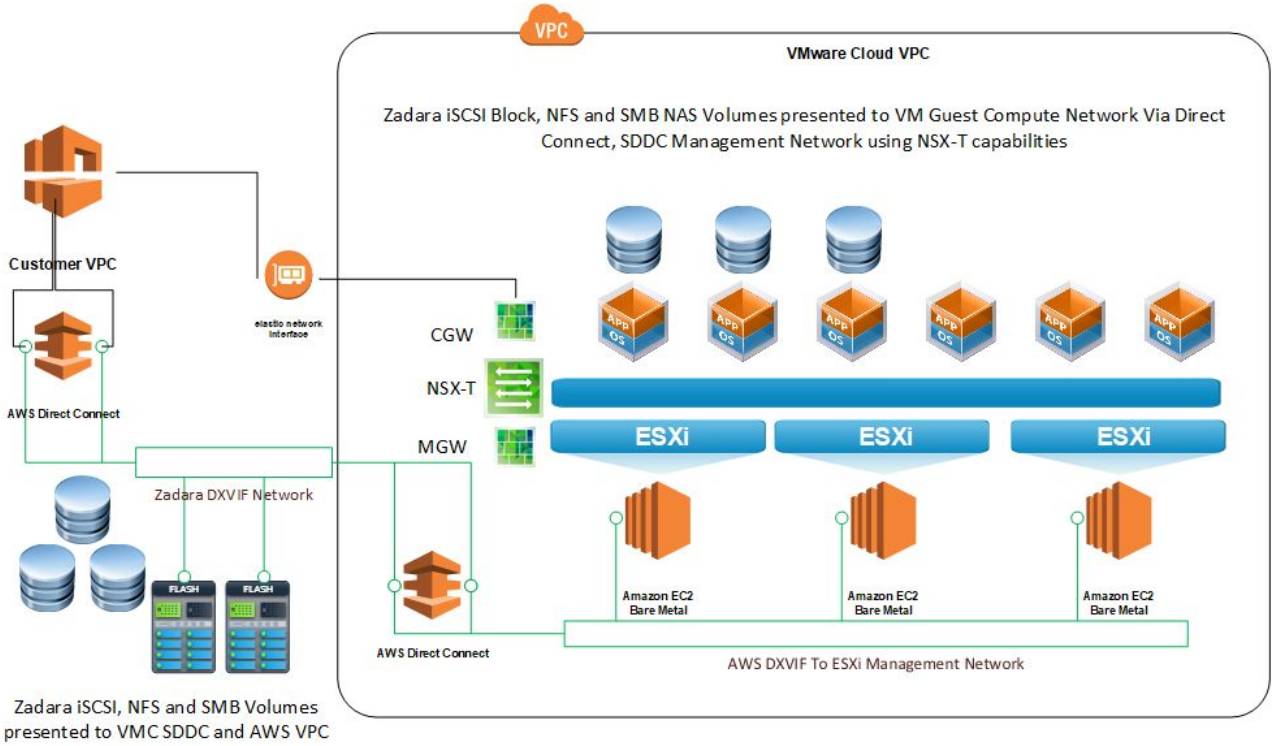


Figure 1. Overview diagram

Walkthrough

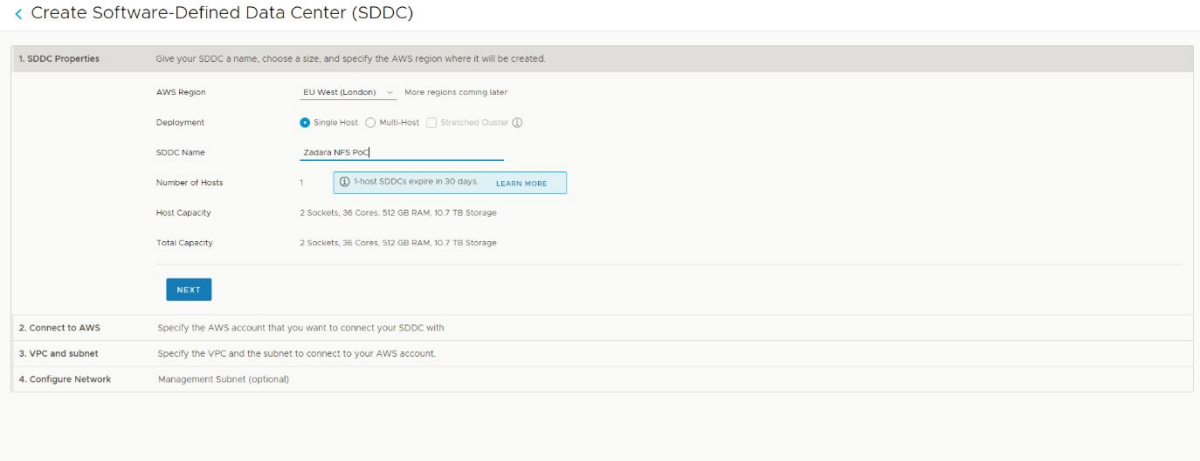
Planning Notes

- Make sure that you have Cloud Formation rights in your AWS account
- Review the latest Zadara Setup Guide (http://guides.zadarastorage.com/)
- By default, the SDDC will utilize a 10.0.0.0/20 network for management functions. Please ensure that this is not in use
- Zadara VPSAs will typically be on a 172.x.x.x network, depending upon region. However, Zadara supports custom networks and this can be set to a customer specific range if required

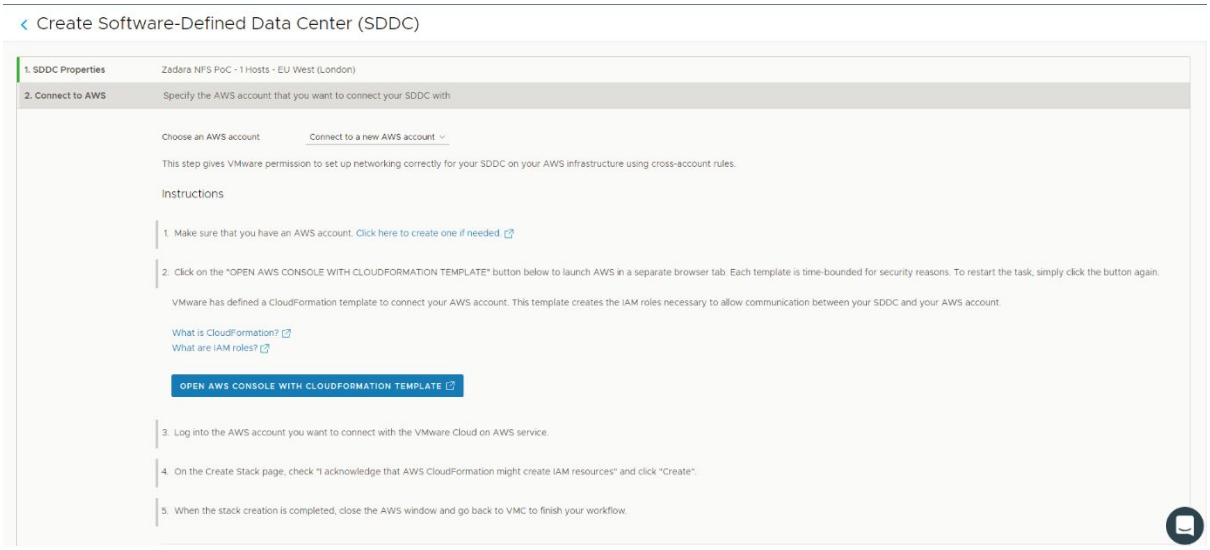
Steps

1. Create an organization account on AWS and VMware Cloud
2. CRITICAL: make sure to request that the NSX-T flags are enabled on your organization before proceeding
3. Request a new SDDC at https://cloud.vmware.com/vmc-aws
4. Step through the SDDC creation wizard

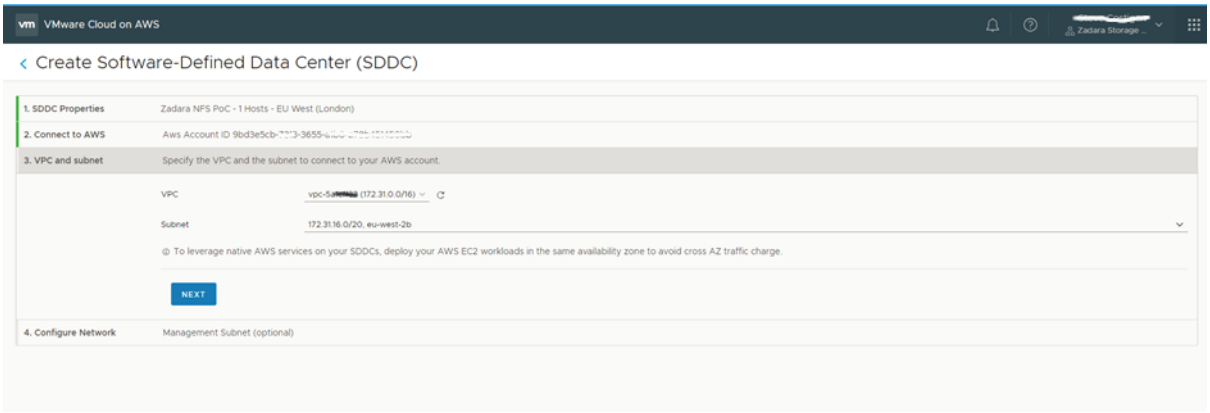
    a. Configure basic SDDC properties.



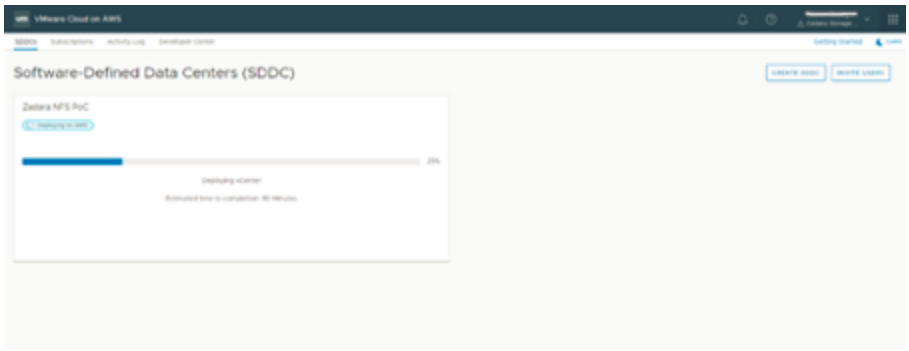
b. Link AWS account (you must have cloud formation rights).

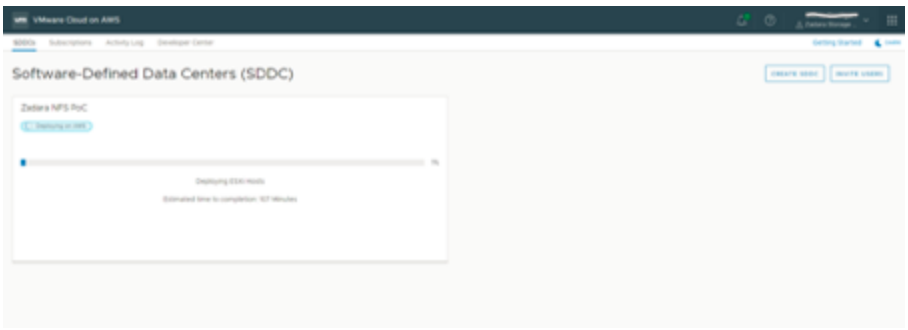


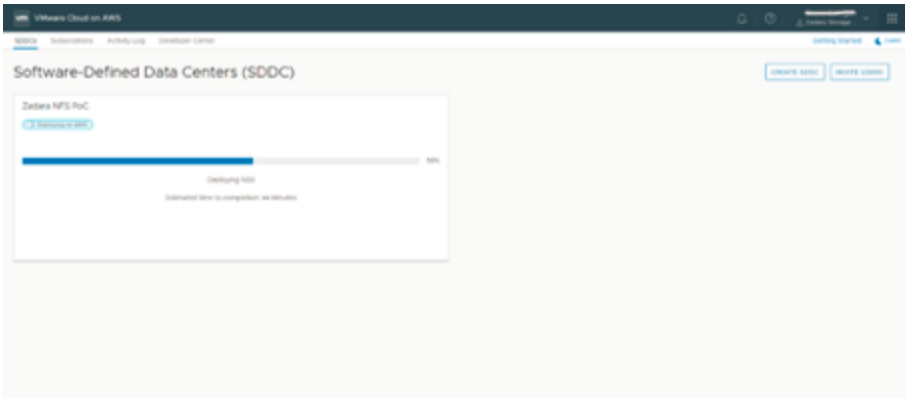
c. Identify the VPC and subnet that the SDDC will be connected to.



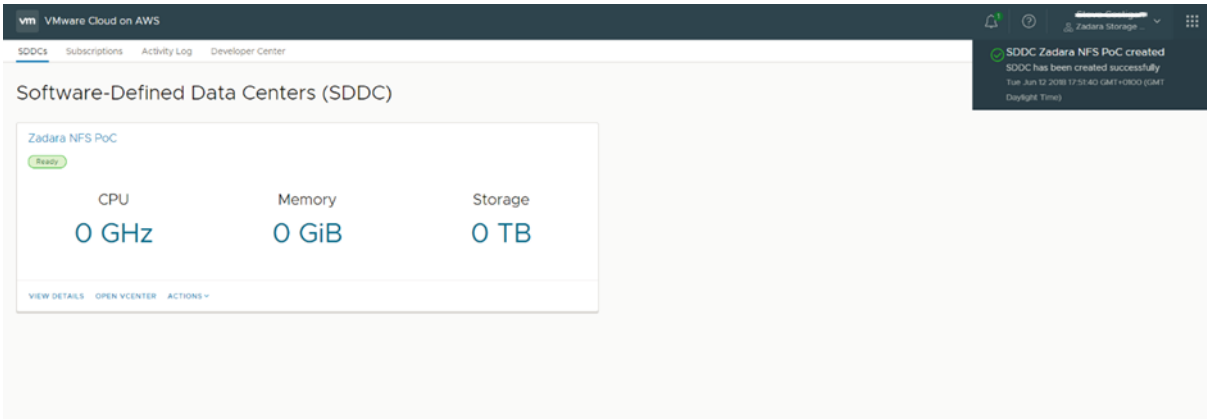
d. When configuration has been completed and submitted, the provisioning progress screen is presented (the bar will move).



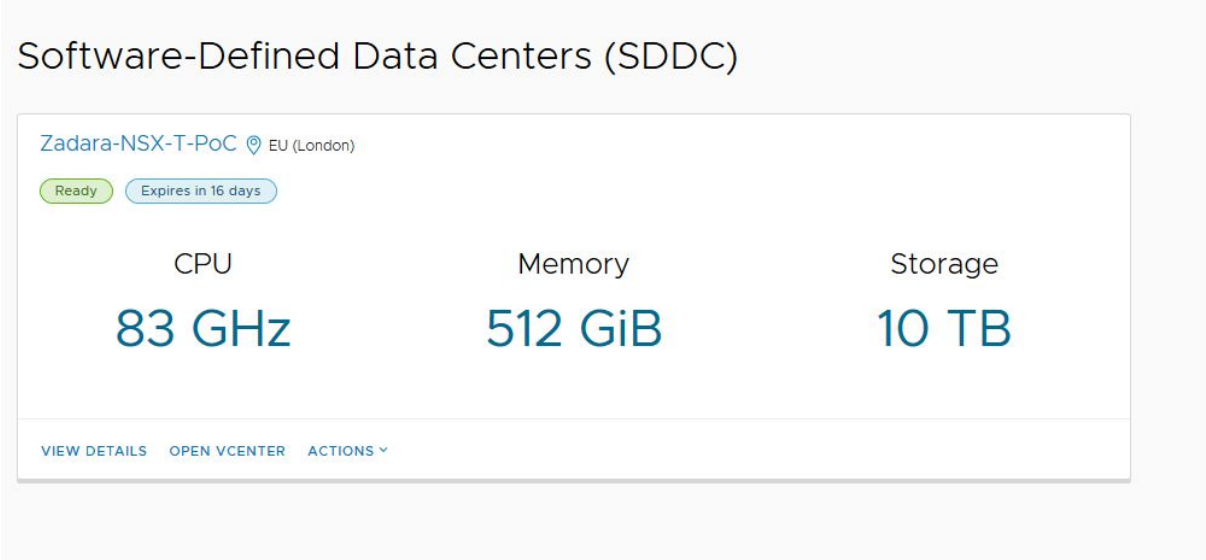




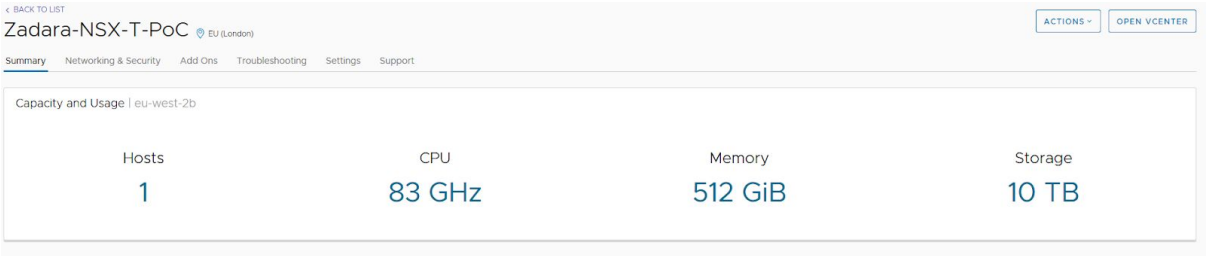
e. When the process completes, you should see the following:



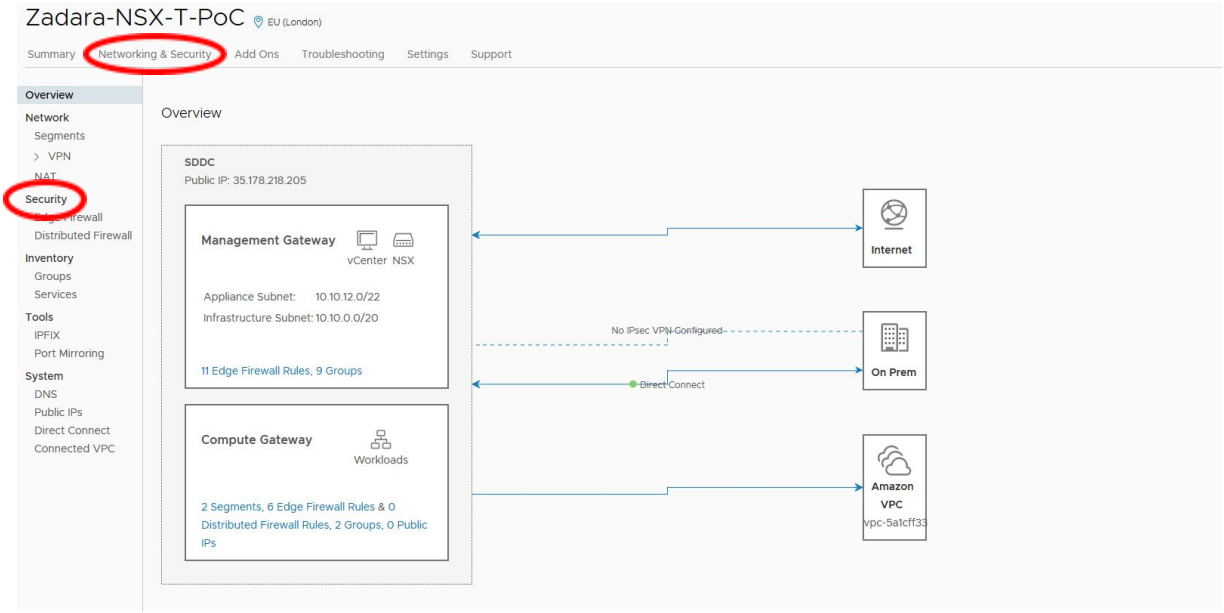
5. After logging into VMware in AWS console you will see the following:



6. View Details allows you to view a summary and set the Networking firewall rules for initial setup

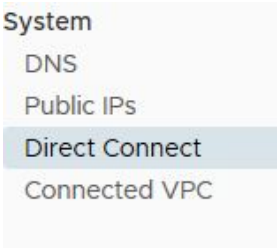


7. Clicking on Networking & Security displays an overview of connections



8. In the Security Tab, define access rules for management and access to vCenter (by default everything is denied). Create New Objects for specific IP's to allow access and grant access to vCenter, e.g.

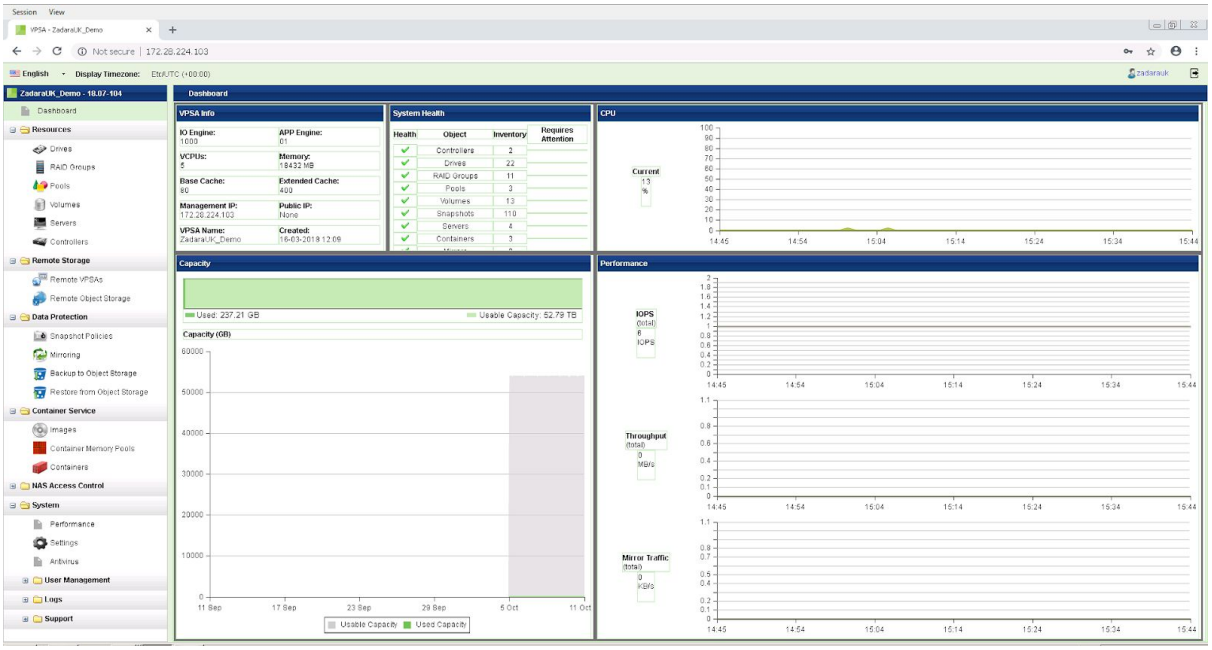
9. Click on Direct Connect on the Networking & Security tab to get the AWS account ID.



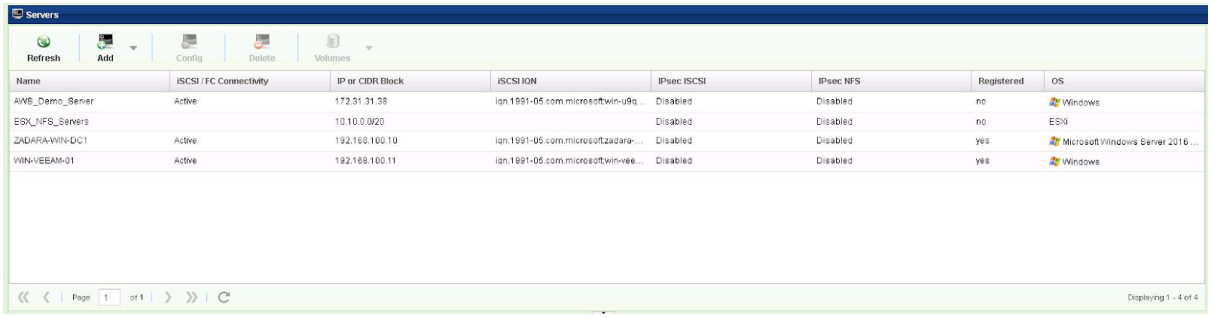
10. Open a new browser window to https://manage.zadarastorage.com and request a new AWS VPSA (make sure it's located in the same AWS region as the just-deployed SDDC).
11. Send an email to Zadara support (support@zadarastorage.com) and outline the VPSA name, your account name, and the AWS account ID (from step 9, above).
12. When you receive confirmation that the VPSA is ready, go back to the SDDC Direct Connect pane and accept the two new virtual interfaces.

13. After a few minutes you should see something similar to this, showing the learned and advertised routes from the SDDC and the Zadara sides.

14. Ensure you have created objects for the Zadara VPSA Network and have configured firewall rules to allow traffic to flow between the Compute Network and the Zadara Network via the SDDC Management Network and Direct Connect Network
15. To enable VPC to VM Compute connectivity make sure that two-way network traffic can flow between EC2 instances in the VPC and the SDDC via the Elastic Network Interface (ENI). Ensure that the ACL Rules applied to the ENI Interface allow two way traffic between the two networks.
16. If VPC EC2 compute instances require access to the same storage types (e.g., iSCSI/Block, CIFS/SMB, Object), then additional DX Virtual Interfaces (VIFs) will need to be provisioned – speak to your Zadara Account Manager to organise this.
17. Log into the newly provisioned VPSA to make sure the dashboard is available.



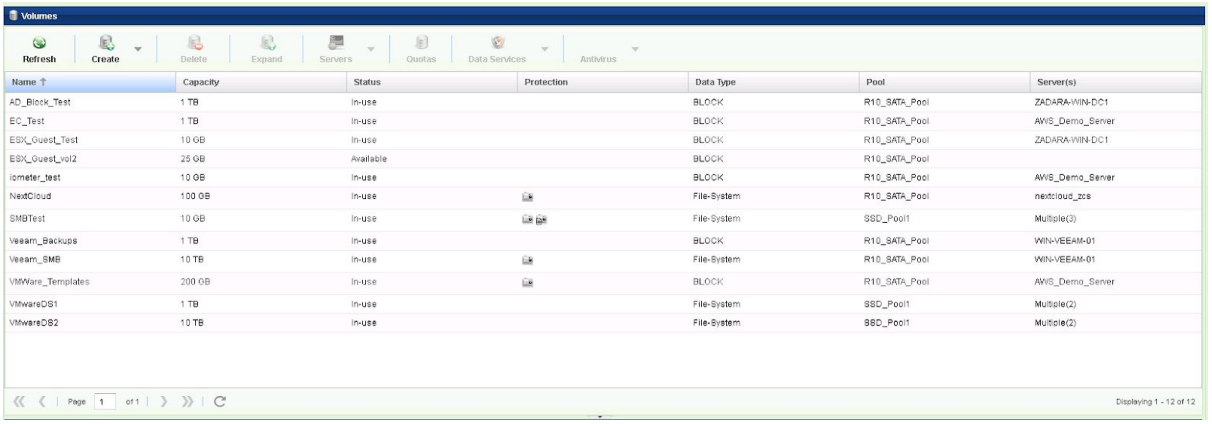
18. Click on the servers tab to register new clients and setup access volumes.



In the above example, you can see we have defined access to the same array via iSCSI and NAS in both the VMware compute network on 192.168.100.0/24 and the AWS VPC 172.31.31.0/24.

Note: Servers can be registered manually or automatically via a setup script from the VPSA

19. Lastly, we can see the range of Volumes presented from the configured VPSA



Conclusion

We have demonstrated how data residing on Zadara storage can be simultaneously presented to applications running in VMware Cloud for AWS environments, AWS EC2 instances, and on-premises servers. This data centric, location agnostic approach enables Zadara customers to enhance data availability, accelerate application performance, optimize flexibility, and capture maximum value from data.

To further explore Zadara solutions for AWS, please visit https://www.zadara.com/sol_aws.php or call us at +1-949-251-0360 (US) or +1-949-284-0713 (International).

Transform your business with zero-risk enterprise storage.

Zadara transforms storage-related costs from a variable mix of equipment and management expenses to a predictable, on-demand, pay-per-use, elastic service that greatly simplifies planning, streamlines budgeting, and improves return on investment (ROI). Find out how zero-risk enterprise storage can help transform your business. Call or email today.