Lenovo

Disaster Recovery Solution for Lenovo ThinkAgile VX with VMware Cloud on AWS

Provides a deep dive into the architecture and the recommended best practices for the solution

Helps answer key questions when architecting a disaster recovery solution

Provides details on the different components used in this solution

Describes how to test and implement a disaster recovery solution

Bhavin Shah, Lenovo

Prasad Kalpurekkal, VMware

Akshay Pathak, VMware

LENOVO PRESS

Abstract

Lenovo® ThinkAgile™ VX Series and VMware Cloud on AWS with VMware Site Recovery Service helps you build a resilient disaster recovery solution. This document provides a deep dive into the architecture and the best practices that should be followed when implementing the solution. It will also help answer key questions needed to implement a disaster recovery solution while describing the different software components needed to test and implement this solution.

The intended audience for this document includes sales engineers, field consultants, IT managers and partner engineering personnel. This document is also intended for customers who want to take advantage of all the best practices and guidelines for creating a resilient disaster recovery solution using ThinkAgile VX and VMware Cloud on AWS.

The paper is the result of a collaboration between Lenovo and VMware.

Contents

Introduction

Over time, IT organizations have increasingly taken an active role in driving business growth. They have come a long way from simply being a cost center to having a seat at the table. One of the key responsibilities IT organizations have, is to ensure that business critical applications are always online and available. In addition to making these applications robust and highly available, IT administrators also need to plan for disaster events. Although infrequent, disasters can have a long term impact on the success of the business.

Architecting a disaster recovery solution, that is both resilient and cost-effective can be challenging at times, and you should start the journey by answering these questions.

- What are my Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements?
- Which are the most business critical applications that my team is responsible for?
- What steps do I need to take to create reliable Recovery plans?
- How can I maintain a cost-effective secondary site for recovery?
- Who is responsible for maintaining the secondary site to ensure that it is able to run the business critical applications in case of a disaster event?

Lenovo ThinkAgile VX along with VMware Cloud on AWS with VMware Site Recovery Service helps you answer these questions and create a fool-proof, reliable, and cost-effective disaster recovery solution.

This document provides a deep dive into the architecture and best practices that should be followed when implementing this solution for your business.

For further information about VMware Cloud on AWS, go to:

https://cloud.vmware.com/vmc-aws

For further information about Lenovo ThinkAgile VX, go to:

https://www.lenovo.com/us/en/data-center/software-defined-infrastructure/ThinkAgile-VX-Series/p/WMD00000340

Solution technology

This disaster recovery solution is built on Lenovo ThinkAgile VX at the primary (protected) site and VMware Cloud on AWS at the secondary (recovery) site. Both sites are configured and connected using best practices from both Lenovo and VMware.

The software components listed in Table 1 were used in the solution validation phase.

Table 1 Solution components

Component	Version	Primary Site (ThinkAgile VX)	Secondary Site (VMC)
ESXi Hypervisor	6.7	Available with Lenovo ThinkAgile VX	Available as part of the SDDC deployment
VMware vSAN	6.7	Available with Lenovo ThinkAgile VX	Available as part of the SDDC deployment
NSX Manager	6.4.1	Additional Configuration needed	Available as part of the SDDC deployment

Component	Version	Primary Site (ThinkAgile VX)	Secondary Site (VMC)
Site Recovery Manager	8.1	Additional Configuration needed	Need to enable the Site Recovery Service Add-On
vSphere Replication	8.1	Additional Configuration needed	Included in the Site Recovery Service Add-On

Figure 1 is a high level diagram showing the two options you have for connecting your data center running ThinkAgile VX-based SDDC and the VMware Cloud on AWS SDDC.

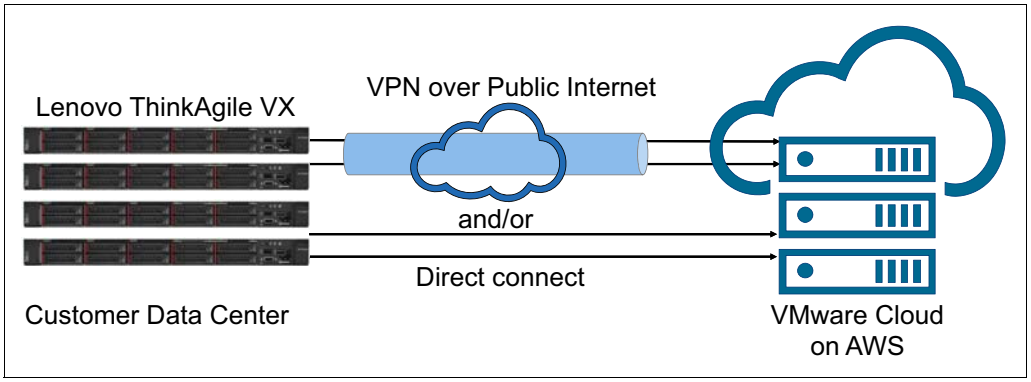

Figure 1 Solution overview

For the purposes of this document, we used an IPsec VPN Tunnel to connect our On-Premises environment to the VMware Cloud on AWS SDDC. We describe the steps to configure the solution in “Solution configuration” on page 9.

Use case summary

This document describes using Lenovo ThinkAgile VX, VMware Cloud on AWS, and VMware Site Recovery Service to provide a reliable, scalable, and cost-effective disaster recovery solution for the following use cases:

- Disaster Avoidance: VMware Site Recovery helps you perform planned migration operations of the applications running in your primary site when you are anticipating downtime.
- Disaster Recovery: Unexpected site failures aren’t frequent, but they are a possibility and you need to plan for that. VMware Site Recovery helps you automate and orchestrate the recovery of your applications to the VMware Cloud on AWS environment.
- Upgrade and Patch Testing: Having a secondary environment with copies of your applications can be helpful when you want to test upgrades and patches without affecting your production workloads.

Lenovo ThinkAgile VX

Lenovo ThinkAgile VX Series appliances combine virtualized compute, storage, and networking resources into a single system, which allows you to focus on your business rather than how to build out your infrastructure. Built on ThinkSystem™ servers, rated #1 in reliability and customer satisfaction, ThinkAgile VX Series has the configuration flexibility to meet all your application needs and quickly scale your infrastructure to grow with your business.

ThinkAgile VX also includes the following key features:

- ThinkAgile VX appliances are powered by VMware vSAN, which allows you to “pay-as-you-grow” by scaling non-disruptively from 3 to 64 hosts per cluster.
- Advanced capacity management including deduplication, compression, and erasure coding (RAID 5/6), which helps deliver greater storage utilization with dramatically lower storage capacity and costs.
- Cost-efficient hybrid and performance-optimized all-flash storage configurations to meet various workload demands.
- Centralized management with provisioning, administering, and monitoring of virtual resources across multiple hosts and clusters using VMware vCenter, and of physical hosts using Lenovo XClarity™. The Lenovo XClarity Integrator plugin for vCenter eliminates maintenance downtime by coordinating non-disruptive rolling firmware updates reboots, and a variety of hardware management tasks

For more information on how Lenovo ThinkAgile VX series appliances can help you build a reliable SDDC environment, see the ThinkAgile VX datasheet:

https://lenovopress.com/datasheet/ds0023-lenovo-thinkagile-vx-series

For details about the offerings, see the ThinkAgile VX Product Guides:

https://lenovopress.com/servers/thinkagile/vx-series#rt=product-guide

VMware Cloud on AWS

VMware Cloud on AWS is an enterprise-class software-defined data center (SDDC) offering. powered by VMware Cloud Foundation. VMware Cloud on AWS is a unified SDDC platform that integrates the following components:

- VMware vSphere for compute
- VMware vSAN for storage
- VMware NSX for networking
- VMware vCenter Server management

This service is optimized to run on dedicated, elastic, bare-metal AWS infrastructure and work seamlessly with on-premises VMware-based private clouds and advanced AWS services.

VMware Cloud on AWS is sold, operated and supported by VMware as an on-demand, flexible consumption cloud service that enables cloud migration and portability, increases IT efficiency, and creates new opportunities for customers to leverage a hybrid cloud environment. To get started with VMware Cloud on AWS, go to:

http://cloud.vmware.com/vmc-aws

VMware vSAN in VMware Cloud on AWS

The primary storage for the VMware Cloud on AWS SDDC cluster is backed by VMware vSAN (Virtual SAN) in an all-flash configuration. Each host is equipped with eight NVMe devices and a total of 10TB of raw capacity, not including the cache capacity of the vSAN datastore.

A basic four node cluster of 32 NVMe encrypted devices provides 40 TB of raw capacity, for VMs to consume. Each host has two vSAN disk groups, each using three NVMe drives as the

capacity tier and one NVMe drive as the write-caching tier. The default storage policy setting for fault tolerance is RAID 1, but if you have a larger cluster, you can use RAID 5 or 6.

VMware Cloud on AWS introduces a new vSAN capability that provides two logical datastores – one for management VMs and the other for customer workload VMs. To provide data security, all local storage NVMe devices are encrypted at the firmware level by AWS.

VMware NSX in VMware Cloud on AWS

VMware Cloud on AWS leverages NSX for network virtualization. NSX is optimized to work with vSphere, integrates with AWS Virtual Private Cloud (VPC) networks, and provides network attachment for user VMs. When you create a VMware Cloud on AWS SDDC, VMware automatically installs NSX Manager and creates two Gateway Instances for the SDDC environment: a Management Gateway (MGW) and a Customer Gateway (CGW).

The Management Gateway (MGW) utilizes an NSX Edge instance that connects to the vCenter Server. You can configure firewall rules, an IPsec VPN, and DNS for the management gateway.

The Compute Gateway (CGW) utilizes an NSX Edge instance and a distributed logical router (DLR) to enable ingress and egress of VM network traffic. You can configure firewall rules, inbound NAT, VPN connections, DNS, and public IP addresses for the Compute Gateway

An IPsec layer 3 VPN is set up to securely connect the on-premises vCenter Server instance with the management components running on the VMware Cloud on AWS SDDC cluster. A separate IPsec Layer 3 VPN is set up to establish connectivity between the on-premises workloads and the VMs running inside the VMC SDDC cluster.

Figure 2 shows how the networking is configured in VMware Cloud on AWS.

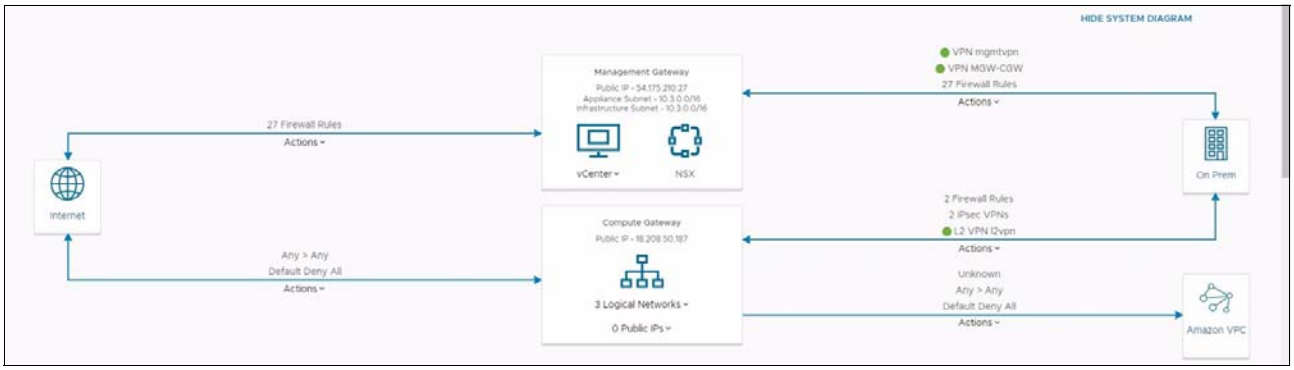

Figure 2 Networking configuration with VMware Cloud on AWS

After creating the IPsec VPN tunnels for both the management and compute gateways, you can create firewall rules to allow all the required traffic. You can also use the Firewall Rules Accelerator to create the basic rules required for vCenter management and Site Recovery Manager Connectivity.

VMware vCenter Hybrid Linked Mode

VMware Cloud on AWS is designed to provide single pane of glass monitoring for hybrid cloud management. The new Hybrid Linked Mode (HLM) feature enables on-premises and in-cloud vCenter Server instances to share data while maintaining some level of administrative separation.

Hybrid Linked Mode enables users to complete the following functions:

- Log in to the vCenter Server instance in their SDDC using their on-premises credentials
- View and manage the inventories of both their on-premises data center and the cloud SDDC from a single vSphere client interface
- Cold-migrate workloads between their on-premises data center and the cloud SDDC

For the detailed configuration of Hybrid Linked Mode (HLM) for VMware Cloud on AWS, see the VMware article *Configuring Hybrid Linked Mode (HLM) for VMware Cloud on AWS*, available from:

https://cloud.vmware.com/community/2017/11/02/configuring-hybrid-linked-mode-hlm-vmware-cloud-aws/

For the purposes of this document, we downloaded and deployed the VMware Cloud Gateway Appliance on the ThinkAgile VX-based SDDC stack On-Prem to enable Hybrid cloud management.

VMware Site Recovery service

The VMware Site Recovery service expands and simplifies traditional disaster recovery operations by delivering on-demand site protection across a common, vSphere-based operating environment from on-premises to the cloud. The service protects workloads between on-premises data centers and VMware Cloud on AWS, as well as between different instances of VMware Cloud on AWS.

To get started with VMware Site Recovery on VMware Cloud on AWS, go to the VMware Cloud on AWS Add-ons page:

https://cloud.vmware.com/vmc-aws/add-ons

VMware Site Recovery uses the host-based replication feature of VMware vSphere Replication and the orchestration of Site Recovery Manager.

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) automates every aspect of executing a recovery plan, including testing, failover to the secondary site and failback to the production site. SRM accelerates recovery and eliminates the risks involved with manual processes.

SRM integrates with the underlying vSphere replication technology to provide policy based management, non-destructive testing and orchestration of the recovery plan. It restores the availability of virtual machines in case of a disaster situation, so, if the primary site goes down, you can easily recover your virtual machines on the DR site.

Figure 3 shows an architectural view of the different components used in SRM.

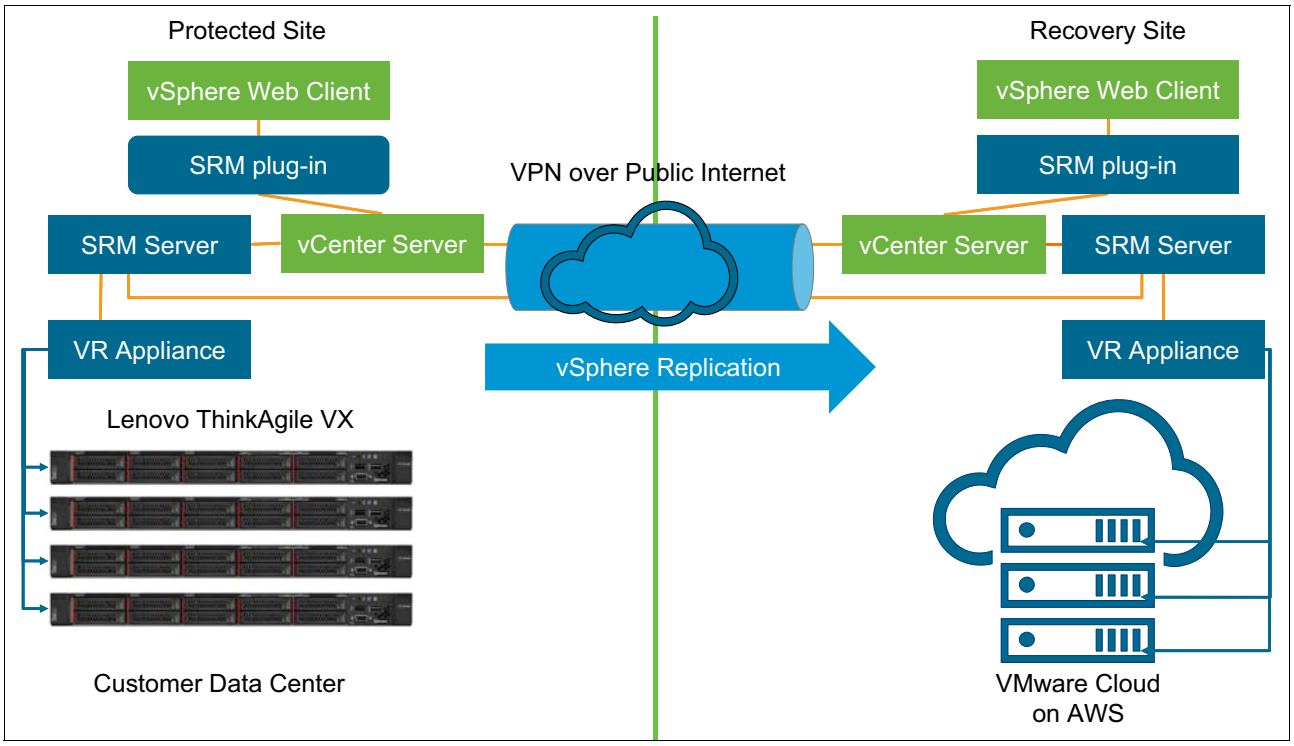

Figure 3 VMware Site Recovery Manager architectural view

SRM is deployed on both the protected site and recovery site SDDC Infrastructure. You can create Site Pairs using SRM Server instances located both On-Prem and within VMware Cloud on AWS. Site Recovery Manager works with VMware vSphere Replication to protect individual virtual machines running on a host.

You can use Site Recovery Manager to implement different types of recovery scenarios from the protected site to the recovery site. Recovery scenarios include:

- Planned migration

  The virtual machines are gracefully migrated from the protected site to the recovery site in an orderly fashion preventing any data loss. For a planned migration to succeed, both sites must be running and fully functioning.

- Disaster recovery

  In a disaster recovery scenario, the protected site could go offline unexpectedly, in such a scenario, failure of operations on the protected site is reported in the recovery site SRM instance, so the administrator may initiate a recovery plan which automatically powers on the virtual machines on the recovery site.

In either scenario, SRM orchestrates the recovery process with the replication mechanisms, to minimize data loss and system down time, as follows:

1. At the protected site, Site Recovery Manager shuts down virtual machines cleanly and synchronizes storage, if the protected site is still running.
2. Site Recovery Manager Powers on the replicated virtual machines at the recovery site according to a recovery plan.

A recovery plan specifies the order in which virtual machines start up on the recovery site. It also helps specify network parameters, such as IP addresses, and can contain user provided scripts that SRM can run to perform custom recovery actions on virtual machines.

SRM lets you test recovery plans by using a temporary copy of the replicated data in a way that does not disrupt ongoing operations at either site. For the detailed information, visit the following VMware Site Recovery technical overview:

https://storagehub.vmware.com/t/site-recovery-manager-3/vmware-site-recovery-technical-overview/introduction-94/

VMware vSphere Replication

VMware vSphere Replication is an extension to VMware vCenter Server that provides a hypervisor-based virtual machine replication and recovery. As an alternative to storage-based replication, vSphere Replication protects virtual machines from partial or complete site failures in the following scenarios:

- From a source site to a target site
- Within a single site from one vSphere cluster to another
- From multiple source sites to a shared remote target site
- From single source site to multiple remote target sites

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site. When you configure a virtual machine for replication, the vSphere Replication agent performs an initial full synchronization of the source virtual machine and its replica copy, then sends changed blocks in the virtual machine disks from the source site to the target site. The changed blocks are applied to the copy of the virtual machine. This process occurs independently of the storage layer.

Solution configuration

In this section, we will describe the configuration steps that were executed to build out the Disaster Recovery Solution for ThinkAgile VX with VMware Cloud on AWS.

We specify the individual site configurations, how the sites are connected together and how business applications are protected using Site Recovery Manager.

On-Prem configuration

The On-Prem customer data center environment (protected site) is implemented using a four-node cluster of Lenovo ThinkAgile VX appliances. ThinkAgile VX simplifies deployment with pre-integrated vSphere software.

The following steps build out the rest of the protected site:

1. Install and Configure a VMware vCenter Server instance to cluster the four ThinkAgile VX nodes.
2. Configure a vSAN cluster of the four ThinkAgile VX nodes for the protected customer workloads.
3. Configure a VMware vSphere Distributed Switch (VDS) across the new cluster.

4. Create or migrate existing virtual machine, vMotion, vSAN, Management, SRM port groups to the VDS.
5. Install the latest version of the NSX Manager appliance, and configure it with three NSX controllers and one NSX Edge Gateway Appliance to serve as the On-Prem endpoint for the IPsec Tunnels to the VMware Cloud on AWS recovery site.
6. Download and install the VMware Site Recovery Manager and VMware vSphere Replication Server on the on-premises VX cluster.
7. Link the on-premises Site Recovery Manager instance to the local vCenter appliance and vSphere Replication Server.

The On-Prem site is now prepared for the configuration and deployment of the customer workloads to protect as part of this Disaster Recovery Solution.

VMware Cloud on AWS configuration

Configuring a VMware Cloud on AWS environment, requires an existing AWS Account, a VMware Cloud Account, and payment method (credit card or subscription credits). Sign in to the VMware Cloud on AWS Console:

https://vmc.vmware.com

From the AWS Console, create an SDDC environment with the following information:

- AWS Region used to deploy the VMware Cloud on AWS recovery site.
- Number of nodes for the recovery site cluster.

  You may start with a single host cluster while you configure the networking and troubleshoot any firewall issues that you might have, then scale up to a four-node cluster with just the click of a button.
- Name for the VMware Cloud on AWS SDDC recovery environment.
- The AWS Account to use with VMware Cloud on AWS.

  An Amazon CloudFormation Template is used to create all the required IAM rules for connecting your existing AWS account and the new VMware Cloud on AWS account. Once these accounts are linked, you can use your existing AWS resources from the VMware Cloud on AWS environment.
- Subnet details to use for the VMware Cloud on AWS SDDC.

  Ensure that these subnet addresses do not overlap with either your On-Prem or AWS VPC subnets.

With all these details, VMware will deploy the SDDC environment with VMware vCenter, Platform Services Controller, and NSX Manager with a couple of Gateway instances. The VMware Cloud on AWS vSAN cluster will include two datastores: one for management VMs and the other for customer workloads.

When the deployment process is complete, you will receive a VMware vCenter Server DNS Name and IP address for accessing your environment. Once you have this secondary environment up and running, you can follow the next section to configure connectivity between your On-Prem environment and your VMware Cloud on AWS environment.

Network connectivity

This section details how to connect the two sites together as a disaster recovery solution.

As shown in Figure 4, two IPsec VPN tunnels are configured between the On-Prem NSX-Edge Appliance hosted in ThinkAgile VX and the Management and Compute Gateway instances in VMware Cloud on AWS.

- IPsec Tunnel between NSX Edge (On-Prem) to Management Gateway: Used to enable access to vCenter, VM Migrations, and Content Libraries.
- IPsec Tunnel between NSX Edge (On-Prem) to Compute Gateway: Used to deploy User Virtual Machines and assign Public IP Addresses. User can also create L2VPN and use that to extend layer 2 networks across the tunnel

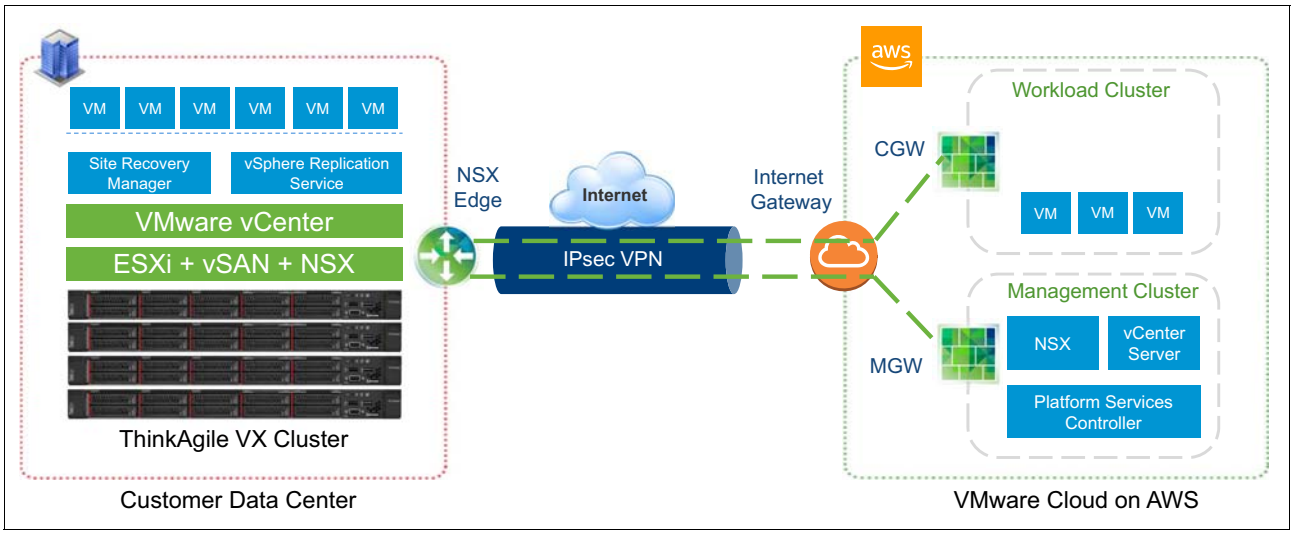

Figure 4 IPsec VPN tunnel

To create these IPsec VPN Tunnels, use the Network tab in the VMware Cloud on AWS Portal and use the Remote Gateway IP Address and the Subnet for the on-prem (protected) site. If the on-prem Remote Gateway is behind a firewall, then you can also specify the public IP address of the firewall in addition to the Remote Gateway IP Address.

Use the NSX Edge Appliance to configure the IPsec Tunnels in the on-prem environment. Create a new NSX-Edge Gateway, if one does not already exist, then specify the Remote Public IP Addresses of the Management and Compute Gateway Instances on the VMware Cloud on AWS recovery site to complete IPsec tunnel configuration.

When both of the tunnels are in the Connected State, create an additional L2VPN over the IPsec tunnel between the VMware Cloud on AWS Compute Gateway and the NSX-Edge Appliance (On-Prem). This L2VPN is used to stretch Layer 2 networks across both sites, so you can have the same Virtual Machine networks across sites, and any VMs deployed in VMware Cloud on AWS can use DNS and DHCP services hosted On-Premises.

Site Recovery Manager configuration

VMware Site Recovery Service automatically deploys a Site Recovery Manager and vSphere Replication Server Instance in the VMware Cloud on AWS SDDC cluster and registers it with the VMware Cloud on AWS vCenter Instance.

Once both the sites have SRM up and running, add the firewall rules required for the SRM Instances to communicate with each other using the Management IPsec Tunnel instance. Use the Firewall Rules Accelerator to help create all of the required rules in VMware Cloud on AWS.

Now, that SRM Instances can communicate, complete the following steps by logging into either one of the SRM instance:

1. Create a Site Pair to connect the On-Prem and VMware Cloud on AWS SRM instances.
2. Select a Placeholder Datastore on both the sites, which will be used to store the Placeholder Virtual Machine files.

   Placeholder Virtual Machines are created and maintained in a power off state during normal operations. Placeholder virtual machines do not have any virtual disks and hence they consume minimal amount of storage. During Disaster or Planned Migration scenarios, the placeholder virtual machines are replaced by the secondary copies of the virtual machines, which are then powered on.
3. Configure Resource Mapping between the two sites by selecting the appropriate networks, datastores.

With the above pre-requisites completed, proceed to configure VM replication:

1. Select individual virtual machines and set RPO settings.
2. Create Protection Groups that will contain the virtual machines that you initiated replication for in the previous step.
3. Create Recovery Plans that can contain one or more Protection Groups.
4. Test the Recovery plans, to ensure that there are no issues with the configured settings.
5. SRM removes the guesswork accompanied with disaster recovery planning. You can test, execute a planned migration or even run disaster recovery scenarios for individual recovery plans on-demand.

Note: In the event of a disaster, an administrator must log into the SRM instance at the recovery site and manually initiate a recovery plan -- automated initiation is not supported. Once a recovery plan has been initiated, SRM will manage starting the secondary copies of the virtual machines on the recovery site based on the settings configured in the Recovery Plan.

Solution verification

We used the test cases listed in Table 2 to verify the solution architecture.

Table 2 Test scenarios

Test Scenario	Test Details	Observations
VM Migration	After configuring vCenter Hybrid Linked Mode, an application instance was migrated from the ThinkAgile VX SDDC on-premises to VMware Cloud on AWS SDDC	All migrations were performed successfully. **Note**: Live migration between On-Premises SDDC and VMware Cloud on AWS requires a Direct Connect link, otherwise, only cold migration is supported
Planned Migration	To validate the SRM Recovery Plan, a planned migration was performed with a Linux-based application, a Windows-based application and a SQL Server database instance.	All the planned migrations were completed successfully. Upon executing a recovery plan, SRM performs an orderly evacuation of virtual machines from the protected site to the recovery site. For Planned Migrations, both sites must be running and fully functional.

Test Scenario	Test Details	Observations
Disaster Recovery	A disaster event was simulated On-Premises by suddenly removing power from the ThinkAgile VX SDDC cluster hosting the protected site.	Manually accessing the VMware Cloud on AWS SRM instance, initiating the recovery plan automates the orderly startup of replication VMs on the recovery site.

Best practices

The following are the best practices which we recommend you follow while configuring this solution.

- **Software Versions**

  Ensure all VMware component versions comply with VMware Compatibility matrices.

- **Network Services**

  All of the VMware components (i.e. ESXi hosts, vCenter Server, Site Recovery Manager, etc.) should be configured to use the same DNS and NTP servers to avoid any configuration drift.

- **Management Traffic**

  Isolate the Management Traffic from the Virtual Machine Network Traffic. The Management traffic should use a secure private network.

- **Database Servers**

  Use separate Database Server instances for vCenter and Site Recovery Manager in the on-premises (protected) site.

- **Network Configuration**

  Ensure that there are no asymmetric network configurations. For networks spanning across sites using L2VPN, ensure that the gateway forwards traffic to the NSX Edge endpoint On-Prem.

- **VPN Tunnel Configuration**

  If the on-premises NSX Edge appliance is behind a firewall, you will need to configure the following firewall rules to forward IPsec VPN protocol traffic:

  - UDP Port 500 to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through the firewall
  - Set IP protocol ID 50 to allow IPsec Encapsulating Security Protocol (ESP) traffic to be forwarded through the firewall
  - Set IP protocol ID 51 to allow Authentication Header (AH) traffic to be forwarded through the firewall

- **SRM Configuration**

  After creating the Site Pair between the SRM instances on-prem and VMware Cloud on AWS, create firewall rules to allow access to the VMware Cloud on AWS SRM instance in case of a disaster.

Conclusion

Timely recovery after a disaster event is a critical driver for business success. Preparing recovery plans that are configured correctly and tested regularly can make all the difference during the chaos that occurs when a disaster strikes.

The disaster recovery solution and best practices described in this document can help you prepare your own data center using Lenovo ThinkAgile VX with VMware Cloud on AWS.

Resources

For more information, consult these resources:

- Lenovo ThinkAgile VX product web page:

  https://www.lenovo.com/us/en/data-center/software-defined-infrastructure/ThinkAgile-VX-Series/p/WMD00000340
- Lenovo ThinkAgile VX datasheet

  https://lenovopress.com/datasheet/ds0023-lenovo-thinkagile-vx-series
- Lenovo ThinkAgile VX product guides:

  https://lenovopress.com/servers/thinkagile/vx-series#rt=product-guide
- VMware Cloud on AWS product page:

  https://cloud.vmware.com/vmc-aws
- VMware Site Recovery Service:

  https://cloud.vmware.com/vmc-aws/add-ons
- vSphere Replication 8.1 Administration Guide

  https://docs.vmware.com/en/vSphere-Replication/8.1/vsphere-replication-81-admin.pdf
- Site Recovery Manager Install and Configuration Guide

  https://docs.vmware.com/en/Site-Recovery-Manager/8.1/srm-install-config-8-1.pdf

Authors

This paper was produced by the following team of specialists:

Bhavin Shah is a Technical Product Marketing Manager with the Software Defined Infrastructure Group at Lenovo, with deep expertise in VMware and AWS Technologies. He has more than 5 years of experience with different virtualization, storage and cloud technologies. He is AWS Certified Solutions Architect, SysOps Administrator, and Developer Associate. He has been working with customers to build out reference architecture solutions that helps meet customer needs.

Akshay Pathak is a Consulting Architect working in Solution Engineering at VMware. He has a total of 14 years of experience in the IT Industry, with the last 5 years with VMware products such ESXi, vSphere, NSX and vSAN. He has deep understanding of VMware features such as vMotion, HA, DRS, Load Balancing, SRM, VMware Cloud on AWS, and Persistent Memory. He is a VMware Certified Professional for Data Center Virtualization 6.5 & Network Virtualization 6.0.

Prasad Kalpurekkal is a Senior Consultant working in Solution Engineering at VMware. He has total of 9 years of field experience in virtualization domain and has intimate knowledge on VMware products such as vSphere, vRealize, Pivotal Container Service (PKS), VMware Disaster Recovery Solutions, NSX, vSAN, VMware Cloud Foundation and VMware Cloud on AWS. He is a VMware Certified Professional for Data Center Virtualization 6.5 & Network Virtualization 6.0. Most recently, Prasad co-authored a blog post, *Pivotal Container Service (PKS) Integration With NSX-T Data Center: A lab study with Tips* available from https://blogs.vmware.com/networkvirtualization/2018/06/pks-nsx-t-lab.html/.

Thanks to the following people for their contributions to this project:

- John Encizo, Lenovo
- Henry Vail, Lenovo
- Robert Campbell, VMware
- Anthony Dukes, VMware
- Glenn Sizemore, VMware
- VMware Cloud on AWS support team
- David Watts, Lenovo Press

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document was created or updated on August 23, 2018.

Send us your comments via the **Rate & Provide Feedback** form found at
http://lenovopress.com/lp0947

Trademarks

Lenovo, the Lenovo logo, and For Those Who Do are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. These and other Lenovo trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by Lenovo at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of Lenovo trademarks is available on the Web at http://www.lenovo.com/legal/copytrade.html.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®	Lenovo(logo)®	ThinkSystem™
Lenovo XClarity™	ThinkAgile™	

The following terms are trademarks of other companies:

SQL Server and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.