FREQUENTLY ASKED QUESTIONS: September 2024

VMware Live Recovery Frequently Asked Questions (FAQs)

Index

vmware by Broadcom

General

Q. What is VMware Live Recovery?

VMware Live Recovery delivers powerful cyber and data resiliency for VMware Cloud Foundation. Customers can protect applications and data from modern ransomware and other disasters across VMware Cloud Foundation environments on-premises and in public clouds with flexible licensing for changing business needs and threats.

Q. What are the key benefits of VMware Live Recovery?

VMware Live Recovery provides a variety of benefits, including:

- Unified service experience: centralized visibility and monitoring of ransomware recovery and disaster recovery across on-premises and public clouds, with access to respective management consoles.
- Secure cyber recovery: industry-leading ransomware recovery-as-a-service with immutable snapshots, guided workflows, isolated “clean rooms” and embedded behavioral analysis.
- Simplified consumption: single subscription that provides a full range of cyber and disaster recovery capabilities, as well as licensing flexibility for changing business needs and threats.

Q. What does VMware Live Recovery consist of?

VMware Live Recovery offers ransomware recovery and disaster recovery leveraging two technology stacks:

- VMware Live Cyber Recovery (formerly known as VMware Cloud Disaster Recovery)
- VMware Live Site Recovery (formerly known as VMware Site Recovery Manager)

Please review respective sections below for each of the above technology stack options of VMware Live Recovery.

Q. Who is VMware Live Recovery for?

VMware Live Recovery is primarily for IT administrators responsible for IT infrastructure and services resiliency and recovery.

Q. What challenges does VMware Live Recovery solve for customers?

Below are some of the key challenges which VMware Live Recovery addresses:

- Inconsistent operating models: Customers often need to piece together multiple solutions to address their ransomware and disaster recovery needs. This leads to siloed infrastructure and team support for these essential functions. Increasing complexity of
- ransomware attacks: Modern ransomware attacks leverage native, legitimate programs and are therefore hard to detect and recover from. Immutable and air-gapped backups are not enough because modern ransomware can remain dormant in backups and reinfect systems after recovery. Traditional file scanning is also not enough because fileless attacks can only be detected by performing behavioral analysis on running workloads.
- Lack of flexibility and agility: Lack of flexibility and agility between different recovery solutions as the customer’s environment and cloud strategy evolves.

Q. How does VMware Live Recovery compare to other ransomware and disaster recovery solutions?

VMware Live Recovery is the only solution that provides unified protection for ransomware and disaster recovery between on-premises sites and to the public cloud from a central interface. It also offers industry-leading ransomware recovery capabilities that enable customers to confidently recover from existential threats, accelerate recovery with guided automation, and simplify recovery operations. These capabilities are delivered with a simple and flexible licensing model.

Getting Started

Q. How do I learn more or get started with VMware Live Recovery

Reach out to your VMware Sales Representative to learn more or get started with VMware Live Recovery.

Q. Do I need to learn new tools?

No. If you are familiar with VMware Cloud Disaster Recovery you will be familiar with VMware Live Cyber Recovery (VLCR). If you are familiar with Site Recovery Manager, you will be familiar with VMware Live Site Recovery (VLSR). These are technology stacks under VMware Live Recovery and no new learning tools are needed.

Q. If I choose to use VMware Live Recovery, what do I need to deploy on my on-premises site(s) source site?

Depending on whether you choose to deploy VMware Live Cyber Recovery and/or VMware Live Site Recovery, you need to deploy different components on your source site. If you choose to deploy VMware Live Cyber Recovery, you need to deploy one or more DRaaS Connector virtual machines on your source site vSphere environment to connect to the VMware Live Cyber Recovery cloud-based components. The DRaaS Connector is an easy-to-deploy OVA. If you choose to deploy VMware Live Site Recovery, you should download & deploy the VMware Live Site Recovery vSphere Replication appliances on your protected and recovery sites and connect it to VMware Live Recovery cloud console.

VMware Live Cyber Recovery

Q. What is VMware Live Cyber Recovery?

VMware Live Cyber Recovery is a technology stack under VMware Live Recovery, and is an easy-to-use, on-demand disaster recovery (DR) solution, delivered as SaaS, with cloud economics.

Q. How is VMware Live Cyber Recovery a cost-effective DRaaS solution?

There are three primary ways in which VMware Live Cyber Recovery is cost-effective. First, you no longer need to own and continuously maintain a secondary DR site. Second, you can utilize an efficient cloud storage layer provided by the service to store your backups during the steady state and only consume failover compute and primary storage capacity when a disaster event occurs. Finally, this service provides an operationally consistent and familiar vSphere experience across the production and DR sites, so your IT staff doesn't need to learn new tools.

Q. Can I bring my own existing AWS account for VMware Live Recovery to use for the cloud storage?

The AWS account will be owned and managed by VMware, so you cannot bring your own AWS account.

Q. How can I be sure that my disaster recovery plan will work when I need it?

Compliance checks are automatically run every 30 minutes to increase your confidence that your cyber recovery plan will work when you need it. Additionally, SLA Status view shows status for items related to Protection and Recoverability, including cyber recovery plans. You will be notified should an item require attention.

Q. Can I use an existing VMware Cloud on AWS SDDC deployed from the VMware Cloud console for recovery?

Yes, you can leverage an existing VMware Cloud on AWS SDDC deployed from the VMware Cloud console for recovery. Clusters and hosts added from VMware Cloud console to this SDDC are automatically recognized by VMware Live Cyber Recovery.

Q. How does VMware Live Cyber Recovery work?

Using a simple, cloud-based UI, you can configure backup policies to protect your VMs and cyber recovery plans to orchestrate cyber recovery workflows. Backups are encrypted and stored in the native vSphere VM format in a highly efficient cloud storage layer called the Scale-out Cloud File System (SCFS) instead of primary vSAN storage in a VMware Cloud on AWS SDDC. When a cyber thread event occurs, with a few clicks you can validate and cleanse your VMs to make them production ready. The service can be used to quickly provision VMware resources and SDDCs in VMware Cloud on AWS.

Q. How do I achieve fast recovery times?

The "live mount" capability of VMware Live Cyber Recovery provides fast recovery without a time-consuming rehydration

the backup data from cloud storage to VMware Cloud on AWS hosts. The backed-up data is immediately made available in the recovery SDDC via an NFS datastore mounted to the SDDC hosts. Having a small deployment of pre-provisioned pilot light hosts makes the recovery process even faster.

Q. Do I need a VMware Cloud on AWS SDDC in the steady state when I am only replicating to the cloud?

You do not need a VMware Cloud on AWS SDDC to be provisioned in the steady state. However, it is recommended that you purchase VMware Cloud on AWS SDDC subscriptions in advance.

Q. What regions are currently supported with VMware Live Cyber Recovery?

US West (Oregon)	Europe (Zurich)
US East (N. Virginia)	Asia Pacific (Melbourne)
US West (N. California)	Asia Pacific (Singapore)
US East (Ohio)	Asia Pacific (Mumbai)
Canada (Central)	Asia Pacific (Sydney)
S. America (Sao Paulo)	Asia Pacific (Tokyo)
Europe (Ireland)	Asia Pacific (Seoul)
Europe (London)	Asia Pacific (Osaka)
Europe (Milan)	Asia Pacific (Hong Kong)
Europe (Frankfurt)	Asia Pacific (Hyderabad)
Europe (Paris)	Africa (Cape Town)
Europe (Stockholm)	Middle East (Bahrain)

Q. Does VMware Live Cyber Recovery convert the VMs to a different format for cyber recovery?

Unlike many other cloud-based data protection solutions, VMware Live Cyber Recovery keeps your protected VMs in their native vSphere VM format which eliminates the need for brittle VM conversions that slow down recovery and make failback error-prone

Q. Does VMware Live Cyber Recovery support multiple backups for a single VM?

Yes, VMware Live Cyber Recovery supports the ability to retain multiple point-in-time snapshots for any protected VM.

Q. Can I recover from an older point-in-time snapshot?

You can recover from any point-in-time snapshot that is available based on your configured retention policies. Any of these snapshots – including the most recent one – can be used to immediately power-on your VMs, using the “live mount” capability.

Q. What storage options do you support for protection with VMware Live Cyber Recovery?

VMware Live Cyber Recovery supports the protection of vSphere VMs running on any vSphere compatible storage on a VMFS, NFS, vVols or vSAN datastore.

Q. How does the Connector get updated?

Connector will be updated automatically and seamlessly without your intervention so that it stays compatible with the cloud service.

Q. How can I get ransomware protection with VMware Live Cyber Recovery?

VMware Live Cyber Recovery offers a purpose-built ransomware recovery as-a-service solution delivering the following capabilities:

- Provides air-gapped immutable cloud-based VMDK backups from which users can protect and then recover their VMDKs and data.
- An on-demand Isolated Recovery Environment (IRE) for safely and securely powering on infected VMs for the purpose of inspection and cleansing.
- A guided ransomware recovery workflow that tracks users through the end-to-end process across identification, validation and restore of recovery points.
- Guided restore point selection that surfaces metrics such as VMDK rate of change and file entropy to inform selection of recovery point candidates.
- Embedded NGAV and behavioral analysis of powered-on workloads in an on-demand, VMware- managed Isolated Recovery Environment (IRE).
- Push-button VM level network isolation levels to prevent reinfection during restore point validation in the IRE.

- This is integrated into the VMware Live Cyber Recovery UI, and all these workflows and features can be invoked directly from there.

Q. What is an Isolated Recovery Environment (IRE)?
An IRE, or 'clean room', is a secure and safe environment used for validating VMs infected with ransomware that leverages VMware Cloud on AWS.

Q. How is VMware Live Cyber Recovery's Isolated Recovery Environment different from other vendors or approaches?
By leveraging VMware Cloud on AWS and using a small Pilot Light or on-demand deployment, customers can avoid the expense of building secondary / isolated datacenter infrastructure stacks to construct and manually manage their own IREs (Isolated Recovery Environments). The Recovery SDDC used as the IRE is also instrumented with an integrated NGAV toolset as well as advanced firewall capabilities at the recovered VM control level.

Q. Does VMware Live Cyber Recovery analyze and scan the running recovery-candidate snapshots to find ransomware attack indicators and related malicious code?
Yes. VMware Live Cyber Recovery embeds NextGen Antivirus (NGAV) and behavioral analysis directly inside of the ransomware recovery workflow and automatically analyzes snapshots recovered to the IRE for ransomware attack Indicators of Compromise (IOCs), searches for workload vulnerabilities (unpatched software) and performs malware scanning.

Q. What is NextGen Antivirus and behavioral analysis and why does it help identify ransomware attacks vectors?
NextGen Antivirus takes traditional antivirus software to a new, advanced level of endpoint security protection. It goes beyond known file-based malware signature searches by using predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to:

- Detect and prevent malware and fileless non-malware attacks.
- Identify malicious behavior and Tactics Techniques & Procedures (TTPs) from unknown sources.
- Collect and analyze comprehensive endpoint data to determine root causes.
- Respond to new and emerging threats that previously go undetected.

Learn more about NGAV and behavioral analysis by clicking here.

Q. Is traditional file scanning effective at finding ransomware?
No. Ransomware bad actors learned many years ago how to avoid being detected by traditional file scanning tools. They often change file hashes prior to loading a malicious payload on the victim's machine and delete the malicious file(s) immediately after being utilized to begin the attack sequence – both (and other TTPs) defeat the traditional file scanning approach.

Q. Can I integrate other EDR products with VMware Live Cyber Recovery (i.e., CrowdStrike, MSFT Defender)?
While other EDR products may continue to be used on the Protected site, use of non-VMware NGAV and behavioral analysis tools in conjunction with VMware Live Cyber Recovery will require a manual process of opening Isolated Recovery Environment networking paths to allow VM access to third party cloud-based security tools.

VMware Live Site Recovery

Q. What is VMware Live Site Recovery?
VMware Live Site Recovery is the industry-leading disaster recovery management solution. VMware Live Site Recovery offers automated orchestration and non- disruptive testing of centralized recovery plans for all virtualized applications.

Q. What topologies does VMware Live Site Recovery currently support?
VMware Live Site Recovery supports on-premises to on-premises disaster recovery.

Q. How does VMware Live Site Recovery work?
VMware Live Site Recovery integrates with VMware vSphere

through VMware vCenter Server and an underlying replication technology. It can integrate natively with vSphere Replication or with a broad range of storage array-based replication solutions from leading storage vendors through storage replication adapters or VMware Virtual Volumes. VMware Live Site Recovery guides users through the process of configuring recovery plans. At the time of failover or testing, VMware Live Site Recovery automates the execution of the recovery plan.

Q. How is technical support purchased?
When you purchase a VMware Live Recovery term subscription, production support is automatically included in the subscription term.

Q. What components are required for a VMware Live Site Recovery deployment?
Instances of vSphere, vCenter Server and VMware Live Site Recovery are required at both the protected site and the recovery site. Additionally, VMware Live Site Recovery requires pairing the protected and recovery sites with the VM Live Recovery instance in the cloud. VMware Live Site Recovery also requires an underlying replication product to copy virtual machines to the recovery site. Customers can choose to use either vSphere Replication or third-party array-based replication software. When using array-based replication software, a Storage Replication Adapter (SRA) is also required. Using VMware Virtual Volumes integrated with VMware Live Site Recovery does not require an SRA.

Q. Which editions and versions of VMware vSphere are compatible with VMware Live Site Recovery?
VMware Live Site Recovery is supported with VMware Cloud Foundation, VMware vSphere Foundation, vSphere Essentials Plus and vSphere Standard. See the Product Interoperability Matrix for specific versions of vSphere that are supported for each version of VMware Live Site Recovery.

Q. What is VMware vSphere Replication?
vSphere Replication is VMware's hypervisor-based replication technology for vSphere virtual machines. vSphere Replication is a robust and scalable solution that simplifies DR protection through storage-independent, VM-centric replication with customizable recovery point objectives (RPO) and multiple point-in-time recovery. vSphere Replication is included as part of VMware Live Recovery entitlement.

Q. Which array-based replication products are compatible with VMware Live Site Recovery?
VMware Live Site Recovery integrates with third-party storage array-based replication products through VMware Virtual Volumes or a Storage Replication Adapter (SRA). See this Compatibility Guide for supported VMware Virtual Volumes array vendors and this Compatibility Guide for supported SRAs.

Q. Is VMware Live Site Recovery compatible with stretched storage solutions?
Yes. VMware Live Site Recovery 9.0 and newer versions support stretched storage solutions available by some major VMware storage partners. For details, check their SRA documentation.

Q. Does VMware Live Site Recovery work with VMware vSAN?
Yes, vSAN is fully supported as either a protected or recovery site for VMware Live Site Recovery when using vSphere Replication.

Q. Will VMware Live Site Recovery work with VMware Virtual Volumes?
Yes, VMware Live Site Recovery is compatible with VMs located on VMware Virtual Volumes and replicated either with array-based replication or vSphere Replication. For a list of Virtual Volumes array-based replication compatible vendors see here.

Q. Does VMware Live Site Recovery work with 'x' vSphere feature?
VMware Live Site Recovery works with many of the features in vSphere. For a complete list and details around usage check here.

Q. Which replication software is supported with VMware Live Site Recovery?
VMware Live Site Recovery requires either vSphere Replication or storage array-based replication for iSCSI, Fiber Channel, or

NFS storage arrays. For storage array- based replication, VMware works with storage partners to ensure that customers can deploy VMware Live Site Recovery with their choice of storage and storage replication platform. VMware Live Site Recovery is architected to work with various replication software through “storage replication adapter” plug-ins developed and certified by storage vendors for use with VMware Live Site Recovery supported is available online in the Storage Partner Compatibility Matrix. New adapters can be added at any time without requiring a new release of VMware Live Site Recovery. Please contact your storage partner for specific information about when specific replication adapters will be available.

Q. Does VMware Live Site Recovery protect workloads on physical servers?

VMware Live Site Recovery orchestrates the recovery process for virtual machines. In cases in which some workloads are running on physical servers with a separate disaster recovery solution, VMware Live Site Recovery coordinates the recovery process by allowing users to create custom scripts that ensure that workloads are restored in the appropriate order.

Q. Does VMware Live Site Recovery provide automated failback?

Yes, VMware Live Site Recovery provides automated failback. The first step is to perform a “reprotect” of the virtual machines from the failover site to the original production site. This consists of coordinating the reversal of replication to the original site and mapping virtual machines back to their original virtual machine folders, virtual switches, and resource pools. The second step is to execute the planned migration back to the original site, using the original recovery plan executed in the reverse direction.

Q. Are VMware vSphere licenses required for both the protected and recovery sites?

Yes, vSphere licenses are required for any server on which vSphere is installed, whether that host is at a protected or recovery site, and whether a server is running or powered down at the recovery site. VMware Live Site Recovery requires at least one licensed vSphere server at protected and recovery sites.

Q. Are vCenter Server licenses required for both the protected and recovery sites?

Yes, VMware Live Site Recovery requires two active and licensed vCenter Server instances, one at each site (protected and recovery). NOTE: The shared recovery sites feature in VMware Live Site Recovery enables multiple protected sites with multiple vCenter Server instances to be recovered at a site with a single vCenter Server instance. (i.e., the multiple instances of VMware Live Site Recovery running at the shared recovery site are registered with the same instance of vCenter Server at the shared recovery site, so you do not need multiple vCenter Server instances at the shared recovery site.).

Q. Are VMware Live Site Recovery subscriptions required for the recovery site?

Only virtual machines protected by VMware Live Site Recovery require VMware Live Site Recovery subscriptions. Subscriptions are required for all protected virtual machines, even if they are powered off. There are two scenarios to consider:

Uni-directional protection: VMware Live Site Recovery is configured only to fail over virtual machines from site A to site B. In this case, a subscription is required only for the protected virtual machines at protected site A.

Bi-directional protection: VMware Live Site Recovery is configured to fail over virtual machines from site A to site B while it is configured to fail over a different set of virtual machines from site B to site A. In this case, VMware Live Site Recovery subscription must be purchased for the protected virtual machines at both sites.

Q. After failover, what are the license requirements for failback?

To fail back from site B to site A (after failover from site A to site B), a VMware Live Recovery subscription is required for the “re-protected” virtual machines at Site B. The “per virtual machine” subscription originally used at site A can be used at site B for this purpose, if the subscription is no longer in use at site A.

Q. When using the shared recovery sites feature, are extra subscriptions needed at the shared recovery site?

A VMware Live Recovery subscription is required only for protected virtual machines. In a shared recovery site scenario

(multiple protected sites configured to failover into a shared recovery site) VMware Live Recovery subscriptions are required only at the protected sites. The shared recovery site does not require any additional VMware Live Recovery subscription to protect those sites.

Q. What is the difference between planned migration and DR failover?

Planned migration and DR failover both leverage the same recovery plans. DR failover is used in the event of a disaster and is designed to recover virtual machines at the failover site quickly. Planned migration is used for preventive failovers or for routine migrations. Planned migration ensures an orderly shutdown of virtual machines at the protected site, synchronizes the data with the failover site by ensuring complete replication of all the data, and finally, recovers virtual machines at the failover site. Planned migration ensures an application-consistent copy of the data to the secondary site with no data loss.

Q. Does VMware Live Site Recovery provide application-consistent or crash-consistent recovery?

The level of consistency depends on the recovery process and the underlying replication solution. For DR failovers, the underlying replication solution provides consistency. With storage-based replication, many VMware partners offer solutions to ensure application-consistent replication and recoveries. vSphere Replication supports VSS-based application consistency for Windows environments. In all other environments, VMware Live Site Recovery provides file-consistent recovery.

When executing a planned migration (as opposed to DR failover), VMware Live Site Recovery provides fully application-consistent migrations between sites since virtual machines are gracefully shutdown before completing replication and initiating the recovery plan.

Q. Does VMware Live Site Recovery support active/ active sites?

Yes, VMware Live Site Recovery supports configurations in which both sites are running active virtual machines that VMware Live Site Recovery can recover at the other site. It also supports active/passive sites in which VMware Live Site Recovery recovers virtual machines from a protected site at a recovery site that is not running other virtual machines during normal operation. In an active/active scenario, users configure recovery plan workflows in one direction from Site 1 to Site 2 for the protected virtual machines at Site 1. Recovery plan workflows are configured in the opposite direction from Site 2 to Site 1 for the protected virtual machines at Site 2.

Q. Can I use VMware Live Site Recovery if I don't have access to the internet?

Yes, VMware Live Site Recovery can work in offline mode without internet connectivity. To take advantage of VMware Live Recovery benefits including cloud economics, it is recommended to connect to VMware Live Recovery Cloud Console.

Q. Can I use VMware Live Site Recovery with VMC on AWS?

No.

Q. Can I use VMware Live Site Recovery with Azure VMware Solution, Google Cloud VMware Engine or Oracle Cloud VMware Solution?

Yes. You must purchase VMware Live Recovery subscriptions for using VMware Live Site Recovery with Hyperscalers such as Azure VMware Solution, Google Cloud VMware Engine or Oracle Cloud VMware Solution.

Q. Can I protect a single virtual machine using both VMware Live Site Recovery and VMware Live Cyber Recovery?

Yes, you can protect a single virtual machine using VMware Live Site Recovery and VMware Live Cyber Recovery. This setup can offer you dual protection against disasters and ransomware. Do note that dual-protection is limited to Array-Based Replication (ABR) only and will require two VMware Live Recovery entitlements for a single virtual machine, as it is protected twice. More details are noted in the documentation.

Q. What RPO can I expect with vSphere Replication?

With vSphere Replication, users can select the replication schedule for each VM. The RPO can be selected from 1 minute to 24 hours.

Support and Additional Resources

Q. How can I get support when using VMware Live Recovery?

You can contact support through Broadcom Support Portal here.

Q. Is there technical documentation available?

You can find the official technical documentation for VMware Live Recovery here.

Q. Where can I find operational limits for VMware Live Recovery?

You can find the operational limits for VMware Live Recovery here.

Q. Is there a Hands-on-Lab that I can use?

Hands-on-Lab for VMware Live Cyber Recovery for DR is available in VMware HOL catalog here and for Ransomware Recovery is here. A Hands-on-Lab for VMware Live Site Recovery is available in VMware HOL catalog here.

Q. Where can I find the solution brief for VMware Live Recovery?

You can find the solution brief for VMware Live Recovery here.

Q. What versions of other VMware software such as vCenter Server and ESXi work with VMware Live Recovery?

You can find the versions of VMware software that interop with VMware Live Recovery here.

Q. What service level agreement (SLA) do you offer for VMware Live Recovery?

Please refer to the Service Level Agreement document for VMware Live Recovery available here.

Q. Where can I find the terms and conditions for using VMware Live Recovery?

You can refer to the service Terms & Conditions here

Q. Where can I find information about the most recent updates to VMware Live Recovery?

For information about the latest features and updates to the service, please refer to the release notes here.

Q. Where can I find the price for VMware Live Recovery?

You can reach out to your VMware Account Representative for pricing information.

Subscriptions and Usage

Q. What happens to customers currently using VMware Cloud Disaster Recovery?

Customers who have VMware Cloud Disaster Recovery subscriptions will get access to all VMware Live Recovery features until the end of their current term subscription at no additional charge. At the end of the term, customers should work with their VMware Account Representative to purchase a subscription for VMware Live Recovery. Customers who want to expand their ransomware recovery and disaster recovery usage must purchase term subscription of VMware Live Recovery to cover the usage.

Q. What happens to VMware Ransomware Recovery?

Customers who have already deployed VMware Cloud DR, regardless of whether they subscribed to VMware Ransomware Recovery, will inherit VMware Ransomware Recovery feature at no additional charge.

Q. What happens to customers currently using VMware Site Recovery Manager?

Customers who have VMware Site Recovery Manager subscription can continue to use the product until the end of the subscription term. At the end of term, customers will need to purchase a new subscription of VMware Live Recovery to continue using the product. Customers who want to expand their disaster recovery
usage must purchase a term subscription of VMware Live Recovery to cover that additional usage.

Q. Can my legacy VMware Site Recovery Manager licenses and new VMware Live Recovery subscriptions co-exist?

You cannot have different license types on a single VMware Site Recovery Manager server. You can have a legacy term license on a Site Recovery Manager server, and a VMware Live

Recovery subscription license on a different Site Recovery Manager server within a single VMware vCenter.

Q. How does VMware Live Recovery define a protected VM?
A protected VM is defined as one unique combination of protection method and protection target endpoint instance under one VMware Cloud Services Organization. A VM purchase of VMware Live Recovery entitles a customer to assign that VM to a protection method.

Q. How does VMware Live Recovery define Protected capacity?
Protected capacity in TiB is calculated as the sum of the logical storage size of the protected VMs and all the incremental cloud backups you choose to retain (where 1 TiB is equal to 240 or 1,099,511,627,776 bytes). For an accurate calculation of data capacity, please engage your VMware Account Representative. Protected capacity is only required for VMware Live Cyber Recovery.

Q. Are there any additional charges when running VMware Live Cyber Recovery?
Disaster recovery “failback” and “sync back” data transfer (i.e., egress) charges billed by cloud hosting providers will be borne by VMware by Broadcom up to 50% of the protected VM storage capacity. VMware by Broadcom reserves the right to charge for excessive failback or sync back data transfer, which is more than 50% of VM storage capacity.

Q. What happens when a customer's usage is more than their active subscriptions?
Overages occur when customer’s usage of VMware Live Recovery protected VM or protected TiB is more than their active subscriptions. Before May 6th, overages will be charged to customers and billed in arrears at a price higher than the subscription price. After May 6th, it is the customer’s responsibility to make sure their subscriptions cover their usage by purchasing additional subscriptions as needed. Failure to do so might result in restrictions in the service capability.

Q. What currencies are supported for purchasing VMware Live Recovery?
VMware Live Recovery can be purchased through USD only.

Q. When will I pay for VMware Live Recovery service?
When you purchase a term subscription, you will be charged upfront for the full amount for the term subscription.

Q. When does the VMware Live Recovery subscription start?
As soon as your subscription order is processed, the term for subscription starts. You will get an email link to access VMware Live Recovery simultaneously.

Q. How are charges determined for VMware Live Recovery?
VMware Live Recovery pricing consists of a per-VM charge for each protected VM and a per-TiB charge (only for VMware Live Cyber Recovery) which consists of the sum of logical storage size of the protected VMs, and all incremental cloud backups retained. The service is offered through commit subscriptions only and a minimum purchase of 10TiB per subscription region is required while using VMware Live Cyber Recovery.

Term subscriptions do not auto-renew at the end of their term. Continued service use beyond an expired subscription term is not permitted and new term subscriptions should be purchased to cover any service usage. Disaster recovery “failback” and “sync back” data transfer (i.e., egress) charges billed by cloud hosting providers will be borne by VMware up to 50% of the protected VM storage capacity. VMware reserves the right to charge for excessive failback or sync back data transfer, which is more than 50% of VM storage capacity.

Q. Does the VMware Live Recovery pricing include VMware Cloud on AWS hosts?
No, VMware Cloud on AWS subscriptions must be purchased separately and is not included in the VMware Live Recovery pricing or subscriptions.

Q. I am using VMware Live Cyber Recovery to protect workloads on VMware Cloud on AWS SDDC. How will I get charged for data transfer between source SDDC and recovery site?
When using VMware Live Cyber Recovery to protect workloads on VMware Cloud on AWS SDDC, there will be replication traffic

going out from the protected SDDC to VMware Live Cyber Recovery. Depending on the network connectivity and the location of your source and target site, you might get charged for data transfer. Data transfer charges show up on your VMware Cloud on AWS bill. Refer to this article to find your VMware Cloud on AWS data transfer costs.

Q. Are there any other costs that I should be aware about?
The VMware Live Cyber Recovery price includes the underlying cloud infrastructure used by the service including cloud storage, cloud compute instances, managed databases, cloud network devices, and cloud management tools. Additionally, egress data charges incurred during typical use of the service for replication from on-premises to the cloud and failback or sync back to the original protected site over the internet are also covered in the price. However, VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers for failback or sync back.

Q. What do you consider excessive egress data transfers, for which I might be billed additional charges?
After you have recovered your virtual machines into a VMware Cloud on AWS SDDC, you may choose to use the failback capability to move your VMs back to your original protected site. To facilitate this failback in an efficient manner, VMware Live Cyber Recovery transfers only the VM data that has changed since the VMs were recovered into VMware Cloud on AWS. Additionally, you can reduce DR failback times, by performing 'sync back' operations after a failover to periodically transfer incremental, delta-based updates for failed-over workloads on the cloud file system. You will not receive a separate bill from AWS for the egress data transfer charges over the internet incurred in this process, and instead these charges will be borne by VMware. However, the amount of data transferred can become excessively large if there is a long delay between the recovery and the failback if none of the old data is available on the protected site any longer, or if you have performed an excessive amount of sync back operations. VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers as part of a failback or sync back operation – defined as more than 50% of the protected data capacity. You may be charged by Broadcom for such excess data transfers at the prevailing rates published by AWS for Data Transfer out from an EC2 instance to the Internet. These rates are listed on this AWS page. To look up the specific rate applicable to your deployment on this page, please select the AWS region corresponding to your VMware Live Cyber Recovery region and look up the rates in the "Data Transfer OUT From Amazon EC2 To Internet" table.

Q. Does the VMware Live Cyber Recovery price include egress data transfers for VMs running on the recovery SDDC in VMware Cloud on AWS?
No, you will be separately charged for egress data transfers incurred by the recovered VMs when they are running in a VMware Cloud on AWS SDDC at the applicable VMware Cloud on AWS rates.

Q. Can I expand my existing VMware Live Recovery term subscriptions?
Yes, you can expand your existing VMware Live Recovery term subscriptions. You can increase the quantity or increase the duration of term.