VMware Live Recovery

Specific Program Documentation ("SPD") and SaaS Listing

The Broadcom software program(s) ("Broadcom Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the Broadcom quote, order form, statement of work, or other mutually agreed ordering document (each a "Transaction Document") under the applicable end user agreement or governing contract (collectively, the "Agreement") entered into by Customer and the Broadcom entity ("Broadcom") through which Customer obtained a license for the Broadcom Software. These terms shall be effective from the effective date of such Transaction Document. Capitalized terms have the meanings ascribed to them herein, or, otherwise, in the Agreement.

The version of the SPD published on legaldocs.broadcom.com on the date that Broadcom accepts the Customer's Transaction Document for Broadcom Software applies to the version of Broadcom Software in that Transaction Document. If Customer installs a release of Broadcom Software that Broadcom provides as part of Support services, then the then-current version of the SPD published on legaldocs.broadcom.com on the date Customer installs that release applies to that release of Broadcom Software.

Program Name: *VMware Live Recovery*

1. DEFINITIONS.

All terms defined in the Broadcom Software Glossary located at legaldocs.broadcom.com apply to this SPD unless specified herein.

"**Cloud Services**" means computing infrastructure and platform services (such as compute resources, storage capabilities, databases or virtual machines and other computing infrastructure and platforms services) that a third party makes available for consumption by customers.

"**Internally Developed Application**" means: i) a computer applications that Customer has created or developed and (ii) a third-party computer application(s) that is ancillary to Customer's application-based service, and (b) cannot be accessed directly by end users of Customer's application-based service.

"**Server**" means a hardware system capable of running the server software. A hardware partition or blade is considered a separate hardware system.

"**TiB**" means a unit of physical storage capacity that is equal to 2^40 bytes.

2. USE RIGHTS AND LIMITATIONS.

Overview

- 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.
- VMware Live Recovery offers ransomware recovery and disaster recovery leveraging two technology stacks:
    - VMware Live Cyber Recovery (formerly known as VMware Cloud Disaster Recovery), which is a SaaS product.
    - VMware Live Site Recovery (formerly known as VMware Site Recovery Manager), which is an on-premises product.

- This document serves as the SPD for VMware Live Cyber Recovery, and as the SaaS Listing for VMware Live Site Recovery.

License Metrics

- VMware Live Recovery is licensed per protected Virtual Machine (VM). VMware Live Recovery is recommended for purchase with a minimum 3-year term. Pricing includes production support.
- For the use of VMware Live Cyber Recovery, additional protected capacity measured in tebibyte (TiB) is required. Protected capacity is defined as the sum of the logical (used) storage size of all protected virtual machines and all incremental cloud backups (snapshots) on VMware Live Cyber Recovery. A minimum purchase of 10 TiB per subscription region is required.
- Egress data charges incurred during typical use of the service for replication to the cloud and failback to the original protected site are covered by the VMware Live Recovery prices. VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers.

Use Rights and Limitations

- **Feature restrictions.** To facilitate quick recovery of protected virtual machines to a VMware Cloud on AWS SDDC, VMware Live Cyber Recovery automatically creates one or more Network File System (NFS) datastores and attaches them to the SDDC. These datastores facilitate the immediate recovery of protected virtual machines, with virtual disk backups continuing to reside on the Scale-out Cloud File System (SCFS). Virtual machines in the SDDC can immediately power on by directly accessing these datastores either while virtual disk backup data is copied to the VMware vSAN™ datastore on the SDDC (referred to as "Live Mount"), or for an extended period during production failover (referred to as "Running on the Cloud Filesystem"). Virtual Machines running on the SCFS are permitted to use the NFS share in this manner for a maximum of 30 days, after which time all failed-over virtual machine storage must be copied to the VMware vSAN datastore on the SDDC. These NFS datastores are created exclusively for the purpose of exposing the virtual machine backups to the SDDC to facilitate disaster recovery and must never be used as general purpose storage. Customer is not permitted to use the vSphere Client, vSphere APIs, or any method other than the interfaces provided by VMware Live Recovery to create and power on virtual machines directly on these NFS datastores except through capabilities and workflows exposed in the service. If this restriction is not adhered to, VMware will not guarantee support for the affected instances of the service.

  The use of Carbon Black or Carbon Black Cloud feature, products and/or technology in conjunction with VMware Live Cyber Recovery is limited to use within the Isolated Recovery Environment and Ransomware Recovery workflow. Any use of Carbon Black products or technologies in a production setting is strictly prohibited unless those Carbon Black products are properly licensed.

- **Limits on SDDC resources for Recovery.** For customers who do not have access to VMware Cloud on AWS service, the VMware Live Recovery service includes the Recovery SDDC resources needed for disaster recovery or ransomware recovery workflows ("Recovery SDDC"). Customers may simultaneously recover up to 500 VMs in Recovery SDDC. Recovery SDDC should not be deployed for a duration exceeding 14 days in a calendar year.

  For customers who have existing access to VMware Cloud on AWS service must separately purchase the hosts needed for disaster recovery or ransomware recovery. Availability of VMware Cloud on AWS host capacity on an on-demand basis is not guaranteed, and will be considered on a best efforts basis.

- **PCI Compliance.** VMware Lve Cyber Recovery is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Crowe LLP, an independent Qualified Security Assessor (QSA). After initial deployment of the service, Customer must affirmatively take steps to configure its environment to meet Customer's responsibilities as described in the Shared Responsibility Model, at:

  https://vmc.techzone.vmware.com/resource/vmware-cloud-disaster-recovery-shared-responsibility-model

  Customer must ensure that the VMware Cloud on AWS SDDC used with the VMware Live Cyber Recovery service for recovering Customer's VMs is PCI hardened, which may require disabling several VMware Cloud on AWS SDDC add-on capabilities to maintain compliance, including VMware HCX®. VMware will provide a customer-facing website, listing compliant offerings, that Customer can reference to ensure that Customer disables non-compliant VMC add-ons to maintain

PCI compliance for Customer's VMC on AWS environment. In addition, once a VMware Cloud on AWS SDDC is configured for PCI compliance, the networking and security configuration can be managed by Customer directly via the VMware NSX® Manager™ deployed in the SDDC, rather than by the VMware Cloud Console.

For more details, refer to the documentation at docs.vmware.com. See the following for VMware Cloud on AWS Regions that are available for deployment of PCI compliant SDDCs: https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-19FB6A08-B1DA-4A6F-88A3-50ED445CFFCF.html

Before deploying any other VMware service in Customer's instance of VMware Live Cyber Recovery, Customer should review the interoperability and compliance information for that other service. See https://cloud.vmware.com/trust-center/compliance for the most current information on compliant offerings. Customer is responsible for ensuring that any additional service deployed in its VMware Live Cyber Recovery instance meets Customer's compliance and security requirements.

- **Data Retention and Deletion.** Customer data is stored up to 90 days after the subscription term end date and will be deleted permanently and not recoverable.

- **Excess Consumption.** Customers are allowed to use the service up to their purchased quantity. If Customer uses the service in excess of the purchased quantity, Customer must purchase additional quantities to cover excessive usage. A customer will be considered non-compliant if they do not meet this requirement. For offline VMware Live Site Recovery deployments, the protected VMs entitled using the license key generated from Broadcom Support portal will count towards the purchased VMware Live Recovery subscriptions.

- **Restrictions on Use with Public Cloud Services.** Customer must not (and must not allow Customer's Third-Party Agents to) use or deploy the Software on, or with, any Cloud Services.

- **Hosting Rights and Restrictions.** Customer may use the Software to deliver Internally Developed Applications as a service to a third party via an internal or external network. Except as expressly provided in this paragraph and the License Agreement, the use of the Software for any other types of hosting or for the benefit of any third party in any manner is strictly prohibited unless Customer is an authorized participant in a VMware program that is governed by a separate set of terms and conditions which authorizes such activity.

3. SERVICE LEVEL AGREEMENT.

This Service Level Agreement ("SLA") is only applicable to VMware Live Cyber Recovery ("Service Offering"). For clarity, the VMware Live Site Recovery component of VMware Live Recovery is not subject to this SLA and does not have any service level commitments (as it is an on-premises product).

Availability

Broadcom will use commercially reasonable efforts to ensure that the Service Offering is available during a given billing month equal to the "Availability Commitment" specified in the table below.

Service	Availability Commitment
VMware Live Cyber Recovery component of VMware Live Recovery	99.9%

If the Availability of the Service Offering is less than the Availability Commitment, then you may request an SLA Credit. Availability in a given billing month is calculated according to the following formula:

"Availability" = ([total minutes in a billing month – total minutes Unavailable] / total minutes in a billing month) x 100

Disaster Recovery Failover

Broadcom will use commercially reasonable efforts to ensure that a Disaster Recovery Failover ("DR Failover") will meet the specified Recovery Time Objective ("RTO") specified in the table below. "RTO" means the period of time beginning when the customer initiates a failover of a vSphere workload protected by VMware Live Recovery (specifically VMware Live Cyber Recovery) to the time when that workload starts powering on in a recovery SDDC.

Service	Recovery Time Objective
DR Failover	< 2 hours

SLA Events

The Service Offering will be considered "Unavailable", subject to the Service Level Agreement Limitations set forth below, if Broadcom's monitoring tools determine one of the following events (each, an "SLA Event") has occurred.

The total minutes that the Service Offering is Unavailable for a particular SLA Event is measured from the time that Broadcom validates the SLA Event has occurred, as defined below, until the time that VMware resolves the SLA Event such that the Service Offering is Available to you.

If two or more SLA Events occur simultaneously, the SLA Event with the longest duration will be used to determine the total minutes Unavailable.

Each of the following will be considered an SLA Event for the Service Offering:

- Your VMware Live Cyber Recovery orchestrator user interface is inaccessible for ten consecutive minutes.
- Your retained cloud backups in VMware Live Cyber Recovery are inaccessible for ten consecutive minutes.
- You are unable to create or modify protection groups and disaster recovery (DR) plans in VMware Live Cyber Recovery for ten consecutive minutes.
- You are unable to initiate a DR plan as a test or failover in VMware Live Cyber Recovery for ten consecutive minutes.
- You are unable to initiate deployment of a recovery SDDC using VMware Live Cyber Recovery for ten consecutive minutes, even though VMware Cloud on AWS host capacity is available in the region.
- None of your recovered virtual machines running directly off the Scale-Out Cloud File System ("SCFS") can access the virtual disk storage on the SCFS for ten consecutive minutes.

Availability of the Service Offering is dependent on and subject to availability of the underlying services on which the Service Offering is hosted. Availability of the underlying services is not covered by the service availability metrics set forth in this Service Level Agreement. If the underlying services are unavailable, and therefore the Service Offering is unavailable, your sole recourse pursuant to the Agreement is to VMware.

Requirements

To be eligible to receive any SLA Credits for an SLA Event, you must meet the following requirements:

- You must ensure that your environment meets all pre-requisites for deployment and use of the Service Offering as explained in the technical documentation, including but not limited to outbound network connectivity from your protected site and the configuration of an unexpired and properly scoped API token within the user interface of the Service Offering.
- You must not modify the settings of the SDDC used for recovery of your virtual machines in a manner that disrupts the functionality of the Service Offering (e.g., changing the firewall configuration to interrupt access from the SDDC to the SCFS or Orchestrator components, attempting to unmount the Network File System ("NFS") datastores provisioned by the Service Offering, etc.). Please refer to this documentation page for guidance related to this: https://docs.vmware.com/en/VMware-Live-Recovery/services/vmware-live-cyber-recovery/GUID-4D3F8766-220A-473D-844E-45F188B16B11.html
- You must not use the vSphere Client, vSphere APIs, or any method other than the interfaces provided by the Service Offering to create and power on virtual machines directly on the NFS datastore created by the Service Offering on the recovery SDDC.

- There must be sufficient capacity on the recovery SDDC and recovery cluster(s) to support starting a virtual machine.

SLA Credits

Monthly Uptime Percentage	SLA Credit Percentage
Less than 99.9% but equal to or greater than 99.0%	10%
Less than 99.0%	30%
Recovery Time Objective for DR Failover	SLA Credit Percentage
< 2 hours	100%

Each "SLA Credit" is an amount equal to the specified percentage of the per-TiB and the per-virtual machine charges (net of any discounts) charged for the billing month in which the SLA event occurred, as specified in the following table:

Note: To calculate the SLA Credits amount, VMWare Cloud on AWS host charges are not considered. You may be able to separately claim SLA Credits for VMware Cloud on AWS subject to the terms and conditions in the VMware Cloud on AWS Service Level Agreement available at:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-level-agreement.pdf

Service Level Agreement Limitations

The following will be excluded from any time-based calculations related to the Service Offering being Unavailable:

.scheduled maintenance where you have been notified at least 24 hours in advance,

.recurring or zero-impact maintenance that is generally applicable to all customers,

.your misuse of the service offering or a service component,

.force majeure events, denial of service attacks, viruses, or hacking attacks for which there is no commercially reasonable known solution, or any other events that are not within our control or that could not have been avoided with commercially reasonable care,

.acts or orders of government,

.packet loss, network or internet problems beyond Broadcom's border router supporting our public internet connectivity, or

.bugs in code or services for which there is no commercially reasonable known fix (even if there is a known workaround).

RTO:

The following will be excluded from any calculations related to the RTO:

.time associated with customer's manual action or execution of custom script,

.time associated with any customization defined by the customer, such as IP customization,

.time required to boot up virtual machines, or

.any wait time for availability of VMware Cloud on AWS host capacity.

Eligibility:

You will not be eligible to receive an SLA Credit if:

. you are delinquent on any payments for the Service Offering, or

. the SLA Event was due to your failure to meet your security responsibilities as set forth in the Agreement.

Broadcom's monitoring tools, data, and records will be the sole source of information used to track and validate Availability. Upon request, Broadcom will provide to you, within 45 days after a confirmed SLA Event, a copy of the Availability report that Broadcom makes generally available to customers.

Service Level Agreement Claims

To request an SLA Credit, you must file a support request at https://my.vmware.com within thirty (30) days after the suspected SLA Event or the alleged RTO failure. Broadcom will review the request and issue an SLA Credit when Broadcom validates the SLA Event or RTO failure based on Broadcom's data and records.

SLA Credits will be issued to the person or entity that Broadcom invoices for the Service Offering, as a separate credit memo that can be applied towards a future invoice for the Service Offering. If your subscription term for the Service Offering expires or is terminated prior to the issuance of a Service Credit, the Service Credit will become void as of the date of the expiration or termination.

The Service Credits specified in this SLA are your sole and exclusive remedies for any SLA Events or any failure to meet the RTO occurring during your subscription term for the Service Offering or for any other claim in connection with this SLA.

4. THIRD PARTY INFORMATION AND TERMS.

Any required third-party software license terms are incorporated by this reference and are set forth in online documentation at techdocs.broadcom.com or legaldocs.broadcom.com.

- **VMware Tools.** VMware Tools is a suite of utilities and drivers that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine in conjunction with a vSphere hypervisor. Customer may not use VMware Tools with any other hypervisor. Customer may distribute the VMware Tools to third parties solely when installed in a Guest Operating System within a Virtual Machine. Customer is liable for compliance by those third parties with the terms and conditions of the Framework Agreement.