VMware Live Recovery

Specific Program Documentation ("SPD")

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.

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)
  - VMware Live Site Recovery (formerly known as VMware Site Recovery Manager)

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 temporary SDDC resources needed for disaster recovery or ransomware recovery workflows. Customers may simultaneously recover up to 500 VMs. The temporary SDDC should not be deployed for a duration not 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.
- **PCI Compliance.** VMware Live 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 after that
- **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. 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.