Service Description

VMware vCloud® Usage Insight™

Last Updated: 13 September 2019
© 2019 VMware, Inc. All rights reserved. This offering which is the subject of this Service Description is protected by U.S. and international copyright and intellectual property laws. This offering is covered by one or more patents listed at http://www.vmware.com/download/patents.html.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

As used in this Service Description, “VMware”, “we” or “us” means VMware, Inc., a Delaware corporation, if the billing address for your order is in the United States, and VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your order is outside the United States. All terms used but not defined in this Service Description are defined in the Terms of Service or other documents comprising the Agreement between you and us regarding your use of the Service Offering.

VMware, Inc.
3401 Hillview Avenue
Palo Alto, CA 94304
www.vmware.com

Rev. 13 Sept 2019
1. Introduction

VMware vCloud® Usage Insight™ ("vCloud Usage Insight" or the “Service Offering”) is a VMware cloud service offering that automates monthly and end-user usage reporting to the VMware Cloud Provider Program ("VCPP") business portal.

The Service Offering is limited to use by VCPP customers. vCloud Usage Insight is an invite-only service and is available through the VMware Cloud Services Web console; see https://console.cloud.vmware.com. To request an invitation, navigate to https://cloud.vmware.com/vcloud-usage-meter/.

vCloud Usage Insight aggregates reports from vCloud® Usage Meter ("UM") 3.6.x instances. With vCloud Usage Insight, the VCPP partner retains full control to manage the usage report in the VSPP business portal, prior to submittal of the report; the existing manual reporting option remains available.

All data transferred between the UM appliance (available for download at https://www.vmware.com/products/vcloud-usage-meter.html) and vCloud Usage Insight is anonymized to remove any VM name, hostname, end-customer name, etc. Usage Insight supports per-contract and per-site reporting. (For information about VMware vCloud Usage Meter, see https://cloud.vmware.com/vcloud-usage-meter/.)

vCloud Usage Insight reduces the monthly reporting effort by doing the following:

- Automated transfer of reports from UM virtual appliances to the Service Offering
- Automated aggregation of usage across the UM appliances
- Pre-filling usage data into the VSPP business portal
- Full control over the data submitted to the VSPP business portal

vCloud Usage Insight offers two screens - one to register all production UM instances, and the other to pre-fill usage data into the VSPP business portal.

Below is an illustration of the current workflow for usage reporting to the VSPP business portal, and how vCloud Usage Insight automates the reporting process to the VSPP business portal:
Data handling and privacy guidelines

Usage Meter data handling policies and guidelines

Technical Documentation and Training

Documents outlining Key Concepts with usage examples, a “Getting Started” guide, and “How To” guides for key features are available at: https://cloud.vmware.com/vcloud-usage-meter/

Legal Terms

Use of the Service offering is subject to the standard VMware cloud service offering Terms of Service located at https://www.vmware.com/download/eula.html. Use of the vCloud Usage Meter is subject to VMware’s End User License Agreement, found at https://www.vmware.com/download/eula.html.

2. Service Operations

The following sections outline VMware’s roles and responsibilities in the delivery of vCloud Usage Insight. While specific roles and responsibilities have been identified as being owned by you, any roles or responsibilities not included in this Service Description are either not provided with the Service Offering or are assumed to be your responsibility.

2.1 Support

VMware will provide support for problems that you report and selected additional services to assist with adoption of and related to the Service Offering. Support may be provided in any country in which VMware or its providers maintain facilities. To the extent you provide Content (as defined in the Terms of Service) in connection with support requests, VMware will handle Content in any such country in accordance with the Terms of Service.

2.2 Service Provisioning

VMware will provide the following provisioning services:

- Creating an on-boarding link and invite
- Entitling partner access to the Service Offering

2.3 Incident and Problem Management

VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to availability of the Service Offering.

2.4 Change Management

VMware will provide the following change management services:

- Processes and procedures to maintain the health and availability of the Service Offering.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Service Offering.
- You are responsible for installing and upgrading to new releases of the VMware Usage Meter for new features and bug fixes.

2.5 Security

The end-to-end security of the Service Offering is shared between VMware and you. VMware will provide security for the aspects of the Service Offering over which it has sole physical, logical, and administrative level control. You are responsible for the aspects of the Service Offering over which you have administrative level access or control. The primary areas of responsibility between VMware and you are outlined below.

Rev. 13 Sept 2019
VMware will use commercially reasonable efforts to provide:

- **Physical Security**: VMware will protect the data centers housing the Service Offering from physical security breaches.
- **Information Security**: VMware will protect the information systems used to deliver the Service Offering over which it has sole administrative level control.
- **Network Security**: VMware will protect the networks containing its information systems up to the point where you have some control, permission, or access to modify your networks.
- **Security Monitoring**: VMware will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offering over which it has sole administrative level control. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.
- **Patching and Vulnerability Management**: VMware will maintain the systems it uses to deliver the Service Offering, including the application of patches it deems critical for the target systems. VMware will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner.

You are responsible for addressing the following:

- **Information Security**: You are responsible for ensuring adequate protection of the information systems, data, content or applications that you deploy and/or access with the Service Offering. This includes, but is not limited to, any level of patching, security fixes, data encryption, access controls, roles and permissions granted to your internal, external, or third-party users, etc.
- **Network Security**: You are responsible for the security of the networks over which you have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, etc.
- **Security Monitoring**: You are responsible for the detection, classification, and remediation of all security events that are isolated with your Service Offering account, associated with virtual machines, operating systems, applications, data or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate and which are not serviced under another VMware security program.