Technical White Paper: **September 2023**

SDDC Audit Log Events

VMware Cloud on AWS

vmware®

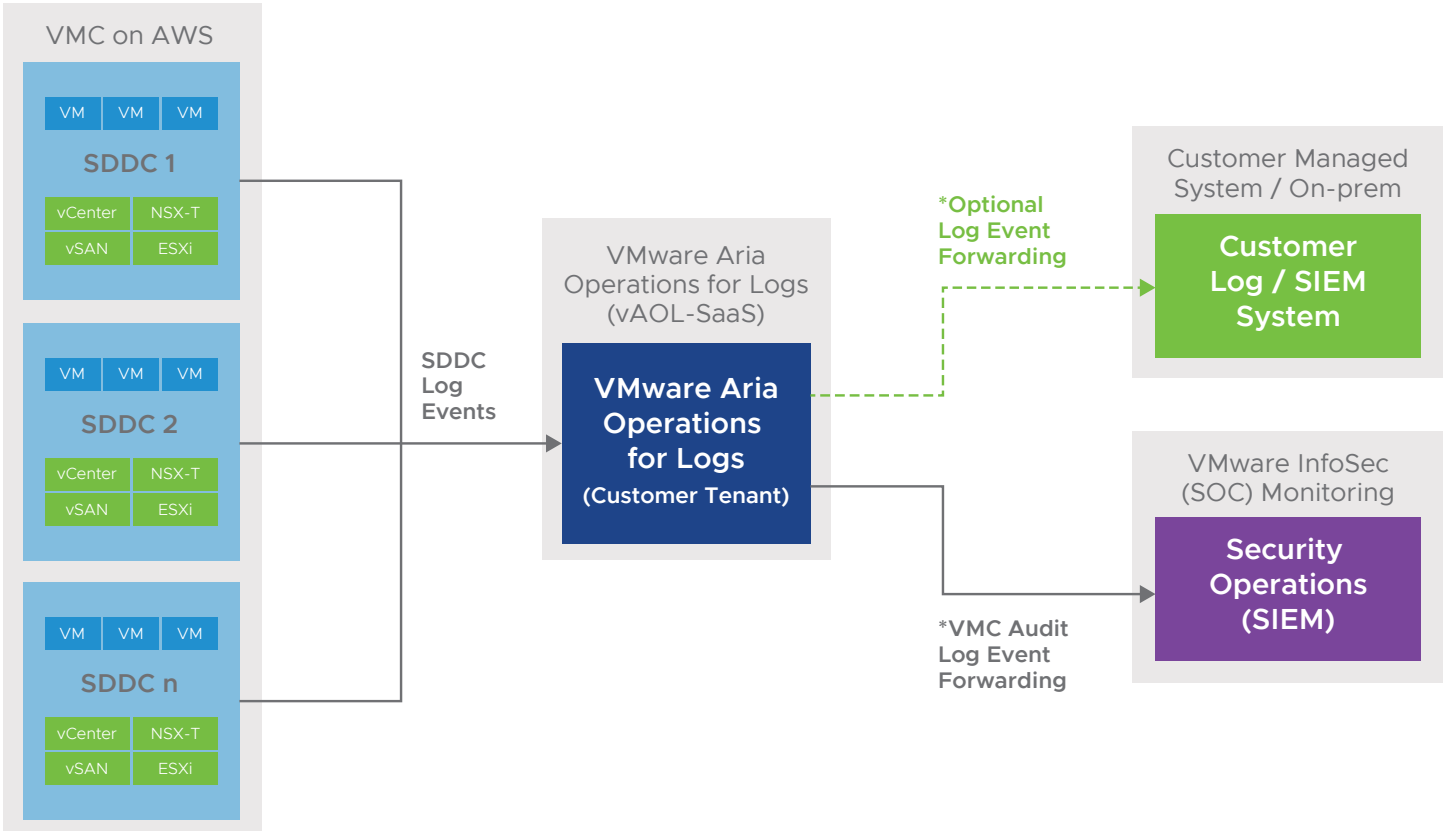
Table of contents

Introduction

VMware Cloud on AWS (VMC) is a modern Infrastructure as a Service offering that enables customers to run VMware vSphere workloads in the AWS Cloud. This whitepaper will describe various aspects of the VMware Cloud on AWS Software Defined Datacenter (SDDC) and audit log events.

VMC Logging Pipeline Overview

The diagram below depicts the high-level logging flows in the VMware Cloud on AWS service. Log events generated by the SDDC Management Components (vCenter, NSX, and vSAN) as well as log events generated by VMC Operations services are forwarded to the log aggregation portal VMware Aria Operations for Logs – SaaS (vAOL-SaaS), formerly vRealize Log Insight Cloud. Within your dedicated VMware vAOL-SaaS tenant instance, you can view, query, and analyze log event data. If you require the use of your log event data externally, you have the option to configure log forwarding from vAOL-SaaS to another system outside of VMware Cloud on AWS. To address VMware's security and compliance obligations for SDDC and Cloud Platform systems security monitoring, SDDC and VMC Operations audit log events are forwarded to the VMware security information and event management (SIEM) system.



Customer SDDC Log Storage Location Options

By default, VMware customer SDDC log events are sent to an instance of vAOL-SaaS residing in the USA (AWS US-West region). Customers with log locality requirements can request for their SDDC log events to be sent to one of our global vAOL-SaaS instances by submitting a support request. Optional customer log storage locations include Asia-Pacific (Sydney), Asia-Pacific (Mumbai), Canada (Montréal), and Europe (Frankfurt). For more information, refer to (Migrating Logs to a New Region).

SDDC Audit Log Events

VMware Cloud on AWS SDDC audit log events are necessary to record administrator activities and access in the context of security and the event. VMware SDDC audit log events contain the "who, what, where, and when" with the same level of transparency as vSphere on-prem environments. Customers will also see actions taken by VMware Support – Site Reliability Engineering, captured within the SDDC audit log events in the customer's vAOL-SaaS instance log aggregation portal. VMware has auditor validated standard processes that meet strict industry compliance standards for log management, including log generation, security, transmission, storage, analysis, retention, and disposal.

VMware audit log events are generated by each SDDC management component (VMware vCenter, NSX-T, vSAN, ESXi, and VMware Add-on Services). 3rd party compliance auditors have verified VMware's SDDC audit logs to ensure that VMware security policies, procedures, and processes are performed in compliance with industry recognized regulations like HIPAA, ISO 27001, ISO 27017, ISO 27018, IRAP, ISMAP, MTCS, OSPAR, PCI-DSS, and SOC 2. Information about VMware Compliance and Privacy programs can be found at Trust Center - VMware and information about centralized SDDC log management can be found at Using VMware Aria Operations for Logs (SaaS).

SDDC Audit Log Components: vCenter, NSX, vSAN, & ESXi

VMware management systems generate audit log events that contain common industry-standard audit log fields. The information found in VMware Cloud on AWS SDDC audit log events is required to identify administrator activities for security monitoring and to support a forensic investigation.

- Time access or change occurred.
- System affected.
- Identify the user or system account related to the activity.
- Identify action or activity (changes to the system).

Common VMware
log _ timestamp
appname
component
event _ type
hostname
org_id
region
sddc id
user/username
source
source hostname

SDDC Management Components (Sample SDDC Audit Log Events)

Some SDDC audit log events may include the customer source IP address:

<99>1 2022-03-24T15:47:04.844Z NSX-Manager-0 NSX 28839 SYSTEM [nsx@6876 audit=true comp=nsx-manager level=INFO subcomp=http] UserName=cloud_admin@10.10.10.6, ModuleName=ACCESS_CONTROL, Operation=LOGIN, Operation status=success");

Some SDDC audit log events may include the customer admin's email address:

<99>1 2022-03-28T18:15:50.263Z NSX-Manager-1 NSX6190 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="0db8582a-bb09-442f-a33c-7ce642843383b" subcomp="policy" username="customer_admin_name@domain.com"] UserName="customer_admin_name@domain.com", ModuleName="PolicyGroupRealization", Operation="GetGroupVMMembers", Operation status="success", New value=["mgw" "PrivateIP_address_Test" {"page_size":1000,"include_mark_for_delete_objects":false}]

VMware Cloud Services Product (CSP) Audit Log Events

The VMware Cloud Services Console is how customers manage the organization, billing, identity, and access to VMware Cloud on AWS. The Activity Log within the Cloud services Console displays events for the last 6 months only. Customers can view additional events and log data in vAOL-SaaS. For more information about VMware Cloud services Product features: Using VMware Cloud Services Guide. For more information about CSP audit log events: Auditing event logs in VMware Cloud Services.

SDDC Administrator Identifiers in VMware SDDC Log Events

Both customers and VMware are responsible for addressing ongoing developments in individual privacy protections under GDPR and other regulations. VMware must include the minimum information in SDDC audit log events to maintain security and compliance requirements while also providing customers with options to safeguard individual privacy.

Customers are responsible for managing identity and access to VMware systems. Customers have options to configure identity and access to avoid 'personal' data identifiers from being recorded in VMware SDDC audit logs.

Personal Data Category	Personal Data Attributes	Purpose of Processing
Identity Details	First Name, Last Name, and Email address of customer's IT administrator(s)	Service functionality such as role-based access controls, alerting, and user identification. Note that VMC on AWS allows customers to anonymize the identity details of customers' IT administrators (names and email addresses). For example, instead of using real names, customers can use aliases such as ADMIN1234, ADMIN2468, etc.
Online Identifiers	IP addresses of customer's IT administrator(s)	Service functionality such as role-based access controls, alerting, and user identification.

If required, you can take steps to change how your administrators' names and email addresses are recorded in VMware SDDC audit log events. The individual's name and email address can be anonymized by substituting values that do not personally identify the individual.

Customer administrators can also choose to use a VPN or Web proxy to connect to VMware systems to prevent the individual administrator's personal IP addresses from being recorded in VMware SDDC audit log events.

VMware – SDDC Log Event Security

VMware Cloud on AWS SDDC log events are forwarded to each customer's vAOL log aggregation tenant within seconds of activity from each management component (vAOL-SaaS has free and paid options available; see Using VMware Aria Operations for Logs (SaaS)). To enable SRE troubleshooting, SDDC logs are also sent to the SRE log tenant and stored for up to 30 days.

VMware log management systems and processes protect the confidentiality, integrity, and availability of audit log event data. VMware security and compliance controls are enabled to ensure end-to-end log data immutability (audit log files are encrypted in transit and at rest). To support compliance requirements and forensic investigations of potential security incidents, SDDC audit log events are securely stored in the VMware SIEM storage for up to 3 years and automatically deleted by storage policy (log management is based on regulatory compliance requirements: HIPAA, ISO 27001, ISO 27017, ISO 27018, IRAP, ISMAP, MTCS, OSPAR, PCI-DSS, and SOC 2).

Customer - SDDC Audit Log Retention, Event Monitoring, and Analysis

vAOL-SaaS features robust log aggregation and sophisticated analytics capabilities that enable customers to determine the root causes of issues quickly and thoroughly. Customers with a VMware Cloud on AWS trial subscription or a VMware Cloud core subscription for vAOL-SaaS, can view and analyze log events generated from vCenter, NSX, vSAN, and CSP to monitor for suspicious behavior in near real-time. For information about vAOL-SaaS subscriptions, refer to: VMware Aria Operations for Logs (SaaS) Subscriptions and Billing.

Customers can configure vAOL-SaaS to archive log data if they want to retain logs older than 30 days (the default retention period). To meet security and compliance objectives, customers may also choose to forward SDDC audit log events to a security information and event management (SIEM) solution to further analyze logs and monitor for threats. Some customers also use vAOL-SaaS to forward SDDC audit log events to VMware Aria Operations for Logs, (VMware's on-premises solution), Splunk, Amazon S3 bucket, or another HTTP endpoint. For information about vAOL-SaaS setup, refer to: Forwarding, Retaining, and Archiving Logs.

VMware - Global Security Operations Center

The VMware SOC is managed by a separate VMware organization and staffed with a team of highly trained VMware employee security analysts. The VMware global security operations team leverages a centralized SIEM solution located in the United States to monitor VMware Cloud on AWS and the global portfolio of VMware's services 24x7x365.

VMware - SOC SDDC Audit Log Event Monitoring

VMware Cloud on AWS SDDC and CSP audit log events are automatically forwarded from source systems and processed in near real-time using rule-based, statistical correlation, and machine-learning methods to detect potential security issues. Security data aggregation enables VMware SOC analysts to effectively monitor the fleet of global systems and respond quickly to security alerts. Audit logs are correlated with other monitoring data from platform systems audit logs, identity and access systems, security configuration and monitoring tools, and threat intelligence feeds to detect, alert, investigate, and respond to potential incidents. If a security incident is detected by the VMware SOC, they will work with the VMware incident response and SRE teams to quickly take steps to address the risk and notify customers with relevant information without delay.

Shared Responsibility Model for VMware Cloud on AWS

Shared responsibility models are commonly used to clarify how the cloud provider and customer actively contribute to maintaining the security of the cloud environment. VMware SDDC audit log events provide important insight into administrative actions taken in the cloud environment and enable the customer and provider to monitor for suspicious activity. Audit log events generated from the SDDC and CSP enable the cloud provider to monitor activity related to the SDDC and cloud platform. Audit log events also enable customers to monitor activity related to the configuration of the SDDC and day-to-day VMware virtual infrastructure administration.

Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the configuration work you need to perform as part of your security responsibilities, customers are responsible for managing data (including in-guest encryption options), classifying assets, and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware responsibility "Security of the Cloud" – VMware is responsible for helping to protect the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles that customers use to provision their SDDCs in VMware Cloud on AWS.

The matrix below describes the VMware Cloud on AWS shared responsibility model and what management operations VMware and customers are responsible for.

Resource	Deployment	Lifecycle	Configuration
Service Consoles			
console.cloud.vmware.com	VMware	VMware	Customer
vmc.vmware.com	VMware	VMware	Customer
Cloud Platform Infrastructure			
Provider VPC	VMware	VMware	VMware
Customer VPC	Customer	Customer	Customer
Bare Metal Hosts	VMware	VMware	VMware
VMware ESXi	VMware	VMware	VMware
VMware vCenter Server	VMware	VMware	VMware
VMware vSAN	VMware	VMware	VMware
VMware NSX-T	VMware	VMware	VMware

Resource	Deployment	Lifecycle	Configuration
SDDC Management & Workloads			
Management Gateway	VMware	VMware	Customer
Compute Gateway	VMware	VMware	Customer
Virtual Machines, OS, Applications	Customer	Customer	Customer
Network Segments	Customer	Customer	Customer
VMware Cloud on AWS Add-On services	Customer	VMware	Customer
ISOs and OVAs	Customer	Customer	Customer
Guest Operating Systems	Customer	Customer	Customer
Logs (vCenter, vSAN, NSX, and CSP)	Customer	Customer	Customer

VMware – Cloud Platform Security Responsibilities

VMware Cloud on AWS automates the deployment and lifecycle of the cloud platform. VMware is responsible for ensuring the availability, stability, performance, and security of the cloud platform (SDDC appliances, SDDC infrastructure, and SaaS service architecture).

Related Resources

For more information about VMware Cloud on AWS, refer to:

- VMware Cloud on AWS Shared Responsibility Model
- VMware Cloud on AWS Privacy Data Sheet
- VMware Cloud on AWS Service Description

Item No: 81395 SDDC Audit Log Events Whitepaper - Design 9/23