VMware Advanced Cyber Compliance (ACC) Frequently Asked Questions (FAQs)

Table of Contents

General Questions

Q. Is ACC only available to VCF customers?

A. Yes

Q. What is included in the ACC Advanced Service today?

A. ACC customers have exclusive access to the below capabilities

- Continuous compliance monitoring and remediation for workloads and VCF stack components
- Full DR replication, automation and orchestration (on-premises)
- Integrated cyber recovery with embedded EDR and guided workflow automation
- Multi-tenant disaster recovery integrated into VCF Automation
- Confidential computing
- Policy-based VPC connectivity

Continuous Compliance Enforcement at Scale powered by VMware Salt

Q. What is the primary function of VMware Salt?

A. VMware Salt is a continuous compliance and configuration management component. VMware Salt manages the state of the virtual machine to ensure that software is installed, services are running, and security patches are applied, correcting any "drift" automatically.

Q. Is VMware Salt the same as open-source Salt?

A. VMware Salt is built on top of open-source Salt. ACC powered by VMware Salt adds an enterprise-level management GUI on top of open-source which provides RBAC, Job Scheduling, Reporting and more. SecOps security compliance and vulnerability scanning are also done via the VMware Salt GUI.

Q. How are the capabilities provided by VMware Salt within ACC different from what's available to customers with core entitlements in VCF Ops?

A. In VCF 9.1, compliance and configuration management transitioned into the VMware Advanced Cyber Compliance Advanced Service. To perform active security posture management, configuration drift visibility, and full-scale compliance management within VCF Operations, customers will require the ACC Advanced Service.

Customers with a standard VCF entitlement can use the Security Operations Dashboard (a centralized view to monitor the overall security health and encryption status of the environment) and Audit Trail Visibility (detailed logging and tracking of user actions and system changes to support forensic analysis).

VMware Salt *Workload management (requires ACC)*	**VCF Operations** *VCF stack management (requires ACC)*
Configuration management/drift with remediation	Configuration management visibility
Compliance (CIS/DISA) and vulnerability (CVEs) scans and remediation	Compliance management (PCI, VCF hardening) and remediation (VCF Operations 9.0) Security posture management (VCF Operations 9.1)
Remote execution and orchestration	Protection and recovery

Q. What compliance standards does ACC with VMware Salt and VCF Operations support?

A. VCF Operations supports the following for VCF components:

- PCI DSS for VCF 9 is the baseline for hardening and auditing guidance for VMware Cloud Foundation
- VCF 9.x Security Configuration Guide is the baseline for hardening and auditing guidance for VMware Cloud Foundation.

VMware Salt supports the following for workloads and operating systems such as Linux and Windows:

- Center for Internet Security (CIS)
- DISA STIG Benchmarks.

Q. What are the VMware Salt components?

A. VMware Salt architecture consists of a handful of system components that work together and interact with each other. The three main components are:

- VMware Salt RaaS (Returner-as-a-Service) (GUI)
- Salt Master
- Salt Minion

Additional components need to be installed as well as pre-requisites:

- postgreSQL database
- valley database

Q. Can VMware Salt be licensed as a standalone service?

A. VMware Salt is only available to customers as part of ACC and cannot be purchased as a standalone service.

Q. How does VMware Salt impact operational efficiency and staff time?

A. VMware Salt automates manual patching of infrastructure and day-to-day administration tasks, which will save on staff time and results in more consistency with fewer errors. VMware Salt can also enforce state on a schedule and/or react to changes and automatically remediate changes.

Q. How does VMware Salt offer visibility into an organization's level of security?

A. VMware Salt provides visibility into compliance and vulnerabilities within Linux and Windows OS's via scans

that can be run manually or programmatically. Also the system can remediate findings to bring the environment back into compliance and patched. This simplifies the continuous visibility and maintenance of system configurations.

Q. Which parts of ACC provide monitoring and remediation for workloads and VCF stack components?

A. VCF Ops provides monitoring and remediation for VCF stack components. VMware Salt provides remediation for workloads.

Q. Does ACC provide reporting to help IT teams meet audit requirements?

A. ACC provides reporting in VCF Ops for VCF reports and VMware Salt provides a json download with the results of the Compliance scans and remediations.

Automated Cyber and Disaster Recovery

Q. Are cyber and disaster recovery capabilities available as part of the core VCF entitlement?

A. Customers with core VCF entitlements benefit from operational recovery only (local snapshots) and would require ACC licenses for orchestrated disaster and cyber recovery capabilities.

Q. What protection and recovery capabilities are covered in ACC entitlement?

- vSAN ESA based operational recovery snapshot replication to a remote site
- Enhanced vSphere Replication with RPOs as low as one minute
- Disaster recovery runbook orchestration
- End-to-end cyber recovery workflow automation with integrated EDR and choice between Carbon Black (default) and Crowdstrike Falcon (BYOL)
- Tenancy-aware VM replication for disaster recovery natively built in VCF Automation requires standalone SRM or ACC entitlements

Q. For cyber and disaster recovery, what is the difference between features available with ACC and Site Recovery Manager (SRM) entitlements?

	Advanced Cyber Compliance (ACC)	Site Recovery Manager (SRM)
VMware Cloud Foundation	Yes	Yes
vSphere Foundation	No	Yes
Cyber Recovery orchestration	Yes	No
Disaster Recovery orchestration	Yes	Yes
Tenancy-aware VM replication	Yes	Yes

Q. Do customers who want to use Crowdstrike for cyber recovery need to bring their own license (BYOL)?

A. ACC cyber recovery includes built-in restore point validation at no additional cost to the customer. However, if the customer chooses to use Crowdstrike as the EDR to test and validate workloads before recovery, they will need to bring their own license (BYOL). This shouldn't result in additional costs to the customer as Crowdstrike licenses in the production site can be ported over to the recovery site while the primary is down. Customers who choose to use Crowdstrike as the EDR for restore point validation will benefit from the same level of integration into the end-to-end cyber recovery workflow offered by ACC.

Q. Can ACC customers recover to a cloud isolated clean room?

A. No, ACC is available only for on-premises VCF environments. Customers looking to leverage cloud-based DR and/or cyber recovery will be required to purchase VMware Live Recovery Cloud along with the associated cloud hosts and storage.

Q. Does ACC support DR and cyber or disaster recovery for containerized applications?

A. At this time, ACC does not support cyber recovery for containerized applications.

Q. Does ACC support DR multi-tenancy?

A. Yes

Q. Does ACC require me to manually integrate EDR capabilities into the isolated clean room?

A. No, EDR integration (Carbon Black as a default, Crowdstrike as a BYOL) is included as part of the ACC license and does not require manual stitching into the cyber recovery workflow.

Q. Does ACC support file and folder-level restore?

A. Yes

Q. Can customers choose between different topologies for the VCF isolated clean room?

A. There are three options customers can choose from to set up their isolated clean rooms for cyber recovery, based on their specific budget and risk management requirements.

1. Dedicated clean room physically separated from disaster recovery site
2. Clean room shared with disaster recovery site with logical separation
3. Clean room on production site with logical separation

Q. Are the snapshots taken by the application consistent?

A. No, the snapshots are crash consistent.

Q. How do I get the license for cyber and/or disaster recovery in ACC?

A. As part of the fulfillment process, a welcome email is sent which has instructions to onboard. Follow instructions here.

Q. Do I need to go to Broadcom Support Portal to get the license keys for cyber and/or disaster recoveryin ACC?

A. No, the license keys should not be used. Follow the instructions here to get onboarded.

Q. Am I eligible to use cyber recovery if I've purchased VMware Live Recovery subscriptions?

A. Yes, if you've purchased VMware Live Recovery subscriptions on or after March 2024 then you are entitled to Cyber Recovery capabilities given that

1) You have carved out VMware Live Recovery licenses by onboarding through Cloud Console (license keys will not work)
2) You have all the other necessary requirements of Clean Room like vSAN ESA and vDefend.

Q. Do I require vSAN ESA on the isolated clean room (recovery site) for cyber recovery?

A. Yes, vSAN ESA with VCF 9.1 is required on the isolated clean room (recovery site).

Q. Do I require vSAN on a protected site?

A. No. Any storage is supported on protected site but do require vSAN for local snapshot (operational recovery).

Q. Do I require NSX on the protected site?

A. No. However, vDefend is required on the recovery site for VM network isolation.

Q. Do I need to build VPCs on a recovery site?

A. Yes, for cyber recovery

Enhanced Platform Security

Q. What confidential computing capabilities are available to ACC customers, and what benefits do they provide?

A. The base functionality includes turning on confidential computing on Intel and AMD based servers specifically for Intel TDX and AMD SEV-SNP respectively. In 9.1, this functionality will become generally available as part of ACC. Additionally, incremental features such as Quick Boot for confidential VMs will be available.

Q. Is confidential computing capability included with VCF?

A. No, confidential capability will only be available with ACC.

Q. Is Intel TDX supported with all versions of Intel processors?

A. No, Intel TDX capability is available with 5th Gen Intel® Xeon Scalable and Intel® Xeon® 6 processors. See here for more information.

Q. Is AMD SEV-SNP supported with all versions of AMD processors?

A. No, AMD EPYC™ 7003 and later processors support SEV-SNP. For full matrix of capabilities for AMD SEV support see here.

Q. How is VPC connectivity in core VCF entitlements different from what's available in ACC?

A. Customers with core VCF entitlements have access to standard VPC connectivity. However, **policy-based** VPC connectivity is only available for ACC customers.

Q. What key benefits does VPC policy-based connectivity provide to ACC customers?

A. VPC policy-based connectivity enables simple policy-based automation without complex firewall rules or external firewalling, efficient use of infrastructure by minimizing required VPC transit gateways, and streamlined compliance management with easier access to consolidated traffic logs across VPC communities.