Health Reporting and Monitoring for VMware Cloud Foundation

Modified on 09 OCT 2024

VMware Cloud Foundation services

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Health Reporting and Monitoring for VMware Cloud Foundation

The *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution provides guidance on monitoring the operational state of your VMware Cloud Foundation environment through ad-hoc reporting or through custom dashboards, alerts, and notifications. The custom dashboards are intended to serve as an extension to native VMware Aria Operations (formerly vRealize Operations) dashboards and dashboards that are enabled by using management packs.

A VMware by Broadcom validated solution is a well-architected and validated implementation, built and tested by VMware to help customers deliver common business use cases. VMware validated solutions are operational, cost-effective, reliable, and secure. Each solution contains a detailed design, implementation, and operational guidance.

Automation for This Design in VMware Cloud Foundation

To provide a fast and efficient path to automating the *Health Reporting and Monitoring for VMware Cloud Foundation* implementation, this document provides Microsoft PowerShell cmdlets using an open-source module as code-based alternatives to completing each procedure in the respective component's user interface.

For additional information, see PowerShell Module for VMware Validated Solutions.

Intended Audience

The *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution is intended for users who regularly monitor the health of their VMware Cloud Foundation environment, such as virtual infrastructure, storage, and network administrators, DevOps, site resiliency engineers, and other types of operators. Users can also use this solution to monitor the health of their environment, in ad-hoc scenarios, as well as prepare for planned and unplanned events.

Support Matrix

The *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution is compatible with specific versions of the VMware products that are used for implementing the solution.

Table 1-1. Software Components in Health Reporting and Monitoring for VMware Cloud Foundation

VMware Cloud Foundation Version	Product Group	Component Versions
5.2.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.2.1 Release Notes.
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.3
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.2
5.2.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.2.0 Release Notes.
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.3
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.2
5.1.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.1.1 Release Notes.
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.2
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.1.2
5.1.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.1.0 Release Notes.
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.0
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.1.0

Table 1-2. End of General Support Software Components in *Identity and Access Management for VMware Cloud Foundation*

VMware Cloud Foundation Version	Product Group	Component Versions
5.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.0 Release Notes. VMware Aria Suite Lifecycle 8.10.0 (EOGS)
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.0

Table 1-2. End of General Support Software Components in *Identity and Access Management for VMware Cloud Foundation* (continued)

VMware Cloud Foundation Version	Product Group	Component Versions
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.1.0
4.5.2	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.5.2 Release Notes. VMware Aria Suite Lifecycle 8.10.0 (EOGS)
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.0
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.1.0
4.5.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.5.1 Release Notes vRealize Suite Lifecycle Manager 8.8.2 (EOGS)
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.0
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.1.0
4.5.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.5.0 Release Notes. vRealize Suite Lifecycle Manager 8.8.2 (EOGS)
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.6.0
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 2.1.0
4.4.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.4.1 Release Notes. vRealize Suite Lifecycle Manager 8.6.2 (EOGS)
	Solution-added components	Host virtual machine
		PowerShell module for VMware Cloud Foundation Reporting 2.1.0
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 1.1.0
4.4.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.4.0 Release Notes. vRealize Suite Lifecycle Manager 8.6.2 (EOGS)
	Solution-added components	Host virtual machine

Table 1-2. End of General Support Software Components in *Identity and Access Management for VMware Cloud Foundation* (continued)

VMware Cloud Foundation Version	Product Group	Component Versions
		PowerShell module for VMware Cloud Foundation Reporting 2.1.0
		Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations 1.1.0

Note The software component versions in this table are in End of General Support (EOGS) phase and are no longer generally supported by VMware. At the time of initial release and during the General Support phase, the software component versions in this solution are actively implemented, tested, and validated by VMware and VMware partners. See VMware Lifecycle Policies.

Before You Apply This Guidance

To design and implement the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution, your environment must have a certain configuration.

Table 1-3. Supported VMware Cloud Foundation Deployment

Workload Domain / Component	Deployment Details
Management domain	■ Automated deployment by using VMware Cloud Builder™. See the following VMware Cloud Foundation Documentation: ■ For information on designing the management domain, see VMware Cloud Foundation Design Guide. ■ For information on deploying the management domain, see Getting Started with VMware Cloud Foundation and VMware Cloud Foundation Deployment Guide. ■ For information on operating the management domain, see VMware Cloud Foundation Administration Guide and VMware Cloud Foundation Operations Guide.
One or more virtual infrastructure (VI) workload domains	Automated deployment by using SDDC Manager. See the following VMware Cloud Foundation Documentation: ■ For information on designing a VI workload domain, see VMware Cloud Foundation Design Guide. ■ For information on deploying the VI workload domains, see Getting Started with VMware Cloud Foundation and VMware Cloud Foundation Administration Guide. ■ For information on operating the VI Workload domain, see VMware Cloud Foundation Operations Guide.
VMware Cloud Foundation integrated with Active Directory	Manual or PowerShell automated configuration of Active Directory over LDAP. See the Identity and Access Management for VMware Cloud Foundation validated solution.
VMware Cloud Foundation integrated with Intelligent Operations.	Manual or PowerShell automated deployment of VMware Aria Operations. See the Intelligent Operations Management for VMware Cloud Foundation validated solution.

Overview of Health Reporting and Monitoring for VMware Cloud Foundation

By applying the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution, you gain operational insights across the availability, health, and compliance of your VMware Cloud Foundation instance.

Table 1-4. Implementation Overview of *Health Reporting and Monitoring for VMware Cloud Foundation*

Stage	Steps
1. Plan and prepare the VMware Cloud Foundation environment.	1 Work with the technology team of your organization to configure the physical servers, network, and storage in the data center. Collect the environment details and write them down in the VMware Cloud Foundation Planning and Preparation Workbook.
2. Install and configure the PowerShell Module for VMware Cloud Foundation Reporting.	1 Deploy and configure a host virtual machine. 2 Install the PowerShell Module for VMware Cloud Foundation Reporting and supporting PowerShell modules from the PowerShell Gallery.
3. Install and configure the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.	1 Install and configure the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations and its dependencies. 2 Install the Python client for VMware Aria Operations. 3 Configure VMware Aria Operations with the provided monitoring artifacts - dashboards, views, super metrics, alerts, and notifications.

Frequently Asked Questions

For additional questions, see VMware Validated Solutions Frequently Asked Questions.

Update History

The *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution is updated when necessary.

Revision	Description
09 OCT 2024	■ This validated solution now supports VMware Cloud Foundation 5.2.1. ■ The `PowerValidatedSolutions` PowerShell module is now version 2.12.0. ■ The `VMware.PowerCLI` PowerShell module is now version 13.3.0. ■ The `ImportExcel` PowerShell module is now version 7.8.9.
23 JUL 2024	■ This validated solution now supports VMware Cloud Foundation 5.2.0. ■ This validated solution now provides a single procedure for PowerShell automation. See Automated PowerShell Implementation of Health Reporting and Monitoring ■ The `PowerValidatedSolutions` PowerShell module is now version 2.11.0.

Revision	Description
28 MAY 2024	■ This solution now supports Dell VxRail nodes for both standard and consolidated architectures. ■ The PowerShell module for VMware Cloud Foundation Reporting is now version 2.6.2. ■ The Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations is now version 2.1.2 ■ The `PowerValidatedSolutions` PowerShell module is now version 2.10.0.
26 MAR 2024	■ This validated solution now supports VMware Cloud Foundation 5.1.1. ■ The `PowerValidatedSolutions` PowerShell module is now version 2.9.0. ■ The `VMware.PowerCLI` PowerShell module is now version 13.2.1.
30 JAN 2024	■ This solution now supports VMware Cloud Foundation multi-instance environments. ■ The `PowerValidatedSolutions` PowerShell module is now version 2.8.0.

07 NOV 2023	■ This validated solution now supports VMware Cloud Foundation 5.1.0.
	■ The `PowerValidatedSolutions` PowerShell module is now version 2.7.0.
	■ The `PowerVCF` PowerShell module is now version 2.4.0.
	■ The following solution-added product names are changing:
	  ■ VMware vRealize Operations is now VMware Aria Operations.
	  ■ VMware vRealize Log Insight is now VMware Aria Operations for Logs.
	For more information on the VMware Aria rebranding, see Multi-Cloud Management and VMware Aria.

29 AUG 2023	■ This validated solution now supports VMware Cloud Foundation 4.5.2. ■ The Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations is now version 2.0.0 ■ The PowerShell module for VMware Cloud Foundation Reporting is now version 2.3.0 ■ The `VMware.PowerCLI` PowerShell module is now version 13.1.0. ■ The `ImportExcel` PowerShell module is now version 7.8.5. ■ The `PowerValidatedSolutions` PowerShell module is now version 2.6.0.

Revision	Description
25 JUL 2023	■ This validated solution now supports VMware Cloud Foundation 5.0. ■ The `PowerValidatedSolutions` PowerShell module is now version 2.5.0. ■ The PowerShell module for VMware Cloud Foundation Reporting is now version 2.2.0
30 MAY 2023	■ This validated solution now supports VMware Cloud Foundation version 4.5.1. ■ The PowerShell module for VMware Cloud Foundation Reporting is now version 2.1.0 ■ The Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations is now version 1.1.0
28 MAR 2023	Initial release.

Design Objectives for Health Reporting and Monitoring for VMware Cloud Foundation

1

The *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution has objectives to deliver prescriptive content about the solution so that it is fast to deploy and is suitable for use in production environments.

VMware Validated Solution Objective	Description
Main objective	Provide health monitoring for the VMware Cloud Foundation components by using HTML reports and through custom dashboards, alerts, and notifications in VMware Aria Operations.

VMware Cloud Foundation architecture support	vSAN ReadyNodes
	■ Standard
	  ■ Single VMware Cloud Foundation instance
	  ■ Multiple VMware Cloud Foundation instances
	■ Consolidated
	Dell VxRail Nodes
	■ Standard
	  ■ Single VMware Cloud Foundation instance
	  ■ Multiple VMware Cloud Foundation instances
	■ Consolidated

Workload domain type support	■ Management workload domain ■ Virtual infrastructure (VI) workload domain
Scope of implementation	Configuration of solution components: ■ SDDC Manager ■ VMware Aria Operations Installation and configuration of solution components: ■ PowerShell Module for VMware Cloud Foundation Reporting ■ Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations
Scope of guidance	■ Detailed design for solution components. ■ Implementation guidance for solution components. ■ Operational guidance for the solution components, such as operational verification, password management, report generation, and monitoring.

VMware Validated Solution Objective	Description
Cloud type	Private Cloud
Authentication, authorization, and access control	■ Use of SDDC Manager credentials with least-privilege access. ■ Use of VMware Aria Operations credentials with least-privilege access.

Detailed Design for Health Reporting and Monitoring for VMware Cloud Foundation

2

The design considers the components of *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution. It includes numbered design decisions, and the justification and implications of each decision.

Read the following topics next:

- Logical Design for Health Reporting and Monitoring for VMware Cloud Foundation
- Deployment Specification for Health Reporting and Monitoring for VMware Cloud Foundation
- Network Design for Health Reporting and Monitoring for VMware Cloud Foundation
- Life Cycle Management Design for Health Reporting and Monitoring for VMware Cloud Foundation
- Information Security and Access Control Design for Health Reporting and Monitoring for VMware Cloud Foundation

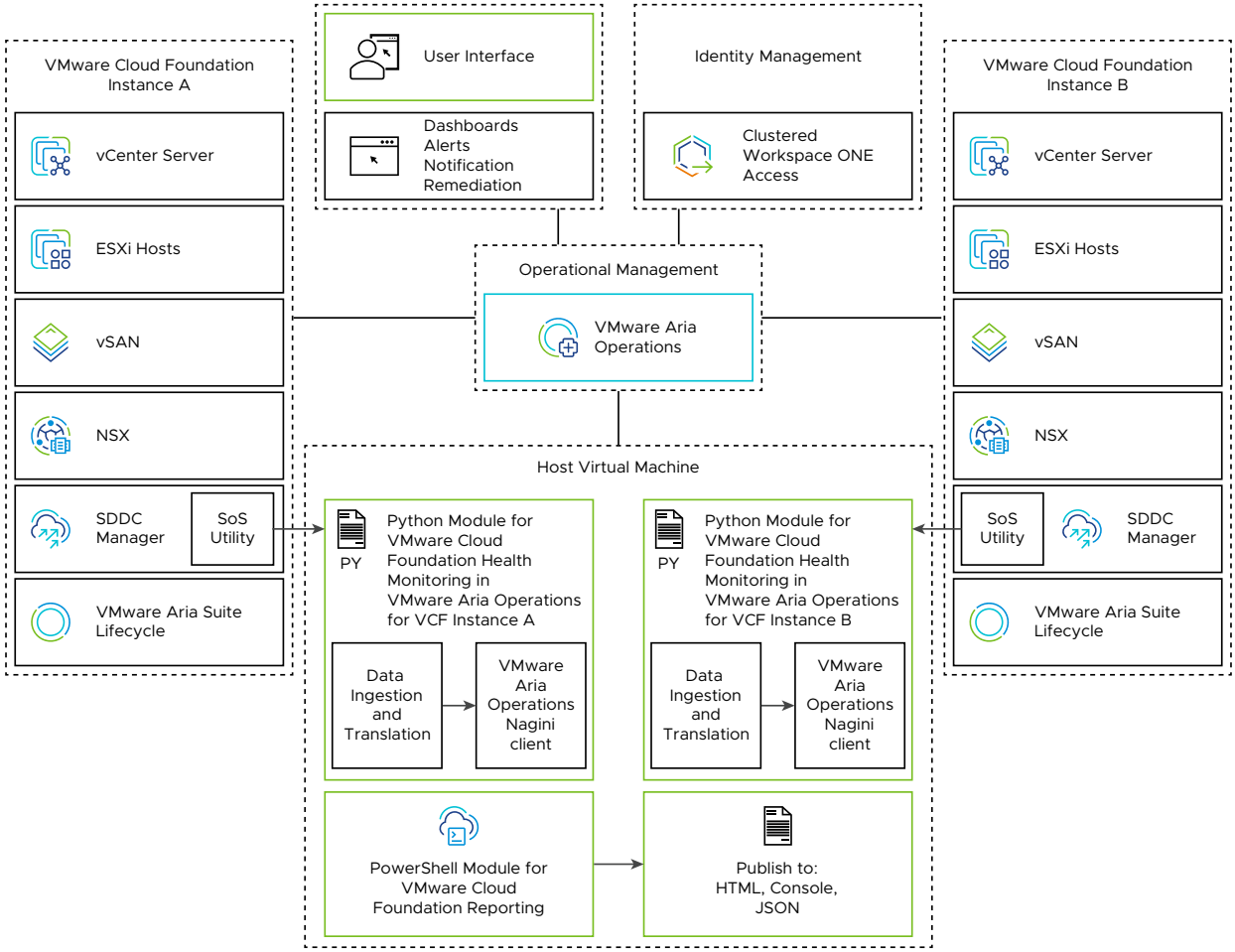
Logical Design for Health Reporting and Monitoring for VMware Cloud Foundation

The logical design provides a high-level overview of the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

Logical Design

The design consists of a host virtual machine deployed in the management domain of your *VMware Cloud Foundation* instance, that hosts the PowerShell module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations. The host virtual machine uses the two modules to periodically connect to the VMware Cloud Foundation Support and Serviceability (SoS) utility and SDDC component APIs to collect health metrics, generate HTML reports, and send the data to VMware Aria Operations. This data is then presented through custom VMware Aria Operations dashboards to provide active health monitoring of your VMware Cloud Foundation instance.

Figure 2-1. Logical Design of Health Reporting and Monitoring for VMware Cloud Foundation



PowerShell Module for VMware Cloud Foundation Reporting

The PowerShell Module for VMware Cloud Foundation Reporting is an open-source PowerShell module that ships with a library of cmdlets that connect to SDDC management components, collect health data, and publish that data in different formats. The cmdlet library contains combined operation, health check, system alert, configuration, and system overview functions. These functions provide insight to the operational state of your VMware Cloud Foundation instance.

The PowerShell module uses the VMware Cloud Foundation Support and Serviceability (SOS) utility as well as SDDC component APIs to collect and publish health data for SDDC Manager, vCenter Server, vSAN, NSX, and VMware Aria Suite Lifecycle. The PowerShell module collects storage, networking, configuration, and security data. You install and configure the PowerShell module on the host virtual machine.

The PowerShell module can generate the following reports:

- System overview report
- Health report

- Alert report
- Configuration report
- Upgrade precheck report

Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

The Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations is an open-source collection of python scripts and VMware Aria Operations artifacts. It uses the VMware Cloud Foundation Supportability and Serviceability (SOS) utility and the supporting PowerShell modules to collect health data for a VMware Cloud Foundation instance and then send this data to objects in VMware Aria Operations as custom metrics for use in dashboards to monitor the platform's health. This enables the creation and configuration of custom dashboards, alerts, notification, and remediation in VMware Aria Operations. You install and configure the Python module on the host virtual machine.

The Python module includes predefined custom VMware Aria Operations dashboards in the VCF Health dashboard group that cover individual component health metrics and an aggregated single pane of glass rollup dashboard.

Table 2-1. Python Module for VMware Cloud Foundation Health Monitoring Predefined VMware Aria Operations Dashboards

Dashboard	Description
VCF Health Rollup	Rollup for all individual dashboards for VCF Health.
VCF Backup Health	Displays the backup status for SDDC Manager, vCenter Servers, and NSX Local Managers.
VCF Certificate Health	Displays the component certificates are valid (within the expiry date).
VCF Compute Health	Displays ESXi health, including host licenses, disk storage, disk partitions, core dumps, free pool, and overall health status. Shows overall health of vCenter Server instances.
VCF Connectivity Health	Displays connectivity health which verifies the connection between SDDC Manager and the underlying components of VMware Cloud Foundation. Includes Ping, SSH connectivity, and API connectivity health checks for SDDC components.
VCF DNS Health	Displays the Forward and Reverse DNS health summary.
VCF Hardware Compatibility	Displays the data from the Hardware Compatibility check which validates ESXi hosts and vSAN devices.
VCF Networking Health	Displays the health of Local NSX Managers, Edge Clusters, Edge Nodes, Transport Nodes, Transport Node Tunnels and Tier-0 Gateway BGP connections.

Table 2-1. Python Module for VMware Cloud Foundation Health Monitoring Predefined VMware Aria Operations Dashboards (continued)

Dashboard	Description
VCF NTP Health	Displays the NTP health which verifies that components have their time synchronized with the NTP server used by SDDC Manager. It also ensures that the hardware and software time stamp of ESXi hosts are within 5 minutes of the SDDC Manager appliance.
VCF Password Health	Displays the password health checking for expiry across the VMware Cloud Foundation instance.
VCF SDDC Manager and vCenter Services Health	Displays service health for services running within SDDC Manager and vCenter Server.
VCF Snapshot Health	Displays the snapshot status for SDDC Manager, vCenter Servers, and NSX Local Managers.
VCF Storage Health	Displays disk capacity health for SDDC Manager, vCenter Servers, ESXi hosts, and datastores. Also displays VMs with Connected CD-ROMs.
VCF vSAN Health	Displays vSAN health across ESXi hosts and vSphere clusters.
VCF Version Health	Displays the component version and compares it with SDDC Manager inventory, the actual installed Bill of Materials (BoM) component version, and the BoM component versions to detect any drift.

Table 2-2. Logical Components for Health Reporting and Monitoring

Single VMware Cloud Foundation Instance with a Single Availability Zone	Single VMware Cloud Foundation Instance with Multiple Availability Zones	Multiple VMware Cloud Foundation Instances
A host virtual machine is deployed on the management VLAN in the management domain.	■ A host virtual machine is deployed on the management VLAN in the management domain. ■ A vSphere Distributed Resource Scheduler VM/Host rule ensures that the host virtual machine is running on an ESXi host group in the first availability zone of the management domain.	In the first VMware Cloud Foundation instance, a host virtual machine is deployed on the management VLAN in the management domain.

Deployment Specification for Health Reporting and Monitoring for VMware Cloud Foundation

The deployment specification details the design decisions covering physical design.

Deployment of the Host Virtual Machine

You deploy a host virtual machine to the management domain vCenter Server instance. You then install both the PowerShell Module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations. The modules collect data from SDDC Manager and SDDC management components to create HTML reports, or populate custom dashboards, and generate alerts and notifications in VMware Aria Operations.

Table 2-3. Design Decisions for Deployment of a Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-CFG-001	Deploy the host virtual machine using a supported guest operating systems (VMware Photon OS or Microsoft Windows Server).	A dedicated host virtual machine is deployed to ensure isolation of the PowerShell and Python modules from other production components.	The host virtual machine must be deployed, configured, and maintained outside of VMware Cloud Foundation automated workflows.
HRM-VM-CFG-002	Deploy the host virtual machine in the default management vSphere cluster.	Required to communicate with SDDC Manager and VMware Aria Operations.	The host virtual machine must be able to connect to SDDC Manager and VMware Aria Operations.
HRM-VM-CFG-003	Protect the host virtual machine by using vSphere High Availability.	Supports the availability objective without requiring manual intervention during an ESXi host failure.	None.
HRM-VM-CFG-004	Place the host virtual machine in a designated virtual machine folder.	Provides organization of the appliances in the management domain vSphere inventory.	You must create the virtual machine folder during deployment.

Deployment of the Host Virtual Machine in Multiple Availability Zones

In an environment with multiple availability zones, the host virtual machine runs in the first availability zone. If a failure occurs in the first availability zone, the virtual machine fails over to the second availability zone.

Table 2-4. Design Decisions for Deployment of the Host Virtual Machine in Multiple Availability Zones

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-CFG-005	When using two availability zones, add the host virtual machine to the VM group of the first availability zone.	Ensures that the host virtual machine runs in the primary availability zone hosts group.	After the implementation of the second availability zone for the management domain, you must update the VM group for the primary availability zone virtual machines to include the host virtual machine.

Deployment of the Host Virtual Machine for Multiple VMware Cloud Foundation Instances

In a VMware Cloud Foundation multi-instance environment, you deploy the host virtual machine in the management cluster in the first VMware Cloud Foundation instance.

Table 2-5. Design Decisions for Deployment of the Host Virtual Machine for Multiple VMware Cloud Foundation Instances

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-CFG-006	In an environment with multiple VMware Cloud Foundation instances, deploy the host virtual machine in the management vSphere cluster in the first VMware Cloud Foundation instance.	Required to communicate with SDDC Manager in each VMware Cloud Foundation instance and VMware Aria Operations.	The host virtual machine must be able to connect to SDDC Manager in each VMware Cloud Foundation instance and VMware Aria Operations.

Sizing Compute and Storage Resources

The host virtual machine has the following resource requirements.

Table 2-6. Sizing Compute and Storage Resources

Operating System	CPU	Memory	Storage
Photon OS	1	2 GB	■ 662 MB (Thin Provisioned) ■ 16 GB (Thick Provisioned)
Windows Server	2	4 GB	60 GB

Installation of PowerShell Module for VMware Cloud Foundation Reporting

The PowerShell Module for VMware Cloud Foundation Reporting is an open-source PowerShell module that enables you to generate HTML based reports on the health of a VMware Cloud Foundation instance.

Table 2-7. Design Decisions for the PowerShell Module for VMware Cloud Foundation Reporting

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PWSH-CFG-001	Use or install a supported edition and version of PowerShell on the host virtual machine guest operating system.	The PowerShell module cmdlets may fail when run on an edition and version of PowerShell that is not supported by the PowerShell module and its dependencies.	None
HRM-PWSH-CFG-002	Install the PowerShell Module for VMware Cloud Foundation Reporting and its dependencies on the host virtual machine.	The PowerShell Module for VMware Cloud Foundation Reporting is required to generate HTML reports.	None

Installation of Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

The Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations is a Python module that pulls data from SDDC Manager, and uses the VMware Aria Operations Nagini client which is a REST client to push the data to corresponding objects in VMware Aria Operations as custom metrics.

Table 2-8. Design Decisions for the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PY-CFG-001	Install Python 3.x on the host virtual machine.	Python 3 is required to run the Python script that pulls data from SDDC Manager and pushes it to VMware Aria Operations.	In an environment with multiple VMware Cloud Foundation instances, multiple copies of the Python module are installed, each corresponding to a VMware Cloud Foundation instance.
HRM-PY-CFG-002	Install the Nagini client, a Python binding package for VMware Aria Operations, on the host virtual machine.	The Nagini client enables the Python module to send data to VMware Aria Operations.	Manual installation and setup depends on the host virtual machine's operating system.

Table 2-8. Design Decisions for the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations (continued)

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PY-CFG-003	On the host virtual machine, schedule daily runs of the Python module to collect health data from SDDC Manager and send it to VMware Aria Operations.	Automates gathering health data.	Manual installation and setup depends on the host virtual machine's operating system.
HRM-PY-CFG-004	Configure the default log retention for logs, generated by the Python module, to 30 days.	Automatic cleanup of logs generated when the `send-data-to-vrops.py` script saves capacity on the host virtual machine's local disk and ensures old data is removed.	You must manually set the log retention period by configuring the *log_retention_in_days* setting in the `env.json` file.

Network Design for Health Reporting and Monitoring for VMware Cloud Foundation

The network design details the design decisions for the network segment placement, IP addressing, name resolution, and time syncronization of the host virtual machine.

Network Segment

This validated solution places the host virtual machine on the management VLAN of the VMware Cloud Foundation instance. This ensures connectivity and close proximity to SDDC Manager and VMware Aria Operations.

Figure 2-2. Network Design for Health Reporting and Monitoring

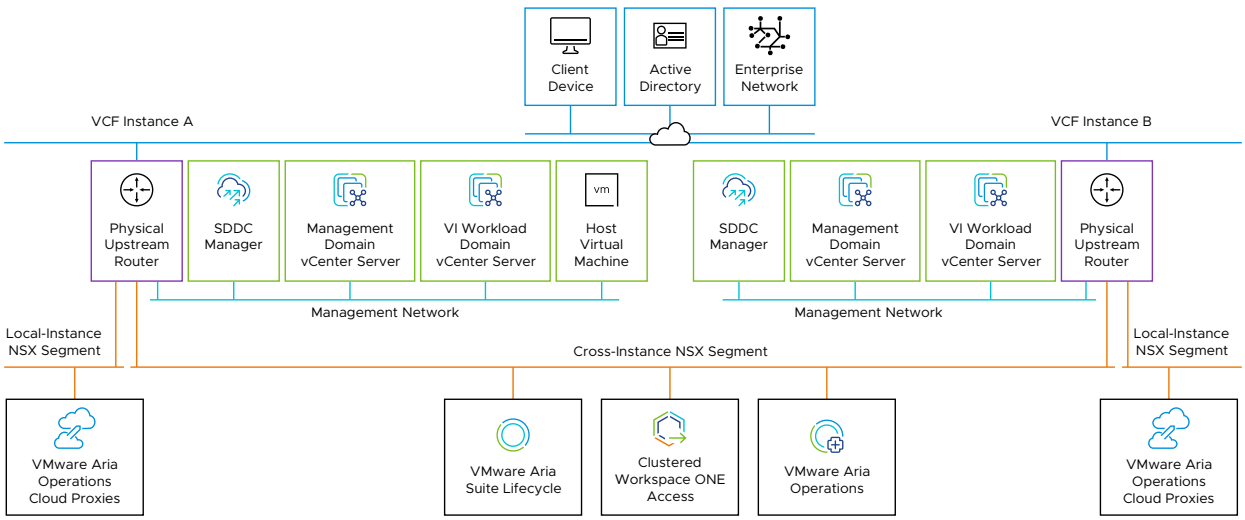


Table 2-9. Design Decisions on Network Segments for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-001	Place the host virtual machine on the management VLAN of the management domain.	Place the host virtual machine on the same network as SDDC Manager for direct communication.	None

IP Addressing

Allocate a statically assigned IP address and host name to the host virtual machine from the corresponding network.

Table 2-10. Design Decisions on IP Addresses for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-002	Allocate statically assigned IP address from the management VLAN to the host virtual machine.	Using statically assigned IP addresses ensures stability of the deployment and simplifies maintenance and tracking.	Requires precise IP address management.

Name Resolution

Name resolution provides the translation between an IP address and a fully qualified domain name (FQDN), which makes it easier to connect to components across the SDDC. The IP address of the host virtual machine must have a valid internal DNS forward (A) and reverse (PTR) records.

Table 2-11. Design Decisions on Name Resolution for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-003	Configure forward and reverse DNS records for the host virtual machine IP address.	Ensures the host virtual machine is accessible by using a fully qualified domain name instead of using IP address only.	■ You must provide a DNS record for the host virtual machine IP address. ■ Firewalls between the host virtual machine and the DNS servers must allow DNS traffic.
HRM-VM-NET-004	Configure DNS servers on the host virtual machine.	Ensures the host virtual machine has accurate name resolution.	■ DNS infrastructure services should be highly-available in the environment. ■ Firewalls between the appliance and the DNS servers must allow DNS traffic. ■ You must provide two or more DNS servers unless a DNS geographic load balancing is active.

Time Synchronization

Time synchronization provided by the Network Time Protocol (NTP) ensures that all components within the SDDC are synchronized to the same time source. This section of the design consists of characteristics and decisions that support the time configuration for the host vitual machine.

Table 2-12. Design Decisions on Time Synchronization for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-005	Configure NTP servers for the host virtual machine.	■ Ensures that the host virtual machine has accurate time synchronization. ■ Assists in the prevention of time mismatch between the host virtual machine and any dependencies.	■ NTP infrastructure services should be highly-available in the environment. ■ Firewalls between the host virtual machine and the NTP servers must allow NTP traffic. ■ You must provide two or more NTP servers unless an NTP geographic load balancing is active.

Life Cycle Management Design for Health Reporting and Monitoring for VMware Cloud Foundation

Life cycle management details the design decisions for the life cycle management of the host virtual machine and the installed software components.

Life cycle management of the host virtual machine, the PowerShell Module for VMware Cloud Foundation Reporting, and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations involves the process of applying updates manually.

Table 2-13. Design Decisions on Life Cycle Management

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-LCM-001	Manage the updates for the host virtual machine's guest operating system using your organization's tools and processes.	Update the host virtual machine in accordance with your organizations processes and policies to ensure security and critical fixes are applied in a timely manner.	The host virtual machine is not managed by SDDC Manager.
HRM-LCM-001	Manually update PowerShell Module for VMware Cloud Foundation Reporting when new versions are available.	Updating the PowerShell Module for VMware Cloud Foundation Reporting when new versions are released ensures the latest features and bug fixes are applied.	None
HRM-LCM-002	Manually update the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations. See the README.md in the GitHub repository.	Updating the Python module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations when new versions are released ensures the latest features and bug fixes are applied.	None

Information Security and Access Control Design for Health Reporting and Monitoring for VMware Cloud Foundation

Information security and access control design details the design decisions for both users and groups, for integration authentication, access controls, and for password management.

Identity Management Design for Health Reporting and Monitoring for VMware Cloud Foundation

You use accounts with least privilege access for authentication and authorization between the host virtual machine, SDDC Manager, and VMware Aria Operations.

You establish integration with the identity provider of your organization with vCenter Single Sign-On through the use of the the *Identity and Access Management for VMware Cloud Foundation* validated solution. With this integration, SDDC Manager uses your organization's directory services for authentication through vCenter Server Single Sign-On. You control authorization to SDDC Manager by assigning roles to users or service accounts from your identity provider.

You establish integration with the identity provider of your organization with clustered Workspace ONE Access through the use of the *Intelligent Operations Management for VMware Cloud Foundation* validated solution. With this integration you synchronise users from your organization's directory services with Workspace ONE Access and then manage access to VMware Aria Operations, by assigning roles to users or service accounts from your identity provider.

Table 2-14. Design Decisions on Identity Management for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-SEC-001	Limit the use of local accounts for interactive or API access and solution integration.	Local accounts are not specific to user identity and do not offer complete auditing from an endpoint back to the user identity.	You must define and manage service accounts, security groups, group membership, and security controls in Active Directory.
HRM-SEC-002	Limit the scope and privileges for accounts used for interactive or API access and solution integration.	The principle of least privilege is a critical aspect of access management and must be part of a comprehensive defense-in-depth security strategy.	You must define and manage custom roles and security controls to limit the scope and privileges used for interactive access or solution integration.
HRM-SEC-003	Assign an SDDC Manager role to a designated service account.	To provide least privilege access to SDDC Manager you assign the service account to a role.	None.
HRM-SEC-004	Assign a custom VMware Aria Operations role to a designated service account.	To provide least privilege access to VMware Aria Operations you assign the service account to a custom role.	You must maintain the custom role required for service account of your organization.

Service Accounts Design for Health Reporting and Monitoring for VMware Cloud Foundation

To enable connectivity between the components of the *Health Reporting and Monitoring forVMware Cloud Foundation* validation solution, you configure service accounts with least privilege access to SDDC Manager and VMware Aria Operations.

This solution ensures that the context of each integration and its associated service account use a least privilege and permissions scope.

The host virtual machine requires credentials that allows for least privilege access to SDDC Manager and VMware Aria Operations.

The PowerShell Module for VMware Cloud Foundation Reporting requires the following access to SDDC Manager:

- VMware Cloud Foundation API
- Appliance Console Access

The Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations requires access to:

- VMware Aria Operations REST API

Table 2-15. Design Decisions on Service Accounts for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PWSH-SEC-001	Assign the **ADMIN** role to an Active Directory user account in each SDDC Manager instance for application-to-application communication between the PowerShell Module for VMware Cloud Foundation Reporting and SDDC Manager.	To generate reports by using the PowerShell Module for VMware Cloud Foundation Reporting, the service account requires the **ADMIN** role for least privilege access.	You must maintain the life cycle and availability of the service account outside of the SDDC stack.
HRM-PY-SEC-001	Create a custom role in VMware Aria Operations and assign it to an Active Directory user account for application-to-application communication between the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.	A custom role with least privileges is required to provide access to the REST API to push custom metrics to VMware Aria Operations.	■ You must maintain the life cycle and availability of the service account outside of the SDDC stack. ■ You must maintain the synchronization and availability of the service account in Workspace ONE Access.

Table 2-15. Design Decisions on Service Accounts for Health Reporting and Monitoring for VMware Cloud Foundation (continued)

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PY-SEC-002	Import the service account to the **Everyone** user group in VMware Aria Operations.	The **Everyone** user group has no roles and scopes. You need to assign the scope and custom role to the service account.	No restrictions to limit access in VMware Aria Operations.
HRM-PY-SEC-003	Assign the scope of permissions to the custom role in VMware Aria Operations.	Provide the limited permission to required adapter instances.	■ Limits access to objects to a custom role in VMware Aria Operations. ■ This narrows the service account access to only NSX, vCenter, VMware Cloud Foundation, and vSAN adapter instance objects.

Password Management Design for Health Reporting and Monitoring for VMware Cloud Foundation

Password management design details the design decisions covering password policy configuration and password management.

Password Policies for Health Reporting and Monitoring

Configuring password policies includes the configuration of password expiration, complexity, and account lockout policies according to the requirements of your organization which can be based on industry or internal compliance standards.

Table 2-16. Design Decisions on Password Policies for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-SEC-001	Configure the local user password expiration policy for the host virtual machine.	You configure the local user password expiration policy for the host virtual machine to align with the requirements of your organization.	You must manage the local user password expiration settings on the host virtual machine.
HRM-VM-SEC-002	Configure the local user password complexity policy for the host virtual machine.	You configure the local user password complexity policy for the host virtual machine to align with the requirements of your organization.	You must manage the local user password complexity settings on the host virtual machine.
HRM-VM-SEC-003	Configure the local user account lockout policy for the host virtual machine.	You configure the local user account lockout policy for the host virtual machine to align with the requirements of your organization.	You must manage the local user account lockout settings on the host virtual machine.

Password Management for Health Reporting and Monitoring

Changing the passwords periodically or when certain events occur, increases the security posture and health of the system. To ensure continued access, you must manage the life cycle of the service account passwords for integration with SDDC Manager and VMware Aria Operations. After you reset the password, you must re-generate the encrypted passwords for the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations. See Encrypt the Service Accounts Passwords for the Python Module for the Integration with SDDC Manager and VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation.

Table 2-17. Design Decisions on Password Management for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-SEC-005	If the SDDC Manager service account is changed, update the user credentials in the **sddc_manager** section of the `env.json`.	You must manually re-establish authentication to SDDC Manager after the service account is changed (including a password change) to ensure that the Python Module for VMware Cloud Foundation Health Monitoring has the correct credentials and access.	You must update the user credentials manually.
HRM-SEC-006	If the VMware Aria Operations service account is changed, update the user credentials in the **vrops** section of the `env.json` file.	You must manually re-establish authentication to VMware Aria Operations after service account is changed (including a password change) to ensure that the Python Module for VMware Cloud Foundation Health Monitoring has the correct credentials and access.	You must update the user credentials manually.
HRM-SEC-007	Encrypt the passwords for SDDC Manager and VMware Aria Operations service accounts by running `encrypt-passwords.py` Python script.	Password encryption enhances the security of the communication between the applications.	You must manually run the Python script to encrypt the passwords.

Planning and Preparation for Health Reporting and Monitoring for VMware Cloud Foundation

3

Before you start implementing the components of the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution, you must ensure the environment has a specific compute, storage, and network configuration, and provides external services to the components of the solution.

Use the VMware Cloud Foundation Planning and Preparation Workbook to capture environment specific input values that are required during the implementation.

Carefully review the VMware Cloud Foundation Planning and Preparation Workbook before implementation to avoid costly rework and delays. Capture input values that are specific to your environment and verify that the components that are required by this solution are available.

The VMware Cloud Foundation Planning and Preparation Workbook contains inputs for each implementation and configuration procedure. Reference your values from the VMware Cloud Foundation Planning and Preparation Workbook to complete the UI or PowerShell procedures.

External Services

You use services that are external to VMware Cloud Foundation when implementing the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

External Service	Description
Active Directory (AD)	Active Directory (AD) is used to provide authentication and authorization to the VMware Cloud Foundation infrastructure. This includes dedicated Domain Users with least privilege access to act as service accounts for component connectivity.
Domain Name Services (DNS)	Domain Name Services is used to ensure components are resolvable by FQDN and by IP address.
Network Time Protocol (NTP)	Network Time Protocol is used to synchronize time consistently across components.

Implementation of Health Reporting and Monitoring for VMware Cloud Foundation

4

Implementing the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution includes the deployment and configuration of a host virtual machine in the management domain of your VMware Cloud Foundation instance. You then install and configure the PowerShell Module for VMware Cloud Foundation Reporting and Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

To implement and configure monitoring of the operational state of your VMware Cloud Foundation environment, alternative methods exist:

Table 4-3. Validated Solution Implementation Options

Method	Description
Implementation by using PowerShell automation	End-to-end automated implementation by using PowerShell. See Automated PowerShell Implementation of Health Reporting and Monitoring.
Implementation by using component user interfaces	End-to-end manual implementation by using components' user interfaces. See User Interface Implementation of Health Reporting and Monitoring.

For information on the health monitoring and reporting design, see Chapter 2 Detailed Design for Health Reporting and Monitoring for VMware Cloud Foundation.

Prerequisites

To complete the implementation of this validated solution, verify that your system fulfils the following prerequisites.

Table 4-1. Prerequisites for Implementation of Health Reporting and Monitoring for VMware Cloud Foundation

Category	Prerequisite
Environment	■ Verify that your VMware Cloud Foundation version is listed in the Support Matrix for this solution. ■ Verify that you configure your environment according to Before You Apply This Guidance. ■ Verify that you capture all parameters for the *Health Reporting and Monitoring* tab of the VMware Cloud Foundation Planning and Preparation Workbook. ■ Verify that your *VMware Cloud Foundation* instance is healthy and fully operational. See VMware Cloud Foundation Operations Guide.
Domain Name Service	■ Verify that the required DNS entries are created in the DNS server for the associated forward and reverse zones.
Active Directory	■ Verify that Active Directory Domain Controllers are available in the environment. ■ Verify that the required service accounts are created in Active Directory.

After you deploy and configure the host virtual machine, you install and configure the additional open-source software in the following order:

1 PowerShell Module for VMware Cloud Foundation Reporting.

2 Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

Table 4-2. Prerequisites for Installation of Open-Source Software of Health Reporting and Monitoring for VMware Cloud Foundation

Category	Prerequisite
Networking	■ Verify that the host virtual machine has network connectivity to the SDDC Manager of each VMware Cloud Instance. ■ Verify that the host virtual machine has network connectivity to VMware Aria Operations.
PowerShell Module for VMware Cloud Foundation Reporting	■ Verify that the host virtual machine is running a supported operating system. ■ Verify that the host virtual machine has a supported version of PowerShell installed. See the Powershell Module documentation in the GitHub repository.
Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations	■ Verify that the host virtual machine has Python 3.x installed. ■ Verify that the host virtual machine has the requried Python libraries installed. See the README.md in the GitHub repository.

For known issues, to report issues, obtain support, or suggest enhancements to the open-source PowerShell and Python modules, use:

- PowerShell Module for VMware Cloud Foundation Reporting GitHub Issues

- Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations GitHub Issues
- Automated PowerShell Implementation of Health Reporting and Monitoring

  Use the PowerShell Module for VMware Validated Solutions to implement the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.
- User Interface Implementation of Health Reporting and Monitoring

  Use the component user interfaces to implement the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

Automated PowerShell Implementation of Health Reporting and Monitoring

Use the PowerShell Module for VMware Validated Solutions to implement the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

PowerShell Module Installation

If you want to use the open source PowerShell Module for VMware Validated Solutions to automate the implementation of this validated solution, you must first prepare the management host.

Note For information on how to install this module, see PowerValidated Solutions.

To report issues, obtain support, or suggest enhancements to the open-source PowerShell Module, use GitHub Issues in the GitHub repository.

Connected Environment

1. Verify that your system has PowerShell 7.2 or later installed. See Microsoft PowerShell.
2. Start PowerShell.
3. Install the PowerShell Module for VMware Validated Solutions together with the supporting modules from the PowerShell Gallery.

   ```
   Install-Module -Name VMware.PowerCLI -MinimumVersion 13.3.0 -Scope AllUsers
   Install-Module -Name VMware.vSphere.SsoAdmin -MinimumVersion 1.3.9 -Scope AllUsers
   Install-Module -Name ImportExcel -MinimumVersion 7.8.9 -Scope AllUsers
   Install-Module -Name PowerVCF -MinimumVersion 2.4.0 -Scope AllUsers
   Install-Module -Name PowerValidatedSolutions -MinimumVersion 2.12.0 -Scope AllUsers
   ```
4. Import the PowerShell Module for VMware Validated Solutions.

   ```
   Import-Module -Name PowerValidatedSolutions
   ```
5. Verify that all PowerShell modules are installed correctly.

   ```
   Test-PowerValidatedSolutionsPrereq
   ```

6 Proceed with the implementation of the validated solution.

Disconnected Environment

1 Verify that your system has PowerShell 7.2 or later installed. See Microsoft PowerShell.

2 Start PowerShell.

3 Create a folder to store the saved PowerShell Modules.

a Replace the variables with your values and run the commands.

```
$drive = "F:\"
$saveModuleFolder = "modules\"
```

b Perform the configuration by running the command in the PowerShell console.

```
New-Item -Path $drive$saveModuleFolder -ItemType Directory
```

4 From a system with an Internet connection, save the module dependencies from the PowerShell Gallery.

```
Save-Module -Name VMware.PowerCLI -Path "$drive$saveModuleFolder" -Repository PSGallery
Save-Module -Name VMware.vSphere.SsoAdmin -Path "$drive$saveModuleFolder" -Repository
PSGallery
Save-Module -Name PowerVCF -Path "$drive$saveModuleFolder" -Repository PSGallery
Save-Module -Name PowerValidatedSolutions -Path "$drive$saveModuleFolder" -Repository
PSGallery
Save-Module -Name ImportExcel -Path "$drive$saveModuleFolder" -Repository PSGallery
```

5 From the system with the Internet connection, copy the module dependencies to a target system.

```
Copy-Item -Path "$drive$saveModuleFolder*" -Destination '\\<destination_host>\C$
\Program Files\WindowsPowerShell\Modules\' -Recurse
```

6 Import the PowerShell Module for VMware Validated Solutions.

```
Import-Module -Name PowerValidatedSolutions
```

7 Verify that all PowerShell modules are installed correctly.

```
Test-PowerValidatedSolutionsPrereq
```

8 Proceed with the implementation of the validated solution.

PowerShell Implementation

Automated configuration using PowerShell supports only preparing the VMware Cloud Foundation intance. The remaining configuration must be performed manually by using the component user interfaces:

- Configure the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation
- Configure VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

1 Start PowerShell.

2 Create a folder structure to store the validated solution PowerShell content.

a Replace the variables with your values and run the commands in the PowerShell console.

```
$drive = "F:\"
$parentFolder = "validatedSolutions\"
$cerificateFolder = "certificates\"
$binariesFolder = "binaries\"
$jsonFolder = "generatedJsons\"
```

b Perform the configuration by running the command in the PowerShell console.

```
New-Item -Path $drive$parentFolder, "$drive$parentFolder$cerificateFolder",
"$drive$parentFolder$jsonFolder", "$drive$parentFolder$binariesFolder" -ItemType
Directory
Set-Location -Path "$drive$parentFolder"
```

3 Start the VMware Validated Solution PowerShell menu.

a Move your completed VMware Cloud Foundation Planning and Preparation Workbook in the `validatedSolutions` root folder.

b Replace the variables with your values and run the command.

```
$pnpWorkbook = "instanceA-pnpWorkbook.xlsx"
```

c Start the VMware Validated Solution PowerShell menu.

```
Start-ValidatedSolutionMenu -jsonPath "$drive$parentFolder$jsonFolder"
-certificatePath "$drive$parentFolder$cerificateFolder"
-binaryPath "$drive$parentFolder$binariesFolder" -protectedWorkbook
"$drive$parentFolder$pnpWorkbook" -logPath "$drive$parentFolder"
```

4 From the main menu, enter **`11. (HRM) Health Reporting and Monitoring`**.

5 To generate the Health Reporting and Monitoring JSON specification file based on the VMware Cloud Foundation Planning and Preparation Workbook, enter **`01. Generate JSON Specification File`**.

6 To verify that your environment meets all prerequisites, enter **`02. Verify Prerequisites`**.

7 To perform the end-to-end deployment, enter **`05. End-to-End Deployment`**.

User Interface Implementation of Health Reporting and Monitoring

Use the component user interfaces to implement the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

Procedure

1 Prepare the VMware Cloud Foundation Instance for Health Reporting and Monitoring

   You deploy the host virtual machine and prepare the VMware Cloud Foundation instance before installing and configuring the PowerShell Module for VMware Cloud Foundation Reporting and Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

2 Configure the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation

   To enable health reporting and monitoring of your VMware Cloud Foundation instance, you install and configure the PowerShell Module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations on the host virtual machine.

3 Configure VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

   After you deploy and configure the host virtual machine with the PowerShell Module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations, you import and configure views, super metrics, dashboards, alerts, and notifications in VMware Aria Operations to enable health data ingestion and aggregation.

Prepare the VMware Cloud Foundation Instance for Health Reporting and Monitoring

You deploy the host virtual machine and prepare the VMware Cloud Foundation instance before installing and configuring the PowerShell Module for VMware Cloud Foundation Reporting and Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

Deploy the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation

You deploy the host virtual machine within the management vCenter Server instance and use it to execute the PowerShell Module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

The host virtual machine can use a Photon OS or Windows Server based operating system that adheres to your orgainzation's standards. For illustration purposes or use within non-production environment, this validated solution uses a sample Photon OS appliance, available for download at Photon OS sample appliance. You can also use the code from the GitHub project to build the appliance as an OVA.

The sample appliance comes with all necessary OS packages. If you deploy a Photon OS host virtual machine instead of using the sample appliance, you must install the following packages:

- *logrotate*
- *wget*
- *git*
- *unzip*
- *tar*
- *jq*
- *cronie*
- *powershell*
- *python3-pip*

To install these packages, run the following commands:

```
tdnf install -y \
  minimal \
  logrotate \
  wget \
  git \
  unzip \
  tar \
  jq \
  cronie \
  powershell \
  python3-pip
```

Procedure

1 Log in to the management domain vCenter Server at **`https://<management_vcenter_server_fqdn>/ui`** by using an account with **Administrator** privileges.

2 In the **Hosts and clusters** inventory, navigate to the default management data center and expand the data center.

3 Right-click the cluster, and select **Deploy OVF template**.

4 On the **Select an OVF template** page, select **Local file**, and click **Upload files**.

5 On the **Open** dialog page, navigate to the OVA file, click **Open**, and click **Next**.

6 On the **Select a name and folder** page, in the **Virtual machine name** text box, configure the settings according to your VMware Cloud Foundation Planning and Preparation Workbook, and click **Next**.

7 On the **Select a compute resource** page, select the compute resource, and click **Next**.

8 On the **Review details** page, review the settings, and click **Next**.

9 On the **Select storage** page, configure the settings according to your VMware Cloud Foundation Planning and Preparation Workbook, and click **Next**.

10 On the **Select networks** page, from the **Destination network** drop-down menu, select the management VLAN port group, and click **Next**.

11 On the **Customize template** page, configure the settings according to your VMware Cloud Foundation Planning and Preparation Workbook, and click **Next**.

12 On the **Ready to complete** page, click **Finish**, and wait for the completion of the process.

13 Power on the host virtual machine.

   a In the **Hosts and clusters** inventory, navigate to the default management data center and expand the data center.

   b Expand the cluster.

   c Right-click the host virtual machine and, from the **Actions** drop-down menu, select **Power > Power on**.

Create Virtual Machine and Template Folder for the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation

To improve ease of management of the host virtual machine, you create a virtual machine folder in the management vCenter Server instance.

Procedure

1 Log in to the management domain vCenter Server at **`https://<management_vcenter_server_fqdn>/ui`** by using an account with **Administrator** privileges.

2 In the **VMs and templates** inventory, navigate to the default management data center, right-click the data center, and select **New folder > New VM and template folder**.

3 In the **New folder** dialog box, enter a name for the folder according to the VMware Cloud Foundation Planning and Preparation Workbook, and click **OK**.

Move the Host Virtual Machine to the Dedicated Folder for Health Reporting and Monitoring for VMware Cloud Foundation

Move the host virtual machine to the dedicated virtual machine folder you previously created.

Procedure

1 Log in to the management domain vCenter Server at **`https://<management_vcenter_server_fqdn>/ui`** as **administrator@vsphere.local**.

2 In the **VMs and templates** inventory, expand the management domain vCenter Server tree and the management domain data center.

3 Right-click the host virtual machine and select **Move to folder**.

4 In the **Move to folder** dialog box, select the dedicated folder for the host virtual machine, and click **OK**.

Add the Host Virtual Machine to the First Availability Zone VM Group for Health Reporting and Monitoring for VMware Cloud Foundation

If the management domain is configured with two availability zones, to provide fail over to the second availability zone, move the host virtual machine to the VM group for the first availability zone. The virtual machine write operations are performed synchronously across both availability zones and each availability zone has a copy of the data.

Procedure

1 Log in to the management domain vCenter Server at **`https://<management_vcenter_server_fqdn>/ui`** as **administrator@vsphere.local**.

2 In the **Hosts and clusters** inventory, expand the management domain vCenter Server tree and expand the management domain data center.

3 Select the default management vSphere cluster and click the **Configure** tab.

4 In the left pane, select **Configuration > VM/Host groups**.

5 Select the VM group for the first availability zone according to your value in the VMware Cloud Foundation Planning and Preparation Workbook and click **Add VM/Host group members**.

6 In the **Add group member** dialog box, select the host virtual machine and click **OK**.

Assign SDDC Manager Role to a Service Account for the PowerShell Module for VMware Cloud Foundation Reporting

To provide the necessary privileges to the service account for the PowerShell Module for VMware Cloud Foundation Reporting, you assign the **ADMIN** role to a service account in SDDC Manager.

The cmdlets in this PowerShell module, and its dependencies, return data from SDDC management components. SDDC Manager provides the credentials for the platform components. For cmdlets that connect to SDDC Manager, you use the VMware Cloud Foundation API and a user or service account with the **ADMIN** role in SDDC Manager.

Procedure

1 Log in to SDDC Manager at **`https://<sddc_manager_fqdn>`** with a user assigned the **Admin** role.

2 For VMware Cloud Foundation 4.4.x, in the navigation pane, click **Administration user**.

3 For VMware Cloud Foundation 4.5 or later, in the navigation pane, click **Administration > Single sign on**.

4 On the **Manage users** page, click **Add user or group**.

5 On the **Add user or group** page, in the **Search user** text box, enter the name of the service account according to the value in your VMware Cloud Foundation Planning and Preparation Workbook.

6 In the **User / group name** column, select the check box for the service account.

7 In the **Role** column, from the **Choose role** drop-down menu, select the **ADMIN** role.

8 Click **Add**.

Synchronize the Active Directory Users for VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

You synchronize the Active Directory users for use by VMware Aria Operations in the clustered Workspace ONE Access.

Procedure

1 Log in to the clustered Workspace ONE Access deployment at **`https://<clustered_workspace_one_access_fqdn>/admin`** with a user assigned the **administrator** role.

2 On the main navigation bar, click **Identity and access management**.

3 Click the **Directories** tab and select your directory name according to the values in your VMware Cloud Foundation Planning and Preparation Workbook.

4 On the **Settings** tab, click **Sync settings**.

5 Click the **Users** tab.

6 Under **Specify the user DNs**, click **Add**.

7 In the text box, enter the base DN for Active Directory users according to the values in your VMware Cloud Foundation Planning and Preparation Workbook.

8 Click **Save and sync**.

9 Click **Sync directory**.

Define a Custom Role in VMware Aria Operations for the Python Module for VMware Cloud Foundation Health Monitoring

To provide the necessary permissions, you create a custom role for the Python module in VMware Aria Operations. These permissions provide least privilege access to VMware Aria Operations REST APIs. Also add the scope for a service account to allows the service account access to NSX, vCenter, VMware Cloud Foundation, and vSAN adapter instance objects.

Procedure

1 Log in to the VMware Aria Operations interface at **`https://<aria_operations_fqdn>`** with a user assigned the **Administrator** role.

2 In the left pane, navigate to **Administration > Control panel**.

3 Click **Access control** and click the **Roles** tab.

4 Click **Add**.

5 Configure the new custom role and assign access control scope.

a On the **Create Role** page in the **Role information** section, configure the settings according to the values in your VMware Cloud Foundation Planning and Preparation Workbook.

b In the **Assign permissions** section, configure the settings and click **Save**.

Category	Permissions
Administration.REST APIs	**All other read, write APIs**
	Read access to APIs

c On the **Access control** page, click the **Scopes** tab.

d To add the scope for a service account, click **Add**.

e On the **Create scope** page in the **Scope information** section, configure the settings according to the values in your VMware Cloud Foundation Planning and Preparation Workbook.

f In the **Select object** section, select the following objects.

Object Hierarchies	Object
Adapter instance	NSX
	vCenter
	VMware Cloud Foundation
	vSAN Adapter

g Click **Save**.

Assign VMware Aria Operations Custom Role to a Service Account for the Python Module for VMware Cloud Foundation Health Monitoring

Import and assign a role to the service account in VMware Aria Operations.

Procedure

1 Log in to the VMware Aria Operations interface at **`https://<aria_operations_fqdn>`** with a user assigned the **Administrator** role.

2 In the left pane, navigate to **Administration > Control panel**.

3 Click **Access control** and click the **User accounts** tab.

4 To import a service account, from the elliptical drop-down menu, select **Import from source**.

   a On the **Import users** page, configure the settings according to the values in your VMware Cloud Foundation Planning and Preparation Workbook and click **Next** then click **Finish**.

5 Assign the custom role to the service account.

   a On the **User accounts** page, select the service account and from the vertical ellipsis drop-down menu, select **Edit**.

   b In **Assign roles and scope** section, configure the settings according to the values in your VMware Cloud Foundation Planning and Preparation Workbook and click **Save**.

Configure the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation

To enable health reporting and monitoring of your VMware Cloud Foundation instance, you install and configure the PowerShell Module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations on the host virtual machine.

Install the PowerShell Module for VMware Cloud Foundation Reporting

You install the PowerShell Module for VMware Cloud Foundation Reporting together with supporting PowerShell modules from the PowerShell gallery on the host virtual machine.

Procedure

1 Log in to the host virtual machine.

   Photon OS

   Log in to the host virtual machine at **`<host_virtual_machine_fqdn>:22`** as the **admin** user by using a Secure Shell (SSH) client.

   Windows Server

   Log in to the host virtual machine at **`<host_virtual_machine_fqdn>`** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.

2 Start PowerShell.

3 Install the PowerShell module and its dependencies from the PowerShell Gallery by running the commands in the console.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Install-Module -Name VMware.PowerCLI -MinimumVersion 13.2.1
Install-Module -Name VMware.vSphere.SsoAdmin -MinimumVersion 1.3.9
Install-Module -Name PowerVCF -MinimumVersion 2.4.1
Install-Module -Name PowerValidatedSolutions -MinimumVersion 2.11.0
Install-Module -Name VMware.CloudFoundation.Reporting -MinimumVersion 2.6.3
```

4 Import the modules by running the commands in the console.

```
Set-PowerCLIConfiguration -Scope AllUsers -ParticipateInCEIP $false -Confirm:$false
Import-Module -Name VMware.PowerCLI
Import-Module -Name VMware.vSphere.SsoAdmin
Import-Module -Name PowerVCF
Import-Module -Name PowerValidatedSolutions
Import-Module -Name VMware.CloudFoundation.Reporting
```

5 Verify the modules are installed correctly by running the command in the console.

```
Test-VcfReportingPrereq
```

Install and Configure the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

Upload the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations to the host virtual machine and configure the necessary settings to enable health data collection and the integration with VMware Aria Operations.

Procedure

Photon OS

1 Log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

2 Install the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

```
pip install vmware-cloud-foundation-health-monitoring --target=/opt/vmware/hrm-
<sddc_manager_vm_name>
```

3 Provide execute permissions to the files in the `hrm` directory.

```
chmod -R 755 /opt/vmware/hrm-<sddc_manager_vm_name>
```

4 Switch to the `hrm-`**<sddc_manager_vm_name>**`/main` directory.

```
cd /opt/vmware/hrm-<sddc_manager_vm_name>/main
```

5 Edit the `env.json` file and configure the values according to your VMware Cloud Foundation Planning and Preparation Workbook.

```
vi env.json
```

6 Encrypt the service account passwords.

```
python encrypt-passwords.py
```

7 Enter the password for the VMware Aria Operations service account.

8 Enter the password for the SDDC Manager service account.

9 Enter the password for the SDDC Manager appliance local user.

10 Repeat this procedure for each VMware Cloud Foundation instance.

Windows Server

1 Log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client and open a PowerShell console.

2 Start Windows Command Prompt.

3 Install the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

```
pip install vmware-cloud-foundation-health-monitoring --target=C:\vmware\hrm-
<sddc_manager_vm_name>\
```

4 Change to the `hrm-<sddc_manager_vm_name>\main` folder.

```
cd c:\vmware\hrm-<sddc_manager_vm_name>\main
```

5 Edit the `env.json` file and configure the values according to your VMware Cloud Foundation Planning and Preparation Workbook.

```
notepad env.json
```

6 Encrypt the service account passwords.

```
python encrypt-passwords.py
```

7 Enter the password for the VMware Aria Operations service account.

8 Enter the password for the SDDC Manager service account.

9 Enter the password for the SDDC Manager appliance local user.

10 Repeat this procedure for each VMware Cloud Foundation instance.

Install the VMware Aria Operations Nagini Client for Health Reporting and Monitoring for VMware Cloud Foundation

The VMware Aria Operations Nagini client is a Python wrapper for Rest API calls to VMware Aria Operations. You install the VMware Aria Operations Nagini client on the host virtual machine to enable the integration between the Python Module for VMware Cloud Foundation Health Monitoring and VMware Aria Operations.

Procedure

Photon OS

1. Log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.
2. Download the Python language bindings package for VMware Aria Operations.

   ```
   wget https://<aria_operations_fqdn>/suite-api/docs/bindings/python/vcops-python.zip --output-document=/opt/vmware/vcops-python.zip
   ```

   Note If your host virtual machine does not trust the Certificate Authority chain, run the above command with `--no-check-certificate` option.
3. Unzip the Python language bindings package zip file.

   ```
   unzip /opt/vmware/vcops-python.zip -d /opt/vmware/vrops-python
   rm /opt/vmware/vcops-python.zip
   ```
4. Navigate to the Python language bindings package directory you previously created.

   ```
   cd /opt/vmware/vrops-python
   ```
5. Install the Python language bindings package.

   ```
   python setup.py install
   ```

Windows Server

1. Log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.
2. Start PowerShell.
3. Download the Python language bindings package for VMware Aria Operations.

   ```
   Invoke-WebRequest -Uri https://<aria_operations_fqdn>/suite-api/docs/bindings/python/vcops-python.zip -OutFile C:\vmware\vcops-python.zip
   ```

   Note If your host virtual machine does not trust the Certificate Authority chain, run the above command with `-skipCertificateCheck` option.

4 Unzip the Python language bindings package zip file.

```
                Expand-Archive C:\vmware\vcops-python.zip -DestinationPath
C:\vmware\vrops-python
Remove-Item -Path c:\vmware\vcops-python.zip
```

5 Navigate to the Python language bindings package directory you previously created.

```
cd C:\vmware\vrops-python
```

6 Install the Python language bindings package.

```
python setup.py install
```

Manually Run the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

Manually run the script to verify that health data from the SDDC management components is received and successfully sent to VMware Aria Operations.

Procedure

Photon OS

1 Log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

2 Run the `send-data-to-vrops.py` script for each VMware Cloud Foundation instance.

```
python /opt/vmware/hrm-<sddc_manager_vm_name>/main/send-data-to-vrops.py
```

Note On a large environment (250 ESXi hosts, 10000 virtual machines) the script may take up to one and a half hours to complete.

While script is running the health check tasks will appear in SDDC Manager, this is normal and expected.

When the script completes, it generates `.json` report files and logs in the *DEFAULT_LOGS_DIR_PATH* directory, set in your `env.json` file.

3 Verify that health data and metrics are sent to VMware Aria Operations.

a Log in to the VMware Aria Operations interface at **https://<aria_operations_fqdn>** with a user assigned the **Administrator** role.

b In the left pane, navigate to **Inventory**.

c On the **Inventory** page, click **Detailed view**.

d Click the **Integrations** tab and, from the drop-down menu, select **All objects**.

e In the inventory pane, navigate to **vCenter > Virtual machine**

f In the **Object browser** pane, navigate to **All objects > vCenter > Virtual machine** and select the Management Domain vCenter Server appliance.

g Click the **Metrics** tab.

h Expand the **Metrics** section and verify that there are 5 metrics whith names beginning with **HRM** and 11 metrics with names beginning with **SOS**.

4 Repeat this procedure for each VMware Cloud Foundation instance.

Windows Servver

1 Log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client and open a PowerShell console.

2 Run the `send-data-to-vrops.py` script for each VMware Cloud Foundation instance.

```
python C:\vmware\hrm-<sddc_manager_vm_name>\main\send-data-to-vrops.py
```

Note On a large environment (250 ESXi hosts, 10000 virtual machines) the script may take up to one and a half hours to complete.

While script is running the health check tasks will appear in SDDC Manager, this is normal and expected.

When the script completes, it generates `.json` report files and logs in the *DEFAULT_LOGS_DIR_PATH* directory, set in your `env.json` file.

3 Verify that health data and metrics are sent to VMware Aria Operations.

a Log in to the VMware Aria Operations interface at **https://<aria_operations_fqdn>** with a user assigned the **Administrator** role.

b In the left pane, navigate to **Environment > Object browser**.

c In the **Object browser** pane, navigate to **All objects > vCenter > Virtual machine** and select the Management Domain vCenter Server appliance.

d Click the **Metrics** tab.

e Expand the **Metrics** section and verify that there are 5 metrics whith names beginning with **HRM** and 10 metrics with names beginning with **SOS**.

4 Repeat this procedure for each VMware Cloud Foundation instance.

Schedule the Python Module for VMware Cloud Foundation Health Reporting in VMware Aria Operations to Run Daily

Automate sending health data to VMware Aria Operations by scheduling the Python module to run daily.

Procedure

Photon OS

1. Log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.
2. Edit the cron tab.

   ```
   crontab -e
   ```

3. Add the following to the file.

   ```
   59 23 * * * /opt/vmware/env/bin/python /opt/vmware/hrm-<sddc_manager_vm_name>/main/
   send-data-to-vrops.py > /dev/null 2>&1
   ```

4. Verify the cron job configuration by running the following command:

   ```
   crontab -l
   ```

5. Repeat this procedure for each VMware Cloud Foundation instance.

Windows Servver

1. Log in to the host virtual machine at **<host_virtual_machine_fqdn>** as **Administrator** by using Remote Desktop Connection (RDC) client.
2. Click **Start**, enter `task` and select **Task scheduler**.
3. In the **Task scheduler** window, from the **Action** drop-down menu, select **Create basic task**.
4. On the **Create a basic task** page, configure the values according to your VMware Cloud Foundation Planning and Preparation Workbook and click **Next**.
5. On the **Task trigger** page, select **Daily** and click **Next**.
6. On the **Daily** page, configure the start time and recurrence according to your VMware Cloud Foundation Planning and Preparation Workbook and click **Next**.
7. On the **Action** page, select **Start a program** and click **Next**.
8. On the **Start a program** page, click **Browse**, navigate to the `c:\vmware\hrm-<sddc_manager_vm_name>\examples\run_send-data-to-vrops.bat` file in the Python module directory, click **Open** and click **Next**.
9. On the **Summary** page, click **Finish**.
10. Repeat this procedure for each VMware Cloud Foundation instance.

Configure VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

After you deploy and configure the host virtual machine with the PowerShell Module for VMware Cloud Foundation Reporting and the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations, you import and configure views, super metrics, dashboards, alerts, and notifications in VMware Aria Operations to enable health data ingestion and aggregation.

Import and Configure Artifacts in VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

To import dashboards, views and super metrics, you perform this procedure in VMware Aria Operations with a user assigned the **Administrator** role.

Note Even if you have multiple VMware Cloud Foundation instances, you need to import the artifacts only once.

You must enable super metrics in the default policy of VMware Aria Operations.

The artifacts reside in the target directory you selected when you installed the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations by using PiP.

Guest Operating System	Artifact Path
Photon OS	`/opt/vmware/hrm-<sddc_manager_vm_name>/artifacts/vSAN`
Windows Server	`C:\vmware\hrm-<sddc_manager_vm_name>\artifacts\vSAN`

Procedure

1. Log in to the VMware Aria Operations interface at **`https://<aria_operations_fqdn>`** with a user assigned the **Administrator** role.
2. Import the pre-defined views.
   a. In the left pane, navigate to **Operations > Views**.
   b. In the **Views** pane, click **Manage**.
   c. From the ellipsis drop-down menu, select **Import**.
   d. In the **Import view** dialog box, click **Browse**, navigate to the `Views.zip` file, click **Open**, click **Import**, and click **Done**.
3. Import the pre-defined super metrics.
   a. In the left pane, navigate to **Operations > Configurations**.
   b. On the **Configuration** page, click **Super metrics**
   c. From the ellipsis drop-down menu, select **Import**.

d In the **Import super metric** dialog box, click **Browse**, navigate to the `Supermetrics.json` file, click **Open**, click **Import**, and click **Done**.

4 Configure the default policy to enable the super metrics.

a In the left pane, navigate to **Operations > Configurations**.

b On the **Configuration** page, click **Policy definitions**.

c On the **Policy definition** page, select the **Default policy** and, from the ellipsis drop-down menu, select **Edit**.

d On the **Default policy** page, click the **Metrics and properties** card.

e From the **Select object type** drop-down menu, select **vCenter > Cluster compute resource**.

f Expand **Super metrics** and select all super metrics beginning with *SM*.

g From the **Actions** drop-down menu, select **State > Activate**.

h On the **Metrics and properties** page, click **Save**.

i Repeat this step to activate the following:

Object Type	Component
vCenter	Cluster computer resource
	Datacenter
	vCenter Server
NSX	NSX
VMware Cloud Foundation	VCF Domain

5 Import the pre-defined dashboards.

a In the left pane, navigate to **Operations > Dashboards**.

b In the **Dashboards** pane, click **Manage**.

c From the ellipsis drop-down menu, select **Import**.

d In the **Import dashboard** dialog box, click **Browse**, navigate to the `Dashboards.zip` file, click **Open**, click **Import**, and click **Done**.

Note After successfully importing and configuring the artifacts, the tables show data immediately. Heat maps on dashboards may take from 12 up to 24 hours to display colors.

Import and Configure Alerts in VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

To enable alerts in VMware Aria Operations, you import the `Alert_Definitions.xml` file provided with the Python Module for VMware Cloud Foundation Health Monitoring in VMware

Aria Operations and enable the alerts. The alerts comprise of an alert definition, one or more symptom definition, and recommendations.

Note Even if you have multiple VMware Cloud Foundation instances, you need to import the `Alert_Definitions.xml` file only once.

Procedure

1 Log in to the VMware Aria Operations interface at **`https://<aria_operations_fqdn>`** with a user assigned the **Administrator** role.

2 Import the pre-defined alerts.

   a In the left pane, navigate to **Operations > Configurations**.

   b On the **Configurations** page, click **Alert definitions**.

   c On the **Alert definitions** page, from the ellipsis drop-down menu, select **Import**.

   d In the **Import alert definition** dialog box, click **Browse**, navigate to the `Alert_Definitions.xml` file, click **Open**, click **Import**, and click **Done**.

3 Configure the default policy to enable the alerts.

   a In the left pane, navigate to **Operations > Configurations**.

   b On the **Configurations** page, click **Policy definition**.

   c On the **Policy definition**page, select the **Default policy** and, from the ellipsis drop-down menu, select **Edit**.

   d On the **Default policy** page, click the **Alerts and symptoms** card.

   e On the **Alerts and symptoms** page, click the **Alert definition** tab.

   f In the **Filter** text box, enter **`SoS`** and click the **Select all** icon.

   g From the **Actions** drop-down menu, select **State > Activated**.

   h On the **Alerts and symptoms** page, click **Save**.

   i Repeat this step to activate the remaining alert definitions by entering **`HRM`** in the **Filter** text box.

Import and Configure Notifications in VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

To send notifications through VMware Aria Operations, you edit the predefined alert notification rules provided with the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations according to your environment and import the `Notifications.json` file in VMware Aria Operations. This solution uses the standard email plug-in as the notification outbound method.

Note Even if you have multiple VMware Cloud Foundation instances, you need to import the `Notifications.json` file only once.

Procedure

1 Log in to the host virtual machine.

   a For Photon OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

   b For Windows Server OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client and open Command Prompt.

2 Generate the `notifications.json` file.

   a Navigate to the `main` directory of the Python Module for VMware Cloud Foundation Health Reporting.

Guest Operating System	Command
Photon OS	`cd /opt/vmware/hrm-<sddc_manager_vm_name>/main/`
Windows Server	`cd C:\vmware\hrm-<sddc_manager_vm_name>\main\`

   b Generate the `notifications.json` file by running the command.

```
python notifications.py
```

   c Select the plug-in type.

   d Enter the plug-in name set in VMware Aria Operations.

   e Depending on the plug-in type, enter the email(s) for the recepient(s) or the webhook for the Slack plug-in.

3 Log in to the VMware Aria Operations interface at **https://<aria_operations_fqdn>** with a user assigned the **Administrator** role.

4 Import the pre-defined notifications.

   a In the VMware Aria Operations operations interface, navigate to **Operations** > **Configurations**.

   b On the **Configurations** page, click **Notifications**.

   c On the **Notifications** page, from the ellipsis drop-down menu, select **Import**.

   d In the **Import notification settings** dialog box, click **Browse**, navigate to the generated `Notifications.json` file, click **Open**, click **Import**, and click **Done**.

Operational Guidance for Health Reporting and Monitoring for VMware Cloud Foundation

5

After you complete the implementation and configuration of the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution, you perform common operations on the environment, such as examining the operational state of the components added to the environment during the implementation and updating service account passwords for these components.

For operational guidance on the components that are deployed automatically in VMware Cloud Foundation or complement the basic VMware Cloud Foundation configuration, see the VMware Cloud Foundation Operations Guide and the VMware Cloud Foundation Administration Guide.

Read the following topics next:

- Personas in Health Reporting and Monitoring for VMware Cloud Foundation
- Operational Verification of Health Reporting and Monitoring for VMware Cloud Foundation
- Password Management for Health Reporting and Monitoring for VMware Cloud Foundation
- Monitoring and Alerting for Health Reporting and Monitoring for VMware Cloud Foundation
- Shutdown and Startup of Health Reporting and Monitoring for VMware Cloud Foundation

Personas in Health Reporting and Monitoring for VMware Cloud Foundation

Personas describe types of system users, aligned with real people and their functions within the organization. You build a persona set based on your organization's requirements for role-based access control.

The following is an example of personas defined by the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution and their equivalent access. It builds upon the Personas in Intelligent Operations Management for VMware Cloud Foundation validated solution. You use this as a baseline for defining and building a set of personas to delegate roles and define access based on roles and responsibilities within your organization's structure.

Table 5-1. Example Personas for VMware Aria Operations

Persona	Responsibility	Solution Component	Roles
Site Resiliency Engineer (SRE)	Privileges to generate HTML reports.	SDDC Manager	ADMIN
	Privileges to perform the actions of the Administrator role except for privileges to user management and cluster management.	VMware Aria Operations	PowerUser

Operational Verification of Health Reporting and Monitoring for VMware Cloud Foundation

After you complete the implementation and configuration of the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution, verify that the components are operational and functioning within expected parameters.

Verify Network Connectivity and Integration between the Host Virtual Machine, SDDC Manager, and VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

Verify that the host virtual machine can communicate and authenticate to the REST APIs for SDDC Manager and VMware Aria Operations.

Expected Outcome
You can successfully authenticate and make API calls to SDDC Manager and VMware Aria Operations from the host virtual machine.

Procedure

1 Log in to the host virtual machine.

   a For Photon OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

   b For Windows Server, log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.

2 Start PowerShell.

3 Verify that host virtual machine can communicate with SDDC Manager.

```
Test-VCFConnection -server <sddc_manager_fqdn>
```

4 Verify you can authenticate to SDDC Manager through the REST API.

```
Test-VCFAuthentication -server <sddc_manager_fqdn> -user <sddc_manager_user> -pass
<sddc_manager_password>
```

5 Verify that the host virtual machine can communicate with VMware Aria Operations.

```
Test-vROPSConnection -server <aria_operations_fqdn>
```

6 Verify that you can authenticate to VMware Aria Operations through the REST API.

```
Test-vROPSAuthentication -server <aria_operations_fqdn> -user <vaops_user>
-pass <vaops_password>
```

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips.

Troubleshooting Tips
■ Ensure that there is network connectivity between the host virtual machine, SDDC Manager, and VMware Aria Operations. ■ Ensure that the credentials used to connect to SDDC Manager and VMware Aria Operations have the correct permissions.

Verify Health Report Generation with the PowerShell Module for VMware Cloud Foundation Reporting

Verify that all PowerShell dependencies for the PowerShell Module for VMware Cloud Foundation Reporting are installed on the host virtual machine and that you can generate an HTML report with the service account with the **ADMIN** role in SDDC Manager.

Expected Outcome
You can successfully generate an HTML report on the host virtual machine using service account with the **ADMIN** role in SDDC Manager.

Procedure

1 Log in to the host virtual machine.

   a For Photon OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

   b For Windows Server, log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.

2 Start PowerShell.

3 Verify that the PowerShell dependencies for the PowerShell module for VMware Cloud Foundation Reporting are installed.

```
Test-VcfReportingPrereq
```

4 Verify successful generation of an HTML report by generating a System Overview report for a VMware Cloud Foundation instance using the SDDC Manager service account.

a For Photon OS, replace the values in the code with your values and run the commands.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "svc-hrm-vcf@sfo.rainpole.io"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$reportPath = "/opt/vmware/reporting"
```

b For Windows Server, replace the values in the code with your values and run the commands.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "svc-hrm-vcf@sfo.rainpole.io"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$reportPath = "F:\Reporting"
```

c Generate the report.

```
Invoke-VcfOverviewReport -sddcManagerFqdn $sddcManagerFqdn -sddcManagerUser
$sddcManagerUser -sddcManagerPass $sddcManagerPass -reportPath $reportPath
```

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips.

Troubleshooting Tips
■ Ensure that there is network connectivity between the host virtual machine and the SDDC Manager. ■ Ensure that all required PowerShell modules for the PowerShell Module for VMware Cloud Foundation Reporting are installed on the host virtual machine. ■ Ensure that the correct credentials are used when running PowerShell command.

Verify the Authentication to VMware Aria Operations by Using the Service Account for Health Reporting and Monitoring for VMware Cloud Foundation

Verify that you can authenticate to VMware Aria Operations with the service account by using VMware Aria Operations REST API.

Expected Outcome
You can successfully authenticate to VMware Aria Operations with the service account using VMware Aria Operations REST API.

Procedure

1 In a Web browser, navigate to **`https://<aria_operations_manager_fqdn>/suite-api/doc/swagger-ui.html`**.

2 Click **Authorize**.

3 In the **Available authorizations** dialog box, enter the service account with permission to access VMware Aria Operations REST API, and the password.

Note The username must be in the format *user@domain@authsource*, where *authsource* must match the `Source display name` of your vIDM source in VMware Aria Operations. The sample username for this validated solution is **svc-hrm-vrops@sfo.rainpole.io@vIDMAuthSource**.

4 On the **Available authorizations**, click **Authorize**.

5 In the **Available authorization** dialog box, verify that the service account is successfully authorized.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips.

Troubleshooting Tips
Ensure that you are using the correct credentials to connect to VMware Aria Operations REST API and that the service account has the necessary permissions.

Password Management for Health Reporting and Monitoring for VMware Cloud Foundation

Manage the passwords of the components deployed according to the design objectives and design guidance of the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

Password management activities include the configuration of password policies, such as password expiration, password complexity or account lockout, and password rotation and remediation.

Changing the passwords periodically or when certain events occur, increases the security posture and health of the system. To ensure continued access, you must manage the life cycle of the service accounts passwords for SDDC Manager and VMware Aria Operations.

Change the Service Accounts for the Python Module for the Integration between the Host Virtual Machine, SDDC Manager, and VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

To change the service accounts for SDDC Manager and VMware Aria Operations, you must reconfigure the `env.json` file of the Python Module for VMware Cloud FoundationHealth Monitoring in VMware Aria Operations.

Procedure

Photon OS

1. Log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.
2. Edit the `env.json` configuration file.

   ```
   vi /opt/vmware/hrm-<sddc_manager_vm_name>/env.json
   ```

3. Update the users for SDDC Manager and VMware Aria Operations.

   Note The user for VMware Aria Operations must be in the format *user@domain@authsource*, where *authsource* must match the `Source display name` of your vIDM source in VMware Aria Operations. The sample user name for this validated solution is **svc-hrm-vrops@sfo.rainpole.io@vIDMAuthSource**.

   ```
   "vrops":{
           "fqdn":"xint-vrops01.rainpole.io",
           "user":"svc-hrm-vrops@sfo.rainpole.io@vIDMAuthSource"
       },
   "sddc_manager":{
           "fqdn":"sfo-vcf01.sfo.rainpole.io",
           "user":"svc-hrm-vcf@sfo.rainpole.io"
       }
   ```

4. Save the file.

   Repeat this procedure for each VMware Cloud Foundation instance.

Windows Servver

1. Log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client and open a PowerShell console.
2. Edit the `env.json`, located in `C:\vmware\hrm-`**<sddc_manager_vm_name>** folder.

   ```
   notepad env.json
   ```

3 Update the users for SDDC Manager and VMware Aria Operations.

Note The user for VMware Aria Operations must be in the format *user@domain@authsource*, where *authsource* must match the `Source display name` of your vIDM source in VMware Aria Operations. The sample user name for this validated solution is **svc-hrm-vrops@sfo.rainpole.io@vIDMAuthSource**.

```
"vrops":{
        "fqdn":"xint-vrops01.rainpole.io",
        "user":"svc-hrm-vrops@sfo.rainpole.io@vIDMAuthSource"
    },
"sddc_manager":{
        "fqdn":"sfo-vcf01.sfo.rainpole.io",
        "user":"svc-hrm-vcf@sfo.rainpole.io"
    }
```

4 Save the file.

5 Repeat this procedure for each VMware Cloud Foundation instance.

Encrypt the Service Accounts Passwords for the Python Module for the Integration with SDDC Manager and VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation

When you change or reset the service account passwords, you must regenerate the encrypted passwords for the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.

Procedure

Photon OS

1 Log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

2 Navigate to `hrm-`**<sddc_manager_vm_name>**`/main/` folder and encrypt the service accounts passwords.

```
cd /opt/vmware/hrm-<sddc_manager_vm_name>/main/
python encrypt-passwords.py
```

3 Enter the password for the VMware Aria Operations service account.

4 Enter the password for the SDDC Manager service account.

5 Enter the password for the SDDC Manager appliance **local** user.

6 Repeat this procedure for each VMware Cloud Foundation instance.

Windows Servver

1 Log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client and open a PowerShell console.

2 Navigate to the `hrm-<sddc_manager_vm_name>\main\` folder and encrypt the service account passwords.

```
cd C:\vmware\hrm-<sddc_manager_vm_name>\main\
python encrypt-passwords.py
```

3 Enter the password for the VMware Aria Operations service account.

4 Enter the password for the SDDC Manager service account.

5 Enter the password for the SDDC Manager appliance **local** user.

6 Repeat this procedure for each VMware Cloud Foundation instance.

Monitoring and Alerting for Health Reporting and Monitoring for VMware Cloud Foundation

Continuously monitor the health of your VMware Cloud Foundation environment by generating health and system alert reports on a recurring schedule. Utilize the pre-defined dashboards in the VMware Cloud Foundation health dashboard group in VMware Aria Operations to extend the parameters you monitor and proactively manage the health of your environment.

The PowerShell Module for VMware Cloud Foundation Reporting provides the ability to generate pre-defined HTML reports for VMware Cloud Foundation. Key reports for reviewing the health of your VMware Cloud Foundation instance include:

- Health Report
- System Alert Report
- Upgrade Precheck Report

Ensure that you generate these reports on a regular basis, review the results, and perform remediation for any issues as part of your operational practices. To display issues only in each report, you can use the optional `-failureOnly` switch with each cmdlet .

Use the daily updated, pre-defined dashboards in the VMware Cloud Foundation Health dashboard group in VMware Aria Operations to continuously monitor the health of your environment. Use the custom alerts and notifications to improve monitoring of focus areas of the SDDC.

Generate a Health Report for Health Reporting and Monitoring for VMware Cloud Foundation

You use the `Invoke-VcfHealthReport` cmdlet in the PowerShell Module for VMware Cloud Foundation Reporting to generate a display only issues health report, that combines information from the VMware Cloud Foundation SoS utility and additional health checks performed against SDDC management components.

Procedure

1 Log in to the host virtual machine.

   a For Photon OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

   b For Windows Server, log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.

2 Start PowerShell.

3 Replace the values in the sample code with your values and run the commands in the PowerShell console.

   a For Photon OS.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "admin@local"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$sddcManagerLocalUser = "vcf"
$sddcManagerLocalPass = "VMw@re1!"

$reportPath = "/opt/vmware/reporting"
```

   b For Windows Server.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "admin@local"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$sddcManagerLocalUser = "vcf"
$sddcManagerLocalPass = "VMw@re1!"

$reportPath = "F:\Reporting"
```

4 Generate the health report with display issues.

```
Invoke-VcfHealthReport -sddcManagerFqdn $sddcManagerFqdn -sddcManagerUser $sddcManagerUser
-sddcManagerPass $sddcManagerPass -sddcManagerLocalUser $sddcManagerLocalUser
-sddcManagerLocalPass $sddcManagerLocalPass -reportPath $reportPath -allDomains
-failureOnly
```

Note To generate a health report for a workload domain with displays issues only, you replace the `-allDomains` flag with the `-workloadDomain` parameter and the `$workloadDomain` variable.

5 Review the HTML report and perform remediation of any identified issues.

Generate a System Alert Report for Health Reporting and Monitoring for VMware Cloud Foundation

You use the `Invoke-VcfSystemAlertReport` cmdlet in the PowerShell module for VMware Cloud Foundation Reporting to generate a display only issues system alert report that collects information about the currently active system alerts in your VMware Cloud Foundation environment.

Procedure

1 Log in to the host virtual machine.

a For Photon OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

b For Windows Server, log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.

2 Start PowerShell.

3 Replace the values in the sample code with your values and run the commands in the PowerShell console.

a For Photon OS.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "admin@local"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$reportPath = "/opt/vmware/reporting"
```

b For Windows Server.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "admin@local"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$reportPath = "F:\Reporting"
```

4 Generate the system alert report with display issues.

```
Invoke-VcfAlertReport -sddcManagerFqdn $sddcManagerFqdn -sddcManagerUser $sddcManagerUser
-sddcManagerPass $sddcManagerPass -reportPath $reportPath -allDomains
```

Note To generate a system alert report for a workload domain with displays issues only, you replace the `-allDomains` flag with the `-workloadDomain` parameter and the `$workloadDomain` variable.

5 Review the HTML report and perform remediation of any identified issues.

Generate an Upgrade Precheck Report for a Workload Domain for Health Reporting and Monitoring for VMware Cloud Foundation

You use the `Invoke-VcfUpgradePrecheck` cmdlet in the PowerShell Module for VMware Cloud Foundation Reporting to generate an upgrade precheck report for a Workload domain.

Procedure

1 Log in to the host virtual machine.

a For Photon OS, log in to the host virtual machine at **<host_virtual_machine_fqdn>:22** as the **admin** user by using a Secure Shell (SSH) client.

b For Windows Server, log in to the host virtual machine at **<host_virtual_machine_fqdn>** as the **Administrator** user by using a Remote Desktop Connection (RDC) client.

2 Start PowerShell.

3 Replace the values in the sample code with your values and run the commands in the PowerShell console.

a For Photon OS.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "admin@local"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$workloadDomain = "sfo-w01"

$reportPath = "F:\Reporting"
```

b For Windows Server.

```
$sddcManagerFqdn = "sfo-vcf01.sfo.rainpole.io"
$sddcManagerUser = "admin@local"
$sddcManagerPass = "VMw@re1!VMw@re1!"

$workloadDomain = "sfo-w01"

$reportPath = "/opt/vmware/reporting"
```

4 Generate the upgrade precheck report for a Workload domain.

```
Invoke-VcfUpgradePrecheck -sddcManagerFqdn $sddcManagerFqdn -sddcManagerUser
$sddcManagerUser -sddcManagerPass $sddcManagerPass -reportPath $reportPath -workloadDomain
$workloadDomain
```

5 Review the HTML report.

Continuous Health Monitoring of VMware Cloud Foundation with VMware Aria Operations

You use the predefined dashboards in VMware Aria Operations to continuously and proactively monitor your VMware Cloud Foundation environment. The included custom alerts and notifications enable you to review and mitigate the noted issues to minimize upgrade preparation and remediate any problems with your environment.

Procedure

1 Log in to the VMware Aria Operations interface at **`https://<aria_operations_fqdn>`** with a user assigned the **Administrator** role.

2 In the left pane, select **Visualize > Dashboards**.

3 In **Dashboards** panel, select **All > VCF Health**.

4 Observe health of the VMware Cloud Foundation environment by reviewing health statuses of each monitored SDDC components. If status is not green, review the reason and remediate the issue.

Note For a list of available VMware Cloud Foundation health dashboards, see Logical Design for Health Reporting and Monitoring for VMware Cloud Foundation.

Shutdown and Startup of Health Reporting and Monitoring for VMware Cloud Foundation

In certain cases, for example, during hardware or power maintenance of the data center, you must shut down the host virtual machine in a VMware Cloud Foundation system in a way that prevents data loss and appliance malfunction, and start it up, restoring component integration after the maintenance operation is over.

Shut Down the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation

To gracefully power off the host virtual machine, use the vCenter Server user interface.

You can shut down the host virtual machine independently. If you shut down the entire management domain follow the full-stack shutdown order of VMware Cloud Foundation, see Shutdown and Startup of VMware Cloud Foundation.

Procedure

1 Log in to the management domain vCenter Server at **`https://<management_vcenter_server_fqdn>/ui`** by using an account with **Administrator** privileges.

2 In the **VMs and templates** inventory, expand the management domain vCenter Server tree and expand the management domain data center.

3 Navigate to the host virtual machine in the inventory.

4 Right-click the virtual machine and select **Power > Shutdown Guest OS**.

5 In the confirmation dialog box, click **Yes**.

Start the Host Virtual Machine for Health Reporting and Monitoring for VMware Cloud Foundation

To start the host virtual machine, use the vCenter Server user interface.

You can start the host virtual machine independently. If you start up the entire management domain follow the full-stack startup order of VMware Cloud Foundation, see Shutdown and Startup of VMware Cloud Foundation.

Procedure

1 Log in to the management domain vCenter Server at **`https://<management_vcenter_server_fqdn>/ui`** by using an account with **Administrator** privileges.

2 In the **VMs and templates** inventory, expand the management domain vCenter Server tree and expand the management domain data center.

3 Navigate to the host virtual machine in the inventory.

4 Right-click the virtual machine and click **Power > Power on**.

5 Verify the operational state of the host virtual machine after the startup. See Verify Network Connectivity and Integration between the Host Virtual Machine, SDDC Manager, and VMware Aria Operations for Health Reporting and Monitoring for VMware Cloud Foundation.

Appendix: Design Decisions for Health Reporting and Monitoring for VMware Cloud Foundation

6

The design decisions determine the deployment configuration to support the *Health Reporting and Monitoring for VMware Cloud Foundation* validated solution.

Deployment Specification

Table 6-1. Design Decisions for Deployment of a Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-CFG-001	Deploy the host virtual machine using a supported guest operating systems (VMware Photon OS or Microsoft Windows Server).	A dedicated host virtual machine is deployed to ensure isolation of the PowerShell and Python modules from other production components.	The host virtual machine must be deployed, configured, and maintained outside of VMware Cloud Foundation automated workflows.
HRM-VM-CFG-002	Deploy the host virtual machine in the default management vSphere cluster.	Required to communicate with SDDC Manager and VMware Aria Operations.	The host virtual machine must be able to connect to SDDC Manager and VMware Aria Operations.
HRM-VM-CFG-003	Protect the host virtual machine by using vSphere High Availability.	Supports the availability objective without requiring manual intervention during an ESXi host failure.	None.
HRM-VM-CFG-004	Place the host virtual machine in a designated virtual machine folder.	Provides organization of the appliances in the management domain vSphere inventory.	You must create the virtual machine folder during deployment.

Table 6-2. Design Decisions for Deployment of the Host Virtual Machine in Multiple Availability Zones

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-CFG-005	When using two availability zones, add the host virtual machine to the VM group of the first availability zone.	Ensures that the host virtual machine runs in the primary availability zone hosts group.	After the implementation of the second availability zone for the management domain, you must update the VM group for the primary availability zone virtual machines to include the host virtual machine.

Table 6-3. Design Decisions for Deployment of the Host Virtual Machine for Multiple VMware Cloud Foundation Instances

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-CFG-006	In an environment with multiple VMware Cloud Foundation instances, deploy the host virtual machine in the management vSphere cluster in the first VMware Cloud Foundation instance.	Required to communicate with SDDC Manager in each VMware Cloud Foundation instance and VMware Aria Operations.	The host virtual machine must be able to connect to SDDC Manager in each VMware Cloud Foundation instance and VMware Aria Operations.

PowerShell Module for VMware Cloud Foundation Reporting Design

Table 6-4. Design Decisions for the PowerShell Module for VMware Cloud Foundation Reporting

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PWSH-CFG-001	Use or install a supported edition and version of PowerShell on the host virtual machine guest operating system.	The PowerShell module cmdlets may fail when run on an edition and version of PowerShell that is not supported by the PowerShell module and its dependencies.	None
HRM-PWSH-CFG-002	Install the PowerShell Module for VMware Cloud Foundation Reporting and its dependencies on the host virtual machine.	The PowerShell Module for VMware Cloud Foundation Reporting is required to generate HTML reports.	None

Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

Table 6-5. Design Decisions for the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PY-CFG-001	Install Python 3.x on the host virtual machine.	Python 3 is required to run the Python script that pulls data from SDDC Manager and pushes it to VMware Aria Operations.	In an environment with multiple VMware Cloud Foundation instances, multiple copies of the Python module are installed, each corresponding to a VMware Cloud Foundation instance.
HRM-PY-CFG-002	Install the Nagini client, a Python binding package for VMware Aria Operations, on the host virtual machine.	The Nagini client enables the Python module to send data to VMware Aria Operations.	Manual installation and setup depends on the host virtual machine's operating system.
HRM-PY-CFG-003	On the host virtual machine, schedule daily runs of the Python module to collect health data from SDDC Manager and send it to VMware Aria Operations.	Automates gathering health data.	Manual installation and setup depends on the host virtual machine's operating system.
HRM-PY-CFG-004	Configure the default log retention for logs, generated by the Python module, to 30 days.	Automatic cleanup of logs generated when the `send-data-to-vrops.py` script saves capacity on the host virtual machine's local disk and ensures old data is removed.	You must manually set the log retention period by configuring the *log_retention_in_days* setting in the `env.json` file.

Network Design

Table 6-6. Design Decisions on Network Segments for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-001	Place the host virtual machine on the management VLAN of the management domain.	Place the host virtual machine on the same network as SDDC Manager for direct communication.	None

Table 6-7. Design Decisions on IP Addresses for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-002	Allocate statically assigned IP address from the management VLAN to the host virtual machine.	Using statically assigned IP addresses ensures stability of the deployment and simplifies maintenance and tracking.	Requires precise IP address management.

Table 6-8. Design Decisions on Name Resolution for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-003	Configure forward and reverse DNS records for the host virtual machine IP address.	Ensures the host virtual machine is accessible by using a fully qualified domain name instead of using IP address only.	■ You must provide a DNS record for the host virtual machine IP address. ■ Firewalls between the host virtual machine and the DNS servers must allow DNS traffic.
HRM-VM-NET-004	Configure DNS servers on the host virtual machine.	Ensures the host virtual machine has accurate name resolution.	■ DNS infrastructure services should be highly-available in the environment. ■ Firewalls between the appliance and the DNS servers must allow DNS traffic. ■ You must provide two or more DNS servers unless a DNS geographic load balancing is active.

Table 6-9. Design Decisions on Time Synchronization for the Host Virtual Machine

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-NET-005	Configure NTP servers for the host virtual machine.	■ Ensures that the host virtual machine has accurate time synchronization. ■ Assists in the prevention of time mismatch between the host virtual machine and any dependencies.	■ NTP infrastructure services should be highly-available in the environment. ■ Firewalls between the host virtual machine and the NTP servers must allow NTP traffic. ■ You must provide two or more NTP servers unless an NTP geographic load balancing is active.

Life Cycle Management

Table 6-10. Design Decisions on Life Cycle Management

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-LCM-001	Manage the updates for the host virtual machine's guest operating system using your organization's tools and processes.	Update the host virtual machine in accordance with your organizations processes and policies to ensure security and critical fixes are applied in a timely manner.	The host virtual machine is not managed by SDDC Manager.
HRM-LCM-001	Manually update PowerShell Module for VMware Cloud Foundation Reporting when new versions are available.	Updating the PowerShell Module for VMware Cloud Foundation Reporting when new versions are released ensures the latest features and bug fixes are applied.	None
HRM-LCM-002	Manually update the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations. See the README.md in the GitHub repository.	Updating the Python module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations when new versions are released ensures the latest features and bug fixes are applied.	None

Information Security and Access Control Design

Table 6-11. Design Decisions on Identity Management for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-SEC-001	Limit the use of local accounts for interactive or API access and solution integration.	Local accounts are not specific to user identity and do not offer complete auditing from an endpoint back to the user identity.	You must define and manage service accounts, security groups, group membership, and security controls in Active Directory.
HRM-SEC-002	Limit the scope and privileges for accounts used for interactive or API access and solution integration.	The principle of least privilege is a critical aspect of access management and must be part of a comprehensive defense-in-depth security strategy.	You must define and manage custom roles and security controls to limit the scope and privileges used for interactive access or solution integration.

Table 6-11. Design Decisions on Identity Management for Health Reporting and Monitoring for VMware Cloud Foundation (continued)

Decision ID	Design Decision	Design Justification	Design Implication
HRM-SEC-003	Assign an SDDC Manager role to a designated service account.	To provide least privilege access to SDDC Manager you assign the service account to a role.	None.
HRM-SEC-004	Assign a custom VMware Aria Operations role to a designated service account.	To provide least privilege access to VMware Aria Operations you assign the service account to a custom role.	You must maintain the custom role required for service account of your organization.

Table 6-12. Design Decisions on Service Accounts for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PWSH-SEC-001	Assign the **ADMIN** role to an Active Directory user account in each SDDC Manager instance for application-to-application communication between the PowerShell Module for VMware Cloud Foundation Reporting and SDDC Manager.	To generate reports by using the PowerShell Module for VMware Cloud Foundation Reporting, the service account requires the **ADMIN** role for least privilege access.	You must maintain the life cycle and availability of the service account outside of the SDDC stack.
HRM-PY-SEC-001	Create a custom role in VMware Aria Operations and assign it to an Active Directory user account for application-to-application communication between the Python Module for VMware Cloud Foundation Health Monitoring in VMware Aria Operations.	A custom role with least privileges is required to provide access to the REST API to push custom metrics to VMware Aria Operations.	■ You must maintain the life cycle and availability of the service account outside of the SDDC stack. ■ You must maintain the synchronization and availability of the service account in Workspace ONE Access.

Table 6-12. Design Decisions on Service Accounts for Health Reporting and Monitoring for VMware Cloud Foundation (continued)

Decision ID	Design Decision	Design Justification	Design Implication
HRM-PY-SEC-002	Import the service account to the **Everyone** user group in VMware Aria Operations.	The **Everyone** user group has no roles and scopes. You need to assign the scope and custom role to the service account.	No restrictions to limit access in VMware Aria Operations.
HRM-PY-SEC-003	Assign the scope of permissions to the custom role in VMware Aria Operations.	Provide the limited permission to required adapter instances.	■ Limits access to objects to a custom role in VMware Aria Operations. ■ This narrows the service account access to only NSX, vCenter, VMware Cloud Foundation, and vSAN adapter instance objects.

Table 6-13. Design Decisions on Password Policies for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-VM-SEC-001	Configure the local user password expiration policy for the host virtual machine.	You configure the local user password expiration policy for the host virtual machine to align with the requirements of your organization.	You must manage the local user password expiration settings on the host virtual machine.
HRM-VM-SEC-002	Configure the local user password complexity policy for the host virtual machine.	You configure the local user password complexity policy for the host virtual machine to align with the requirements of your organization.	You must manage the local user password complexity settings on the host virtual machine.
HRM-VM-SEC-003	Configure the local user account lockout policy for the host virtual machine.	You configure the local user account lockout policy for the host virtual machine to align with the requirements of your organization.	You must manage the local user account lockout settings on the host virtual machine.

Table 6-14. Design Decisions on Password Management for Health Reporting and Monitoring for VMware Cloud Foundation

Decision ID	Design Decision	Design Justification	Design Implication
HRM-SEC-005	If the SDDC Manager service account is changed, update the user credentials in the **sddc_manager** section of the `env.json`.	You must manually re-establish authentication to SDDC Manager after the service account is changed (including a password change) to ensure that the Python Module for VMware Cloud Foundation Health Monitoring has the correct credentials and access.	You must update the user credentials manually.
HRM-SEC-006	If the VMware Aria Operations service account is changed, update the user credentials in the **vrops** section of the `env.json` file.	You must manually re-establish authentication to VMware Aria Operations after service account is changed (including a password change) to ensure that the Python Module for VMware Cloud Foundation Health Monitoring has the correct credentials and access.	You must update the user credentials manually.
HRM-SEC-007	Encrypt the passwords for SDDC Manager and VMware Aria Operations service accounts by running `encrypt-passwords.py` Python script.	Password encryption enhances the security of the communication between the applications.	You must manually run the Python script to encrypt the passwords.