

VMware Skyline Health Diagnostics Installation, Configuration and Operations Guide

VMware Skyline Health Diagnostics

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

<https://docs.vmware.com/>

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

Copyright © 2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About VMware Skyline Health Diagnostics	5
1 Installing VMware Skyline Health Diagnostics	6
Installation Requirements	6
Overview of Installing VMware Skyline Health Diagnostics	7
Preparing the Software Images	8
Download VMware Skyline Health Diagnostics OVA Image	8
Downloading VMware Skyline Health Diagnostics ISO Image for Offline Updates	8
Deploying the OVA Image	9
Deploying VMware Skyline Health Diagnostics Using OVA Image.	9
Optional Post Deployment Configuration	10
Uninstalling the Software	12
2 Configuring VMware Skyline Health Diagnostics	13
Participating in the Customer Experience Improvement Program	13
Manage Customer Experience Improvement Program Status	13
Managing User Accounts	14
Add an Operator Account	14
Change User Details or Reset Password	16
Configuring Password Rotation and Account Lockout Policies	20
Proxy Settings	22
Additional configuration for Proxies acting as MITM (Man-In-The-Middle)	22
Managing Software Updates	23
View Download and Update History	23
Check and Download Software Updates	24
Check and Download Compatibility Guide Updates	25
Managing the Behavior and Performance	26
Updating the Property Value	27
Managing SSL Certificates	28
Custom Certificate Requirements	28
Generate Certificate Signing Request	29
Replace the Default Certificate with the Custom Certificate	30
Reverting to Self-Signed Certificate	31
Managing the Services	31
3 Using VMware Skyline Health Diagnostics	33
Operations in VMware Skyline Health Diagnostics	33
Log in to VMware Skyline Health Diagnostics from Web Browsers	34

Connect and Analyze Log Bundles for vCenter and ESXi	35
Connect and Analyze Log Bundles from the Disconnected ESXi Host	38
Health Checks for VMware Cloud Foundation (Technical Preview Mode)	40
Health Checks for VMware vSAN Storage	43
Upload and Analyze Log Bundles	46
View Analysis Reports	48
Deleting Single Analysis Report	49
Saving or Deleting Multiple Analysis Reports	49
Configuring Auto Delete for Analysis Reports from User Interface	50
Configuring Auto Delete for Analysis Reports using Config File	51
Interpreting the Diagnostics Report	52
Interpreting VCG/vSAN HCL Validation Summary.	56
Interpreting VMware Cloud Foundation Diagnostics Report	58
Interpreting VMware vSAN Storage Report	61
Adding and Removing Tags for the Analysis Report	62
Help and Support	63
View the CEIP Data Collected for Reporting and Analytics	64
4 Updating VMware Skyline Health Diagnostics	66
Update or Upgrade VMware Skyline Health Diagnostics Using Online Mode	66
Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful	67
Update or Upgrade the VMware Skyline Health Diagnostics Offline.	68
Revert to Last Working Set-Up If Update or Upgrade Operation Fails.	70
5 Scale Limits for VMware Skyline Health Diagnostics	72
Scale Limits	72
6 Interaction of Skyline Health Diagnostics with Services	74
Inbound Interaction	74
Outbound Interaction	74

About VMware Skyline Health Diagnostics

VMware Skyline Health Diagnostics is a self-service tool to detect issues using log bundles and suggest the Knowledge Base articles or Steps for remediating the issue in the vSphere, vSAN and VMware Cloud Foundation SDDC Manager product line. It can work in offline mode or disconnected environment. vSphere Administrators can use this tool for troubleshooting issues before contacting the VMware Support. The Installation and Setup guide provides information about installing and configuring VMware Skyline Health Diagnostics.

Intended Audience

System administrators who want to install and configure VMware Skyline Health Diagnostics. This information is written for experienced system administrators who are familiar with VMware vSphere virtual machine management and data center operations.

Installing VMware Skyline Health Diagnostics

1

Instruction to install and setup of VMware Skyline Health Diagnostics (Abbreviated as VMware SHD)

This chapter includes the following topics:

- [Installation Requirements](#)
- [Overview of Installing VMware Skyline Health Diagnostics](#)
- [Preparing the Software Images](#)
- [Deploying the OVA Image](#)
- [Uninstalling the Software](#)

Installation Requirements

Your environment must fulfill certain requirements so that you can install VMware Skyline Health Diagnostics

Software Requirement

- VMware vCenter Server 6.5 or Above (for OVA Deployment)

Hardware Requirements

Default settings for VMware Skyline Health Diagnostics Appliance virtual machine

- 4 vCPUs
- 16 GB RAM
- 250 GB space for the hard disk
- A port group with network connectivity for accessing this virtual machine from your workstation

Network Requirements

VMware Skyline Health Diagnostics requires network connectivity to the vSphere Infrastructure for which you need to run the diagnostics.

Make sure following requirements are met

- VMware Skyline Health Diagnostics Appliance is deployed in an IPV4 network and has a valid IP address (Static or DHCP)
- VMware Skyline Health Diagnostics Appliance is able to connect to vCenter Server and all the ESXi hosts managed by the vCenter Server (Default Port 443) for which the analysis is to be run
- If you have a requirement to analyze disconnected ESXi hosts make sure VMware Skyline Health Diagnostics Appliance is able to connect to ESXi over SSH (Port 22)
- If you have a requirement to analyze VMware Cloud Foundation SDDC Manager (Default Port 443)

Overview of Installing VMware Skyline Health Diagnostics

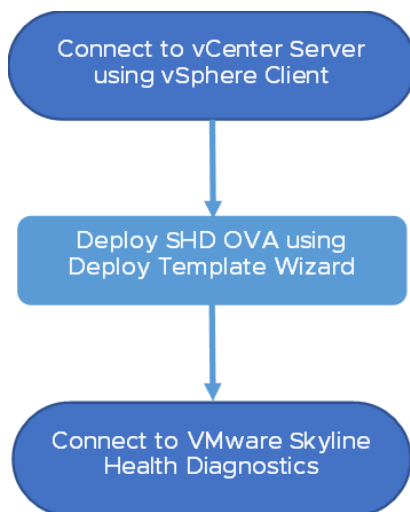
Installing VMware Skyline Health Diagnostics involves deploying the VMware SHD (VMware Skyline Health Diagnostics) Appliance using an OVA image. During the deployment you need to provide host-name, Network Configuration and Passwords for root (Photon OS User) and shd-admin (SHD administrator).

Before installing VMware Skyline Health Diagnostics, you must download the VMware SHD Appliance Image from VMware Downloads.

Appliance Image (OVA) is named with pattern: VMware-Skyline-HealthDiagnostics-Appliance-2.5.1-18319575_OVF10.ova where **2.5.1** and 18319575 are the current available version and build of VMware Skyline Health Diagnostics.

VMware Skyline Health Diagnostics can be deployed in a single step through vSphere Client connected to vCenter Server. This appliance is pre-configured with required software and settings to run VMware Skyline Health Diagnostics.

Figure 1-1. Installation Steps for VMware Skyline Health Diagnostics.



Preparing the Software Images

This section describes the software preparation required for installing VMware Skyline Health Diagnostics.

Download VMware Skyline Health Diagnostics OVA Image

You can download the VMware Skyline Health Diagnostics OVA image from the VMware product download website.

Prerequisites

Verify that your workstation has an HTML5 compatible browser and can connect to the Internet.

Verify that you have credentials to log in to [VMware Customer Connect Portal](#), and you can access [Skyline Health Diagnostics for vSphere product page](#).

Procedure

- 1 Connect to https://my.vmware.com/group/vmware/get-download?downloadGroup=SKYLINE_HD_VSPHERE using your browser
- 2 Click the Download Now to download the OVA Image file for VMware Skyline Health Diagnostics (VMware-Skyline-HealthDiagnostics-Appliance-[VERSION]-[BUILD]_OVF10.ova).
- 3 Read the End User License Agreement in the popup window, click the check box next to **I agree to the terms and conditions outlined in the End User License Agreement**, click **Accept** to start the file download.

Results

The OVA Image File for VMware Skyline Health Diagnostics is downloaded (VMware-Skyline-HealthDiagnostics-Appliance-[VERSION]-[BUILD]_OVF10.ova)

Downloading VMware Skyline Health Diagnostics ISO Image for Offline Updates

You can download the VMware Skyline Health Diagnostics ISO image from the VMware product download website. This ISO image can be used for updating existing VMware SHD Appliance or VMware SHD Installations.

Prerequisites

Verify that your workstation has an HTML5 compatible browser and can connect to the Internet.

Verify that you have credentials to log in to [VMware Customer Connect Portal](#), and you can access [Skyline Health Diagnostics for vSphere product page](#).

Procedure

- 1 Connect to https://my.vmware.com/group/vmware/get-download?downloadGroup=SKYLINE_HD_VSPHERE using your browser
- 2 Click the Download Now to download the ISO Image file for VMware Skyline Health Diagnostics (vmware-shd-[VERSION]-[BUILD].iso).
- 3 Read the End User License Agreement in the popup window, click the check box next to **I agree to the terms and conditions outlined in the End User License Agreement**, click **Accept** to start the file download.

Results

The ISO Image File for VMware Skyline Health Diagnostics is downloaded (vmware-shd-[VERSION]-[BUILD].iso)

Deploying the OVA Image

Deploy the VMware Skyline Health Diagnostics OVA Image into a vCenter (6.5 or above) managed ESXi Server

OVA deployment is simplified and just one step process . You can connect to vCenter Server and deploy the downloaded OVA Image. Post successful deployment the VMware Skyline Health Diagnostics Appliance is ready for use.

Deploying VMware Skyline Health Diagnostics Using OVA Image.

You can deploy VMware Skyline Health Diagnostics using a pre-configured OVA image.

Deploying OVA

Prerequisites

- Verify that you have the OVA Image for VMware Skyline Health Diagnostics is downloaded.
- Verify that you can access vSphere Infrastructure with privileges required for creating and interacting with virtual machine.
- Verify that you have network configuration details for the virtual appliance being deployed.

Procedure

- 1 Using the vSphere Client connected to vCenter Server, right-click the host/Data Center you want to deploy the VMware Skyline Health Diagnostics Virtual Appliance
- 2 Click **Deploy OVF Template** to start the deployment wizard
- 3 Click on **UPLOAD FILES** option and select the OVA Image file of VMware Skyline Health Diagnostics and click **NEXT**
- 4 Enter an appropriate Name for the Virtual Appliance

- 5 Optionally select the destination folder for the VM and click NEXT
- 6 Follow the Wizard to select Compute Resource and click NEXT
- 7 Verify the OVA template details and click NEXT
- 8 Accept the VMWARE END USER LICENSE AGREEMENT and click NEXT
- 9 Select the destination storage and optionally format and storage policy and click NEXT
- 10 Select the Port group to which you want the appliance to connect and click NEXT
- 11 In the "Customize Template" page enter the details

Note on Password

The password must contain at least 8 characters, have characters from at least 2 classes from Group 1 (lowercase alphabet, uppercase alphabet and numbers) and at least 1 character from the class group 2 (Special Characters)

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1slSV@lid
- ThisIsVali\$Too
- ThisisnotVal1d

- a Enter a strong password for *root* user account (OS User)
- b Enter a strong password for *shd-admin* user account

Same password rules as applicable for root user account applies here

- c Enter a suitable host-name for the appliance
- d Enter IPV4 Network Configuration Details (Leave blank if you are planning to use DHCP for assigning IP Address)
- e Click NEXT

- 12 Review the details and click Finish
- 13 After the deployment is complete, Power on the virtual machine
- 14 Wait for at least 5 minutes for the OS to boot and finish the initial configuration

Results

VMware Skyline Health Diagnostics Appliance is deployed and configured

Optional Post Deployment Configuration

User sees VMware **Skyline Health Diagnostics for vSphere - First Boot Password Manager** page and initial configuration gets suspended.

The VMware Skyline Health Diagnostics Appliance expects you enter valid strong passwords for both **root** and **shd-admin** user account. In case the passwords are not considered to be strong, initial configuration is suspended till user completes the initial configuration by entering a strong password through the UI. You can configure password for the VMware Skyline Health Diagnostics Appliance as described in this section. This section applies only in case initial configuration is suspended due to weak password.

Prerequisites

Verify that your workstation has an HTML5 compatible browser.

Procedure

- 1 Connect to VMware Skyline Health Diagnostics Appliance via your browser (https://HOSTNAME_OR_IPADDRESS_OF_VMware_SHD). If you don't see a page with titled "VMware Skyline Health Diagnostics for vSphere - First Boot Password Manager", you don't need to perform any further configuration and your appliance is ready for use.

- 2 Enter the details as requested

Note on Password

The password must contain at least 8 characters, have characters from at least 2 classes from Group 1 (lowercase alphabet, uppercase alphabet and numbers) and at least 1 character from the class group 2 (Special Characters)

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1sISV@lid
- ThisIsVali\$Too
- ThisisnotVal1d

- a You need to provide the passwords entered at deploy time and new password

- 3 Click SUBMIT to complete the configuration
- 4 Once the configuration is completed; Appliance will be set to reboot after 1 minute

Results

Initial password configuration for the appliance is complete

What to do next

- After appliance is rebooted post password configuration is complete, open a browser on your Workstation and go to https://IP_OR_HOSTNAME_OF_VMware_SHD to access the UI services. The log in page is displayed.
- You can log in using the credentials for **shd-admin** account.

- Further user accounts can be created using User Management Section under Settings in the UI

Uninstalling the Software

This section describes the steps to uninstall the VMware Skyline Health Diagnostics.

Prerequisites

- Verify that you have root credentials for the virtual machine where VMware Skyline Health Diagnostics is installed.
- Verify that you can access the virtual machine console.
- Verify that all users are logged out from VMware Skyline Health Diagnostics and no active tasks are running in Skyline Health Diagnostics.

Procedure

- 1 SSH to the VM/Appliance running VMware Skyline Health Diagnostics using root user.
- 2 Run command `shd-config uninstall`
- 3 Optionally you can shut down the VM and Delete it from the disk

Results

All the VMware Skyline Health Diagnostics related services are stopped. VMware Skyline Health Diagnostics software is uninstalled.

Configuring VMware Skyline Health Diagnostics

2

Instructions to perform administrative tasks on VMware Skyline Health Diagnostics .

This chapter includes the following topics:

- [Participating in the Customer Experience Improvement Program](#)
- [Managing User Accounts](#)
- [Proxy Settings](#)
- [Managing Software Updates](#)
- [Managing the Behavior and Performance](#)
- [Managing SSL Certificates](#)
- [Managing the Services](#)

Participating in the Customer Experience Improvement Program

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

This product participates in VMware Customer Experience Improvement Program (CEIP). For more information about CEIP and the purposes for which it is used by VMware, go to the Trust and Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

Manage Customer Experience Improvement Program Status

It is optional to join the Customer Experience Improvement Program (CEIP) . You can join or leave the program at any time.

Procedure

- 1 Open the New browser window and enter the IP address of the Appliance/VM where the VMware Skyline Health Diagnostics is deployed. For example, `https://IP_OR_HOSTNAME_OF_VMware_SHD`
- 2 Log in to VMware Skyline Health Diagnostics by entering the username and password.

- 3 Click the **Settings** tab in the top-menu.
- 4 Click the **Customer Experience Improvement Program** option in the left pane.
- 5 In the CEIP Status section, select or change your CEIP preference.
 - a To leave the CEIP click **Leave Program**.
 - a To join the CEIP, click **Join Program**.
- 6 Click **Sample Data** to view the kind of data that is collected under the CEIP program.

Results

Managing User Accounts

You can add new users using the HTML5 user interface or from the console using commands.

To access the analytic and diagnostics services through the UI interface a user must have a valid account with VMware Skyline Health Diagnostics.

VMware Skyline Health Diagnostics has one built-in admin account called **shd-admin** and is the only account permitted to perform user administration tasks.

Add an Operator Account

The *Add an Operator Account* provides information about adding new user to **VMware Skyline Health Diagnostics**. An Admin may want to delegate the task of troubleshooting the log bundle to other admins with less privilege.

User Interface to Add Operator Account

An operator account can be added using,

- HTML5 user interface
- Appliance/VM console

Add an Operator Account using HTML5 User Interface

You can create an operator account using **VMware Skyline Health Diagnostics** HTML5 user interface.

Prerequisites

- Verify that you can open the HTML5 URL for VMware Skyline Health Diagnostics in browser window.
- Verify that you have password for **shd-admin** user.

Procedure

- 1 Log in to VMware Skyline Health Diagnostics HTML5 user interface

- 2 Click **Setting** tab from the top-menu.
- 3 Click **User Management** option from the left side menu.
- 4 Click **+** to add new user.
- 5 On the **Create User** dialog box , provide following details.
- 6 **Name** : First and last name of the user.
- 7 **Email Id** : Email address of the user.
- 8 **User name** : User id to be given to the user, this will be used at user id at the time of log in.
- 9 **Password** : The password user will use at the time of log in

The password must contain at least 8 characters, have characters from 2 classes of Group 1 and 1 from Group 2.

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1sISV@lid
- ThisIsVali\$Too
- ThisisnotVal1d

- 10 **Confirm Password** : to confirm the password entered in the step above.
- 11 Click **Submit** , the user creation will start in background.

Results

A new operator account is created.

Add an Operator Account using VM Console

You can create an operator account using commands on the Appliance/VM console that has **VMware Skyline Health Diagnostics** running .

Prerequisites

- Verify that you have **root** user credentials for the **Appliance/VM** where **VMware Skyline Health Diagnostics** is running
- Verify that you have password for **shd-admin** user.
- For more information about enabling the root user log in on Photon OS, see: https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html(This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1** Open Appliance/VM Console from the vCenter Server user interface or SSH to Appliance/VM.
- 2** Log in as a **root** user.
- 3** To invoke the user Manager, run the command `shd-user`.
- 4** Enter the password for the user **shd-admin**.

You must set **shd-admin** password now if you did not set it during the install process.

- 5** To add a user, select the option **2. Add new user account**.
- 6** To set a username and password for this new account.

The password must contain at least 8 characters, have characters from 2 classes of Group 1 and 1 from Group 2.

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1sISV@lid
- ThisIsVali\$Too
- ThisisnotVal1d

Results

A new operator account is created.

Change User Details or Reset Password

The *Change or Reset User Details* provides information about configuring user details such as user name, and email address, and password. You might want to change the password every 90 days or according to the organizational security compliance policy. If a user forgets the password, you might want to reset the password. You might want to reset the password expiring.

User Interface to Edit the User Details

The user details can be reset or updated using,

- The HTML5 user interface
- Appliance/VM Console

Change User Details or Reset Password Using HTML5 User Interface

You might want to change user details or reset the password using HTML5 user interface.

Prerequisites

- Verify that you can open the **VMware Skyline Health Diagnostics** HTML5 URL in the browser window.
- For **shd-admin** role, verify that you can log in using **shd-admin** credentials to VMware Skyline Health Diagnostics HTML5 user interface
- For **operator** user role, verify that you can log in using your credentials to **VMware Skyline Health Diagnostics** HTML5 user interface.

Procedure

- 1 Log in to **VMware Skyline Health Diagnostics** HTML5 user interface
- 2 Click **RESET PASSWORD** from the topmost ribbon, if password is expiring.
- 3 Else click **Setting** tab in the top-menu.
- 4 Click **User Management** option from the left side menu.
- 5 Select user to reset the password using any of the following options,
 - a To search by user name, click the **Filter icon** against the **User name** and enter user name and click **Enter**. The users matching the user name will be listed.
 - b To search by user email id, click the **Filter icon** against the **Email Id** and enter user email id and click **Enter**. The users matching the email address will be listed.
 - c To search by user **user id**, click the **Filter icon** against the **Userld** and enter user id and click **Enter**. The users matching the email user id will be listed.
 - d To search by creation date, click the **Filter icon** against the **Created Date** and creation date and click **Enter**. The users matching the creation date will be listed.
- 6 Click the **Edit icon** to reset user password.
- 7 On the **Edit User** dialog box , edit following details as desired. .User name :
 - a **User Name**: First and last name of the user
 - b **Email Id** : Email address of the user.

- c **Password** : The password user will use at the time of log in

The password must contain at least 8 characters, have characters from 2 classes of Group 1 and 1 from Group 2.

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1s1SV@lid
- This1sVali\$Too
- ThisisnotVal1d

- d **Confirm Password** : to confirm the password entered in the step above.

- 8 Click the **Update** to update the user details.

Results

An user details and password are reset.

Change User Details or Reset Password Using Console

Using console and commands user details can be reset or updated.

Prerequisites

- Verify that you have **root** user credentials for the OS where VMware Skyline Health Diagnostics is installed.
- Verify that you able to SSH or open VM Console from vSphere Client to a VM where **VMware Skyline Health Diagnostics** is installed .
- Verify that you can log in using **shd-admin** credentials to VM Console.
- For more information about enabling the root user login on Photon OS, see : https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html(This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1 Open the Appliance/ VM Console using vCenter Server user interface or SSH to Photon VM.
- 2 Log in as **root** user.
- 3 To invoke the user manager run command **shd-user** from the terminal.
- 4 When prompted, enter the password for **shd-admin**
 - a You must set the password for **shd-admin** now if you did not set it during the install process.
- 5 To change password, select option 3. **Change password for a user.**

- 6 To reset the password, select option 4. **Reset password for a user.**
- 7 When prompted, enter the user name for which the action to be performed.
- 8 If prompted, enter the current password to verify the password.
- 9 Enter the new password and confirm it.

The password must contain at least 8 characters, have characters from 2 classes of Group 1 and 1 from Group 2.

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1sISV@lid
- ThisIsVali\$Too
- ThisisnotVal1d

Results

The password is successfully changed for the user.

Resetting the Expired Password for **shd-admin**

The **shd-admin** cannot reset the password when it is already expired, using HTML5 user interface. The VM console with the **root** credentials must be used to reset the expired password for **shd-admin**.

Prerequisites

- Verify that you have **root** user credentials for the Appliance/VM **VMware Skyline Health Diagnostics** is running.
- Verify that you able to SSH or open VM Console from vSphere Client to an Appliance/VM where VMware Skyline Health Diagnostics is running .
- Verify that you can log in using **root** credentials to OS.
- For more information about enabling the root user log in on Photon OS, see : https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html(This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1 Open the VM/Appliance Console using vCenter Server user interface or SSH
- 2 Log in as a **root** user.
- 3 Run command: `shd-config resetadmin`
- 4 Provide the expired password when prompted.

5 Enter the new password and confirm it.

The password must contain at least 8 characters, have characters from 2 classes of Group 1 and 1 from Group 2.

- Valid Character Class Group 1: [a-z], [A-Z], [0-9]
- Valid Character Class Group 2: [~!@#\$\$%^&]

For example,

- Thi1sISV@lid
- ThisIsVali\$Too
- ThisisnotVal1d

6

Results

The **shd-admin** user password is updated.

What to do next

You can only reset the expired password if you have the current expired password for the shd-admin user

Configuring Password Rotation and Account Lockout Policies

You can configure password rotation and account policies for VMware Skyline Health Diagnostics.

You can customize Password and account lockout policies based on the requirements of your organizations. These settings are stored in the configuration file **/opt/vmware-shd/vmware-shd/app/apiserver/vmware-shd.conf** in the *[account]* section

Element	Description	Parameter	Default	Minimum	Maximum
Password History	Number of previous passwords to be remembered. If set, using one of the last 'histories' will be disallowed.	account/history	3	0	5
Maximum password age	Maximum age of a password in days after which UI authentication will fail with password expired error.	account/passage	90	1	No Limit

Element	Description	Parameter	Default	Minimum	Maximum
Log in Failure window	Time window in minutes to track the authentication failures.	account/failwindow	5	1	No Limit
Log in Failure Count	Number of successive failures tolerated before locking the account.	account/failcount	0	1	No Limit
Account Lockout duration	How long in minutes account stays locked.	account/locktime	15	1	No Limit

Caution You must restart the VMware Skyline Health Diagnostics service for the new changes to be effective. Also changing the password history is not tracked if the settings are set 0.

Change Password and User Account Policies

As per organization security compliance policy administrator may like to change the default password and account policies. The default password expiration period is 90 days.

Prerequisites

- Verify that you have **root** user credentials for the Appliance/VM where VMware Skyline Health Diagnostics is running.
- Verify that you can SSH to a VMware SHD Appliance/VM or open the VM Console from vSphere Client as root user
- For more information about enabling the root user log in on Photon OS, see :https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html (This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1 Open VMware SHD Appliance/VM console using vCenter Server user interface or SSH
- 2 Login as the **root** user.
- 3 To change the current directory, run command `cd /opt/vmware-shd/vmware-shd/app/apiserver/`.
- 4 To back-up the current configuration file, run command `cp vmware-shd.conf vmware-shd.conf.back`.
- 5 To edit the configuration file using **vim** editor, run command `vim vmware-shd.conf`.
- 6 In **vi** editor, press the **Insert** key to switch to the edit mode.

- 7 Change the value for the required field.
- 8 To save and exit the editor, press **Esc** key and type **:wq**.
- 9 To restart the services run command `systemctl restart vmware-shd`.

Proxy Settings

You can configure the proxy settings to download the latest software updates.

Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostic HTMLs' user interface using browser.
- Verify that you have the valid credentials to log in VMware Skyline Health Diagnostic
- Verify that you have the details of proxy server and user credentials (if any).
- If your proxy is configured to act as MITM, please see section titled. "Additional configuration for Proxies action as MITM (Man-In-The-Middle)" before configuring the proxy.

Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface
- 2 Click the **Settings** tab in the top-menu.
- 3 Click the **Proxy Settings** option in the left pane.
- 4 Disable the proxy if it is enabled.
Proxy Settings can be edited only when the proxy is disabled.
- 5 Click the **Edit** link on the top-right corner of the proxy dialog box.
Edit Proxy Settings pane appears.
- 6 Enter the required details related to proxy.
- 7 If no user credentials are required for proxy access, select the **Anonymous** Checkbox.
- 8 To check whether the entered details are correct, click the **Test Connection**.
- 9 To persist the settings, click the **Save**.
 - a If you want not to persist, click **Cancel**.

Results

Proxy information updated.

Additional configuration for Proxies acting as MITM (Man-In-The-Middle)

If the proxy is configured to perform SSL decryption and encryption of straight CONNECT and transparently redirected SSL traffic, using configurable CA certificates, it will require additional

configuration on the appliance running VMware Skyline Health Diagnostics. Without this additional configuration, https connections from VMware Skyline Health Diagnostic will fail to verify the proxy generated certificates and result in failures.

Prerequisites

- Verify that you have root credentials to log in VMware Skyline Health Diagnostic Appliance/VM
- Make sure you have the Root Certificate/Certificate used by Proxy to sign the certificates used for connections. Normally this will be root certificate of your internal CA

Procedure

- 1 Open the Root/Proxy Certificate in a text editor and copy the contents
- 2 Log in to the Appliance running VMware Skyline Health Diagnostics as **root** user, using any SSH Clients
- 3 Create a temporary file to hold the copied certificate contents
 - a `vi /tmp/proxy.crt`
 - b Press "I" to change to insert mode
 - c Paste the contents copied in step 1 (Right Click if using putty)
 - d Press "Esc" to switch the insert mode off
 - e Press ":wq" to save and quit the editor
- 4 Update the VMware SHD installation with newly created proxy certificate by executing following command
 - a `shd-config proxycert /tmp/proxy.crt`
- 5 Proceed with configuring the proxy as outlined in the "Proxy Settings" section

Results

Proxy Certificates are installed on VMware Skyline Health Diagnostics

Managing Software Updates

To get regular updates to VMware Skyline Health Diagnostics.

To improve the analytical diagnostics capabilities of VMware Skyline Health Diagnostics, regular updates to the signatures and detection engine are made available. You must keep VMware Skyline Health Diagnostics up to date with new releases to get the latest recommendation on the issues.

View Download and Update History

You can view past download and upgrade history of VMware Skyline Health Diagnostics.

Prerequisites

- Verify that you can open the **VMware Skyline Health Diagnostic** HTML5 user interface in the browser window.
- Verify that you have the valid credential to log in **VMware Skyline Health Diagnostic**.

Procedure

- 1 Log in to the **VMware Skyline Health Diagnostics** UI.
- 2 Click the **Settings** tab in the top-menu.
- 3 Click the **Upgrade & History** in the left pane.
- 4 Click the **Tool Update** tab to see tools upgrade and download history.
- 5 Click the **VCG Update** to see the VMware Compatibility Guide related upgrade and downloads

Results

Under **Upgrade History Summary** section, you can find last 5 upgrade activities.

Under **Download History Summary** section, you can find last 5 download activities.

What to do next

You can optionally check and download new updates.

Check and Download Software Updates

You can get benefited from the latest signatures released for VMware Skyline Health Diagnostics by frequently checking for updates and downloading the updates.

Check and download new updates for **VMware Skyline Health Diagnostics**.

Prerequisites

- Verify that you can access **VMware Skyline Health Diagnostic** HTML5 user interface.
- Verify that **VMware Skyline Health Diagnostics** has Internet connectivity to VMware Server.
- Any authenticated user can check for the updates. But only **shd-admin** user can perform the download action.

Procedure

- 1 Log in to the VMware Skyline Health Diagnostics UI.
- 2 Click the **Settings** tab in the top menu.
- 3 Click the **Upgrade & History** in the left pane.
- 4 Click the **Tool Update** tab.

- 5 To check whether new updates are available, click the **CHECK TOOL UPDATES**.

If new updates are available, a download option is enabled.

- 6 To download the update, click the **DOWNLOAD UPDATES** (This option is available only for the **shd-admin** user.)

Results

New updates are downloaded.

What to do next

After the updates are downloaded, reboot the Appliance/VM running the VMware Skyline Health Diagnostics. On startup, the software is updated automatically.

Check and Download Compatibility Guide Updates

You can get benefited from the latest VMware compatibility guide updates released for ESXi host, hardware, and IO devices by frequently checking for **VCG Updates** and downloading the updates.

Check and download new updates for VCG Database using [VMware Compatibility Guide](#)

Prerequisites

- Verify that you can access VMware Skyline Health Diagnostics the HTML5 user interface.
- Verify that VMware Skyline Health Diagnostics have Internet connectivity to VMware Compatibility Guides (<https://www.vmware.com>).

Procedure

- 1 Log in to the VMware Skyline Health Diagnostics UI.
- 2 Click the **Settings** tab in the top-menu.
- 3 Click the **Upgrade & History** in the left pane.
- 4 Click the **VCG Update** tab.
- 5 Click the **UPDATE VCG DATABASE** to download the VCG updates.

VCG and vSAN HCL data is refreshed with latest data from VMware Compatibility Guides

Results

VCG and vSAN HCL data is refreshed with latest data from VMware Compatibility Guides.

Note: Update process can take substantially long time to complete (~30-40 minutes). Once started the process runs asynchronously and post update, VCG Database details will be updated in the UI. You can proceed with other activities on the UI without blocking/failing updates

Managing the Behavior and Performance

You may want to change the various setting for Skyline Health Diagnostics Appliance for better user experience and performance. The configuration settings are now exposed in the user interface for easy and quick access.

Only **shd-admin** user or user with **Administrative** privilege can modify the following proerties. You can modify following properties from Skyline Health Diagnostics User Interface,

Log File Size	This property indicates the maximum allowed file size for Skyline Health Diagnostics logs. If the size of the logs exceeds this value, the logs are overwritten. Note the value is specified in Megabyte (MB).
Log File Count	This property indicates the number of Skyline Health Diagnostics log files that will be retained after log rotation.
Password History	This property indicates the number of saved passwords that were used previously . Note: You cannot reuse any of the saved passwords.
Password expiry (in days)	This property indicates the duration (in days) for which a password can be used. Beyond this period, the UI authentication will fail. You can set the value as 90 or 180 days.
Log in Failure Count	This property specifies the permitted number of authentication failures before the user account is locked. Setting to 0 will disables Account Lockout.
Log in Failure Window	This property specifies the time duration in minutes to track authentication failures before account lockout.
Account Lockout Duration	This property specifies the amount of time (in minutes) a account remains locked. During this time User is disallowed from accessing the UI.
Log Analyze Limit	Limit the log analysis to log events within last "Log Analyze Limit" days from log collection time. Setting to 0 will disable the limit.
Number of Log Indexers	This property specifies the number of log indexers deployed for log indexing. The log indexer helps to index the logs , faster the indexing done, quickly logs can be analyzed and report can be generated. Recommanded number of indexer are n-1, where n is number of vCPUs for Skyline Health Diagnostics VM. The default vCPUs for VM are four (4) so, its recommaneded to keep this value to three (3).
Number of Log Extractors	This property specifies the number of log extractions that can run in parallel.

Log Generation Timeout	This property specifies period (in minutes) for which a analyze workflow will wait log for log bundle generation to complete . The value being 0 indicates no timeout. Used during the log collection phase of analyze operation.
Log Download Timeout	This property specifies period (in minutes) for which a analyze workflow will wait for log bundle download to complete. The value being 0 indicates no timeout. Used during the log collection phase of analyze operation.
Log Extraction Timeout	This property specifies period (in minutes) for which a analyze workflow will wait for log bundle extraction to complete. The value being 0 indicates no timeout. Used during the log extraction phase of analyze operation.
SSH Keepalive Timeout	This property specifies period (in minutes) for which a workflow will wait for an SSH connection to respond.
Show Owned Reports Only	This property allows access to a report that you own. Note: shd-admin has access to all reports.
Report Retention Period	This property indicates the purge reports older than the specified number of days. Use 0 to disable auto purge.
HTTP/HTTPS Connection Timeout	This property specifies the timespan (in seconds) to wait before the external HTTP/HTTPS connections timeout.
Max VCG Update Connections	This property specifies the number of parallel connections established to VCG site during VCG update.
Max VCG Update Requests/Min	This property specifies the number of requests per minute sent to VCG site during VCG update.

Updating the Property Value


You can update the property value in the configuration setting to change the behavior and performance of the appliance.

Prerequisites

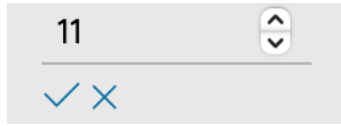
- Verify that you can access VMware Skyline Health Diagnostics the HTML5 user interface.

Procedure

- 1 Log in to the **VMware Skyline Health Diagnostics** UI.
- 2 Click the **Settings** tab in the top-menu.
- 3 Click the **Configuration** in the left pane.
- 4 Select the property you want to modify.

- 5 Click on the edit button  to update the property value.
- 6 You can directly input the desired value or use the up or down arrow to increment or

decrement the value.



- 7 Click OK button  to save the value.

Results

The update value will be saved for the property.

Managing SSL Certificates

You can configure SSL certificates for VMware Skyline Health Diagnostics.

VMware Skyline Health Diagnostics uses SSL certificates to encrypt communications between the server and the client browser to securely access and process the data. By default, the server uses self-signed certificates generated during the installation. Your environments might require use of trusted certificates. You can get a custom certificate as per your organization guideline generated/signed and update VMware Skyline Health Diagnostics to use those. Ensure custom certificate meets [Custom Certificate Requirements](#) mentioned below.

Custom Certificate Requirements

Your custom certificate must satisfy following requirement to adhere to security standards.

Please ensure the custom certificate meets the organizational compliance policy, with following basic requirements.

Element	Suggested Value
Key size	2048 bits (minimum) to 16384 bits (maximum)
Key Encoding	PEM
Key Format	CRT
SSL Version	x509 version 3
SubjectAltName	Must contain DNS Name of the machine hosting VMware Skyline Health Diagnostics.

To replace certificate, **generate a certificate signing request**. Get the certificate signed by certificate authority. Finally replace the certificates for VMware Skyline Health Diagnostics.

Generate Certificate Signing Request

You can replace the default certificates with your custom certificates.

Prerequisites

- Verify that you have **root** credentials for the Appliance/VM where VMware Skyline Health Diagnostics is running
- For more information about enabling the root user log in on Photon OS, see : https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html(This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1 Open Appliance/VM Console where VMware Skyline Health Diagnostics is running either from vCenter Server user interface or SSH
- 2 Log in as a **root** user.
- 3 To navigate to the root directory, run the command **cd /**.
- 4 To create a directory under the root folder on a VM where VMware Skyline Health Diagnostics is installed, run the command **mkdir newcert**.
- 5 To change the working directory to the new directory, run **cdnewcert**.
- 6 To copy the configuration file to the present location, run the command **cp /opt/vmware-shd/vmware-shd/conf/ssl/conf ./.**
- 7 Edit the configuration as required
 - a To edit the configuration file using vi editor, run command **vi conf**.
 - b To match your organization details, edit the [**req_distinguished_name**] section.
 - c Set the entries for commonName and DNS.1 to match the FQDN of the VM.
- 8 To generate a new certificate signing request run **openssl req -new -config conf -newkey rsa:2048 -nodes -keyout rui.key -out rui.csr**.

Key and certificate signing request (CSR) files are created in the current directory. (rui.csr, rui.key).
- 9 Use the rui.csr file for signing request from our internal/external CA.

Results

Certificate signing request generated.

What to do next

Send the certificate signing request to your internal or external CA for signing.

Replace the Default Certificate with the Custom Certificate

You can replace the default self-signed certificate with custom certificate to meet the organization security compliance guidelines.

Prerequisites

- 1 Verify that you have **root** credentials for the Appliance/VM where VMware Skyline Health Diagnostics is running
- 2 Verify that you have the signed SSL Certificate with the CSR generated in the previous section.
- 3 For more information about enabling the root user log in on Photon OS, see https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html (This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1 SSH to the Appliance/VM where VMware Skyline Health Diagnostics running.
- 2 Log in as a **root** user.
- 3 To change the working directory to the directory you created during generating this CSR stage, run the **cd** command. Ex: **cdnewcert**
- 4 To create a new file by name **rui.crt** using **vi** editor, run command **vi rui.crt**.
- 5 To copy the content of CA signature that you received from your CA authority, open the CA signed certificate on your desktop using any text editor and copy the content.
- 6 To paste the content to rui.crt file using **vi** editor, press **I** to enable insert mode.
You must see **-- INSERT --** in the bottom of the screen hitting the insert mode.
- 7 Right-click to paste the copied certificate details.
 - a If your CA provides any intermediate certificates, make sure you paste them following the actual certificate.
- 8 Save the file by pressing the following sequence **Esc:wq**.
- 9 Copy the previously generated key and certificate files to the location where default certificates are saved.
 - a `cp rui.crt rui.key /opt/vmware-shd/vmware-shd/conf/ssl/`
- 10 Restart the web server by running `systemctl restart nginx`.
- 11 Log in to the UI using browser and verify that the new certificates are in use.

Results

The web server runs with customer certificates.

What to do next

You see that the services are not available, you can revert to self-signed certificate following the procedure in [Reverting to Self-Signed Certificate](#).

Reverting to Self-Signed Certificate

If the attempt to replace self-signed certificates with customer certificates fails, Administrator must revert to self-signed certificate.

Prerequisites

- Verify that you have **root** credentials for the Appliance/VM where VMware Skyline Health Diagnostics is running
- For more information about enabling the root user log in on Photon OS, see https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html(This configuration is not necessary for VMware SHD Appliance as by default it is configured to allow root user logins through SSH)

Procedure

- 1 SSH to the Appliance/VM where VMware Skyline Health Diagnostics running.
- 2 Log in as a **root** user.
- 3 To revert to self-signed certificate run command `shd-config refreshcert`.

Results

VMware Skyline Health Diagnostic runs with refreshed self-signed certificates.

Managing the Services

You can configure the services for VMware Skyline Health Diagnostics services running in the Appliance/VM.

A web server and an application server together are responsible for providing UI and diagnostics capabilities of VMware Skyline Health Diagnostics. The server is implemented in the form of services whose settings are auto configured. You need not change the settings unless the technical support guides you.

Server Component	Service Name	Description
Webserver	nginx	Provides HTML5 user interface through the browser.
Application Server	vmware-shd	Handles upload and diagnostics for log bundles.

All the services are configured to auto start on the system startup.

You can use command `systemctl` to check start, stop, restart, and check status (You must log in to shell as the **root** user to perform any service-related activities).

Command: `systemctl start|status|restart|stop SERVICE_NAME`

Using VMware Skyline Health Diagnostics

3

A guide to perform operations in VMware Skyline Health Diagnostics using HTML5 user interface.

This chapter includes the following topics:

- [Operations in VMware Skyline Health Diagnostics](#)
- [Log in to VMware Skyline Health Diagnostics from Web Browsers](#)
- [Connect and Analyze Log Bundles for vCenter and ESXi](#)
- [Connect and Analyze Log Bundles from the Disconnected ESXi Host](#)
- [Health Checks for VMware Cloud Foundation \(Technical Preview Mode\)](#)
- [Health Checks for VMware vSAN Storage](#)
- [Upload and Analyze Log Bundles](#)
- [View Analysis Reports](#)
- [Deleting Single Analysis Report](#)
- [Saving or Deleting Multiple Analysis Reports](#)
- [Configuring Auto Delete for Analysis Reports from User Interface](#)
- [Configuring Auto Delete for Analysis Reports using Config File](#)
- [Interpreting the Diagnostics Report](#)
- [Interpreting VCG/vSAN HCL Validation Summary.](#)
- [Interpreting VMware Cloud Foundation Diagnostics Report](#)
- [Interpreting VMware vSAN Storage Report](#)
- [Adding and Removing Tags for the Analysis Report](#)
- [Help and Support](#)
- [View the CEIP Data Collected for Reporting and Analytics](#)

Operations in VMware Skyline Health Diagnostics

You can upload , analyze, and view the reports using VMware Skyline Health Diagnostics.

Operations

With VMware Skyline Health Diagnostics, you can

- Log in to VMware Skyline Health Diagnostics
- Run Analysis/Diagnostics, directly connecting to vCenter Server or ESXi Server
- Manually upload and analyze the log bundles.
- View results of the analysis in the form of reports.
- View past analysis details up to last 50 executions.

Supported Log Bundles

VMware Skyline Health Diagnostics version **2.5.1** can analyze problems for the following versions for vSphere products,

- Diagnostics Log Bundles form VMware ESXi Server version 6.5 , 6.7 and 7.0.
- Diagnostics Log Bundles form VMware vCenter Server and Appliance version 6.5, 6.7 and 7.0
- Log bundles for the failed install, upgrade, or migrate vCenter Servers version 6.5, 6.7 and 7.0.

Supported Browsers

Operating System	Browser
Windows 10	Microsoft Internet Explorer 11 and later. Mozilla Firefox: 56 and later. Microsoft Edge : 44.18362.449.0 Microsoft Edge HTML : 18.18363 and later Google Chrome: 84 and later. Safari : 12.1 and later
Mac OS	Mozilla Firefox: 56 and later. Google Chrome: 84 and later. Safari : 12.1 and later

Log in to VMware Skyline Health Diagnostics from Web Browsers

VMware Skyline Health Diagnostics provides the HTML5 user interface to log in, upload and analyze the log bundle. User can change setting and download updates.

Prerequisites

- Verify that you have HTML5 compatible browser.
- Verify that you have valid credentials for accessing VMware Skyline Health Diagnostics.

Procedure

- 1 Open a web browser and enter the URL for your VMware Skyline Health Diagnostics instance: **https://vmware-shd_ip_address_or_fqdn.**
- 2 If a warning message about un-trusted SSL certificate appears, select the appropriate action based on your security policy.
- 3 Enter the credentials of an operator user and click login.
- 4 If the credentials are accepted, you will be redirected to the main UI page.
- 5 To log out, click the **Log Out** option on the top corner of the UI

What to do next

Upload a new log bundle or view historical reports.

Connect and Analyze Log Bundles for vCenter and ESXi

You can connect to vCenter Server. You can select Diagnostic or Security assessment base on VMware Security Guideline or vSAN Health or any combination of options base on your requirements. Then collect logs by selecting desired hosts from the inventory and analyze. The successful analysis generates the detailed report having the list of problems and resolutions.

The diagnostics plugin represents generic category of the problems related to the vSphere operations.

The VMware Security Advisory plug-ins represent the security issues identified by VMware Security Advisory.

The vSAN Health plug-ins perform vSAN Health related checks and validation.

The VMware Diagnostics plugin needs log bundle from the target host for the analysis.

The VMware Security Advisory plugin needs the product build information, that gets collected using API.

For the vSAN Health Checks vSAN related data gets collected using API.

Prerequisites

- Verify that you have the vSphere user name and password.
- Verify that the vSphere user has roles and permissions to collect logs.
- Verify that you have login credentials for VMware Skyline Health Diagnostics
- Verify that you have VCSA appliance root credentials if you are planning to collect logs from the vCenter appliance. If, the vCenter UI is not accessible use VCSA appliance root credentials.
- Verify that the vCenter user has following privileges
 - Global.Diagnostics

- System.View
- Read Permissions on the inventory objects (Datacenter/Cluster/Host)

Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 In the top-menu, click **Analyze > Connect and Analyze > vCenter / ESXi Details**.
- 3 Enter the vCenter Server/ESXi Server Hostname or IP address in **Host Name/IP** field.
 If vCenter or ESXi Server is running on not running services on default port 443, append the port number to the Hostname/IP address with s colon.
 Example: VCENTER_HOSTNAME:PORT
- 4 Enter the vCenter Server/ESXi Server user name in the **Username** field.
- 5 Enter the password for the user in the **Password** field.
- 6 Select **Skip SSL Check**, if you want to skip the SSL verification.
 - a Check **Skip SSL Check**, if the vCenter uses the self-signed certificate.
- 7 Select **Connect to vCenter Appliance**, if you want to collect logs using VAMI interface and vCenter HTML user interface is not reachable.
 - a For this use case, please use root user account details in step 5 and 6
- 8 Click **Check Connection**. This action validates the credential by performing a login to the given vCenter/ESXi Server.
 - a If the connection is successful , the message **vSphere API connection is successful**. displayed.
 - b If the error is observed while connecting to vCenter, the Run Diagnostics is **grayed out** and error message displayed.

Run Diagnostics is enabled if the connection to check is successful.
- 9 Click **Run Diagnostics**.
Select Inventory windows shows all the hosts available in vCenter including option to collect the diagnostic log bundle form vCenter Server.

- 10** In step 1, **Inputs for diagnostics start**, Select appropriate plug-ins to run (Diagnostics, VMSA, vSAN Health Check)

Select Plugins and Inventory for Diagnostics

- ☒ Diagnostics Plugins ☒ VMware Security Advisory Plugins
☒ vSAN Health Check Plugins

- 11** To run the diagnostics, select host by clicking the check box of the respective hosts.
- 12** Select **Include vCenter for Analysis** if you want to analyze vCenter (this is required for both **Diagnostics** and **VMware Security Advisory** plug-ins).
- 13** If vSAN Health Check plug-ins are selected, make sure **Include vCenter for Analysis** is selected. All vSAN Cluster's part of this vCenter will be analyzed
- 14** Click **Validate**.
- Submit for Analysis** window is displayed with count of vCenter & host selected of analysis. If any disconnected hosts are part of inventory, you can click 'BACK' and deselect them.
- 15** In step 2 , **Submit for Analysis** , Provide the **Tag Name** to remember the analysis. The tagging helps in quick search of the analysis report afterwards.
- 16** In step 2 , **Submit for Analysis** , Provide the **Log Analyze Limit (Days)** to limit the analysis of logs to the specified number of days from the log collection date. If you do not specify any value, default value is **0** to analyze all the logs. e.g. If you are collection the logs on July 20th and you want to limit the analysis of log from July 10th till July 20th, then you will input value **10** in the **Log Analyze Limit (Days)**

Select Inventory

1 Inputs for diagnostics Start

2 Submit for Analysis

Submit for Analysis

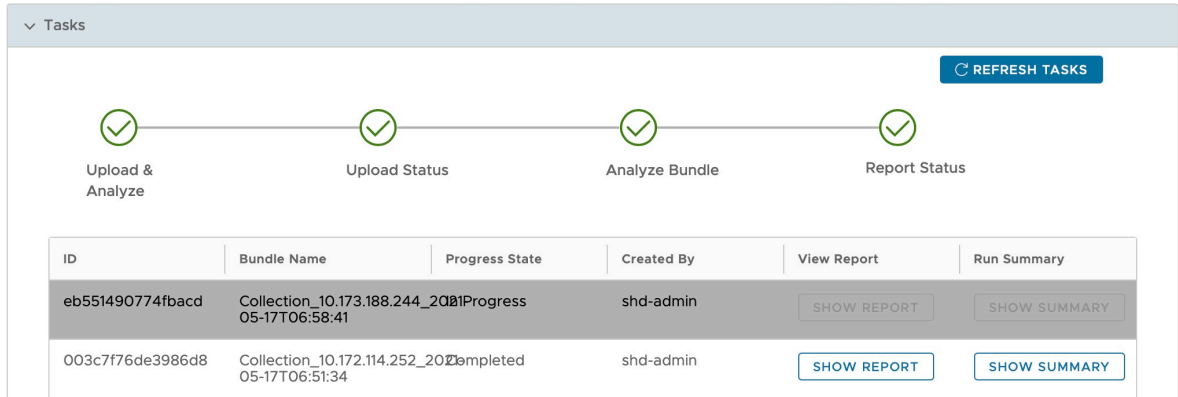
Tag analysis as:

Log Analyze Limit (Days) :

17 Click **Finish** on the **Submit for Analysis** window.

Download and Analysis starts and VI Admin can see the progress under Tasks follows:

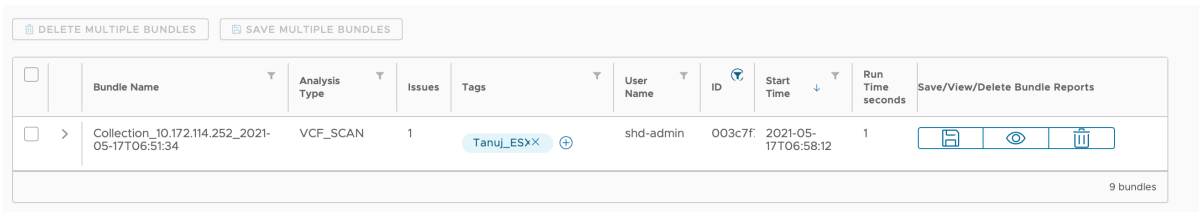
Figure 3-1. Tasks View



18 Once the Analysis is complete, Click **Show Report** button to see the **View Analysis Report** icon.

19 To download the analysis report, click the **Download** icon.

Figure 3-2. Download or View or Delete Report



Connect and Analyze Log Bundles from the Disconnected ESXi Host

You can collect logs and analyze from disconnected ESXi host, collect logs by selecting hosts from the inventory and analyze. The analysis report shows you the issues and remediation KBs.

You can connect to vCenter and see vCenter UI after login.

Prerequisites

- Verify that you have the user credentials or vCenter Sever.
- Verify that the vCenter user has roles and permissions to collect logs.
- Verify that you have login credentials for VMware Skyline Health Diagnostics
- Verify that you have root credentials for disconnected ESXi hosts.
- Verify that ESXi hosts can be connected over SSH

- Verify that the vCenter user has following privileges
 - Global.Diagnostics
 - System.View
 - Read Permissions on the inventory objects (Datacenter/Cluster/Host)

Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 In the top-menu, click **Collect Logs and Analyze**.
- 3 Enter the vCenter Server Hostname or IP address in **Host Name/IP** text box.
 If vCenter Server is running on not running services on default port 443, append the port number to the Hostname/IP address with s colon.
 Example: VCENTER_HOSTNAME:PORT
- 4 Enter the vCenter Server user name in the **Username** text box.
- 5 Enter the password for the user in the **Password** text box.
- 6 Select **Skip SSL Check**, if you want to skip the SSL verification.
 - a Check **Skip SSL Check**, if vCenter uses the self-signed certificate
- 7 Click **Check Connection**. It validates the credential by performing a login to the given vCenter/ESXi Server.
 - a If the connection is successful , you see the **vSphere API connection is successful** message.
 - b If the error is observed while connecting to vCenter, the **Run Diagnostics** is grayed out and error message displayed.

Run Diagnostics is enabled if the connection **Check Connection** operation is successful.
- 8 Click **Run Diagnostics**.
Select Inventory wizard provides the options for selecting the type of plug-ins to include in analysis and lists the inventory tree including option to collect the diagnostic log bundle form vCenter Server.
- 9 Select hosts in the disconnected state to run the diagnostics by clicking the check box of the respective hosts.
- 10 Select **Include vCenter for Analysis** if you want to analyze vCenter.
- 11 Click **Validate**.
- 12 **Submit for Analysis** window is displayed, having the count of ESXi hosts in the disconnected state and requesting the ESXi host credentials.

- 13** Enter the ESXi host user name and password for each host. If the user name and password is same for all the host, select the **Apply same password for all disconnected hosts** option.

VMware Skyline Health Diagnostics have credentials to connect to ESXi host in the disconnected state. **Check Host Connection** button is enabled.

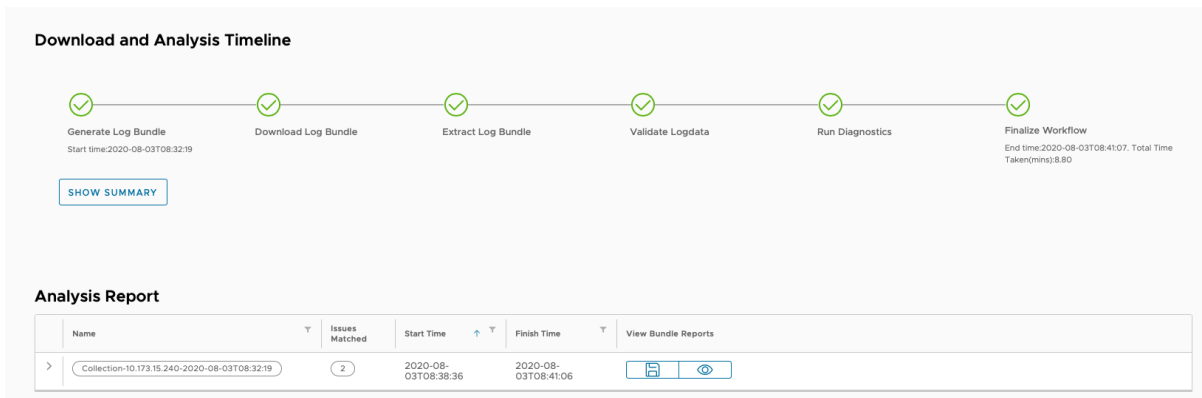
- 14** Click **Check Host Connection** after you user credentials for hosts are entered.
- 15** If the connections to the selected hosts are successful, **Finish** button will be enabled.
- 16** Click **Finish** on **Submit for Analysis** window.

Download and Analysis starts and VI Admin can see the progress as below,



- 17** Once the Analysis is complete, Click **View Report** icon to see the analysis report.

Analysis report



- 18** To download the analysis report, click the **Download** icon.

Health Cheks for VMware Cloud Foundation (Technical Preview Mode)

You can connect to VMware Cloud Foundation SDDC Manager and select Health Check plug-ins to get the health report of the products by collecting logs and other information. Successful analysis generates the detailed report having the list of issues in VMware Cloud Foundation environment.

The VMware Cloud Foundation Health Check plug-in have health checks related to the VMware Cloud Foundation Workload Domains for the products that includes

- vCenter Server
- ESXi

- VMware NSX
- VMware Cloud Foundation SDDC Manager
- VxRail Manager
- VMware vRealize Automation
- vRealize Operations
- vRealize Log Insight
- vRealize Life Cycle Manager

Prerequisites

- Verify that you have login credentials for VMware Skyline Health Diagnostics.
- Verify that you have the VMware Cloud Foundation SDDC Manager user name and password.
- Verify that the VMware Cloud Foundation user has administrative roles and permissions to collect logs and health information.
- Verify that the VMware Cloud Foundation user has following privileges
 - Admin privilege

Procedure

- 1 Log in to the VMware Skyline Health Diagnostics UI using a supported browser.
- 2 In the top-menu, click **Analyze > Connect and Analyze > VMware Cloud Foundation**.
The Connect to SDDC Manager Dialog box opens.
- 3 Enter the SDDC Manager hostname or IP address in **SDDC Manager** text box.
If SDDC Manager Server is not running on default port 443, append the port number to the hostname or IP address with colon.
Example: `https://SDDC-Manager_HostName:Port`
- 4 Enter the SDDC Manager Server user name in the **Username** text box.
- 5 Enter the password for the user in the **Password** text box.
- 6 If the SDDC Manager uses the self-signed certificate please check **Skip SSL Check** else de-select it.
- 7 Click **Check Connection**. This action validates the credential by performing a login to the given SDDC Manager Server.
Validate is enabled if the check connection operation is successful.
- 8 Click **Run Diagnostics**.
The **Select Inventory** windows displays all the Domains registered with the SDDC Manager.

- 9 Select the VMware Cloud Foundation Health Check plug-ins check box.

Select Health Check plug-in

Select Inventory

- Inputs for diagnostics Start
- Submit for Analysis

Select Plugins and Inventory for Diagnostics

☒ Health Check Plugins

☐ 0.0.0.0 (SDDC-Manager)

☐ sfo-m01 (MANAGEMENT-Domain)

CANCEL VALIDATE

- 10 To run diagnostics, select domain by clicking the check box of the respective domain.

- 11 Select **SDDC Manager** if you want to analyze the SDDC Manager.

- 12 Click **Validate**.

Submit for Analysis window displays the input field Tag Name.

- 13 Provide the **Tag Name** to remember the analysis. The tagging helps in quick search of the analysis report afterwards.

- 14 Click **Finish** on the **Submit for Analysis** window.

Log and Health information collection start, the **Tasks** frame shows the progress. VI\VMware Cloud Foundation Admin can see the progress as follows:

Tasks

REFRESH TASKS

✓

Generate Log Bundle

Start time:2021-05-17T06:58:41

✓

Download Log Bundle

✓

Extract Log Bundle

✓

Validate Logdata

✓

Run Diagnostics

ID	Bundle Name	Progress State	Created By	View Report	Run Summary
4d5deb34bab50d49	Collection_10.172.114.252_2021-Progress 05-17T07:52:53		shd-admin	SHOW REPORT	SHOW SUMMARY

- 15 After the analysis is complete, click **Show Report** icon to view the **Save or View or Delete** analysis report option.

Analysis report

Tasks

REFRESH TASKS

Generate Log Bundle
Start time:2021-05-17T06:58:41

Download Log Bundle

Extract Log Bundle

Validate Logdata

Run Diagnostics

ID	Bundle Name	Progress State	Created By	View Report	Run Summary
eb551490774fbacd	Collection_10.173.188.244_2021-05-17T06:58:41	Completed	shd-admin	SHOW REPORT	SHOW SUMMARY

- 16 To download the analysis report, click the **Download** icon.

DELETE MULTIPLE BUNDLES SAVE MULTIPLE BUNDLES

	Analysis Type	Issues	Tags	User Name	ID	Start Time	Run Time seconds	Save/View/Delete Bundle Reports
>	DIAGNOSTICS, VMSA_SCAN, VSA_N_SCAN	22	nitin-1X	shd-admin	eb551490774fbacd	2021-05-17T07:11:40	599	Save View Delete

10 bundles

Health Checks for VMware vSAN Storage

You can connect to VMware vCenter Server and select vSAN-Health Check to get the health report of the vSAN Clusters by collecting logs and other information. Successful analysis generates the detailed report having the list of issues in VMware vSAN Storage.

The VMware vSAN storage Health Check plug-in have health checks related to the VMware vSAN Storage Clusters.

Prerequisites

- Verify that you have login credentials for VMware Skyline Health Diagnostics.
- Verify that you have the VMware vCenter Server user name and password.
- Verify that the VMware vCenter Server has administrative roles and permissions to collect logs and health information.
- Verify that the VMware vCenter user has following privileges
 - Admin privilege

Procedure

- 1 Log in to the VMware Skyline Health Diagnostics UI using a supported browser.

- 2 In the top-menu, click **Analyze > Connect and Analyze > vSAN-HealthCheck**.

The Connect to **vCenter Details** Dialog box opens.

- 3 Enter the vCenter Server hostname or IP address in **vCenter Server** text box.

If vCenter Server is not running on default port 443, append the port number to the hostname or IP address with colon.

Example: `https://vCenter_Server_HostName:Port`

- 4 Enter the vCenter Server user name in the **Username** text box.

- 5 Enter the password for the user in the **Password** text box.

- 6 If the vCenter Server uses the self-signed certificate please check **Skip SSL Check** else de-select it.

- 7 Click **Check Connection**. This action validates the credential by performing a login to the given vCenter Server.

Validate is enabled if the check connection operation is successful.

- 8 Click **Run Diagnostics**.

The **Select Clusters** windows displays all the vSAN enabled clusters in vCenter Server.

- 9 Select the vSAN Health Check plug-ins check box.

Select vSAN Health Check plug-in

The screenshot displays two side-by-side dialog boxes. The left dialog, titled 'Select Clusters', contains a list with two items: '1 Inputs for diagnostics Start' and '2 Submit for Analysis'. The right dialog, titled 'Select Inventory for Diagnostics', contains a section for 'vSAN Health Check Plugins' with a checked checkbox. Below this, a note states 'Only vSAN enabled clusters are listed and vSAN-HealthCheck will be processed'. A list of clusters follows, with 'vLCM-DC' and 'Test-Infra' selected via checkboxes. At the bottom right of the right dialog, there are 'CANCEL' and 'VALIDATE' buttons.

- 10 To run diagnostics, select cluster by clicking the check box of the respective cluster.

- 11 Select **vCenter Server** if you want to analyze the vCenter Server.

12 Click **Validate**.

Submit for Analysis window displays the input field Tag Name.

13 Provide the **Tag Name** to remember the analysis. The tagging helps in quick search of the analysis report afterwards.**14** Click **Finish** on the **Submit for Analysis** window.

Log and Health information collection start, the **Tasks** frame shows the progress. VI\VMware Cloud Foundation Admin can see the progress as follows:

ID	Bundle Name	Progress State	Created By	View Report	Run Summary
4d5deb34bab50d49	Collection_10.172.114.252_2021-Progress 05-17T07:52:53	Progress	shd-admin	SHOW REPORT	SHOW SUMMARY

15 After the analysis is complete, click **Show Report** icon to view the **Save or View or Delete** analysis report option.

Analysis report

ID	Bundle Name	Progress State	Created By	View Report	Run Summary
eb551490774fbacd	Collection_10.173.188.244_2021-Completed 05-17T06:58:41	Completed	shd-admin	SHOW REPORT	SHOW SUMMARY

16 To download the analysis report, click the **Download** icon.

Bundle Name	Analysis Type	Issues	Tags	User Name	ID	Start Time	Run Time(in seconds)	Save/View/Delete Bundle
Collection_10.173.124.1_2021-07-19T08:33:36	VSAN_SCAN	5	vsan: [X] [plus]	shd-admin	cecb1d646ed16566	2021-07-19T08:33:53	5	[Download] [View] [Delete]

Upload and Analyze Log Bundles

You can use this option if you have an existing diagnostic log bundle from vCenter or ESXi Server. You can also use this option to analyze the log bundles from vCenter Install/Upgrade/Migration failures.

Prerequisites

- Verify that you have the log bundle from the ESXi or vCenter Server.
 - Log Bundle: This is the diagnostic data collected from the ESXi or vCenter Server using the Export System logs option from the UI or using the command line option. A single log bundle can contain diagnostic data from multiple ESXi hosts and vCenter Server. You can also use the support bundles collected during failed installations of ESXi or vCenter Server.

Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 In the top-menu, click **Upload Log & Analyze**.
- 3 Provide the **Tag Name** to remember the analysis. The tagging helps in quick search of the analysis report afterwards.

- 4 Provide the **Log Analyze Limit (Days)** to limit the analysis of logs to the specified number of days from the log collection date. If you do not specify any value, default value is **0** to analyze all the logs. e.g. If you are collection the logs on July 20th and you want to limit the analysis of log from July 10th till July 20th, then you will input value **10** in the **Log Analyze Limit (Days)**

Upload Bundle for Analysis

Tag Analysis as:

Tag Name


Log Analyze Limit (Days)

0

Bundle To Upload

Choose File

no file selected


UPLOAD & ANALYZE

- 5 Click **Choose File** to select the log bundle to be analyzed and click **Open**.
- 6 Click **Upload & Analyze** to start upload and analysis.
- The real-time progress of upload and analysis is displayed on the screen.
- 7 The summary appears in the bottom of the UI window with options to see the results.
- 8 To download the report click **Save**.
- 9 To view the report, click **View**.

Results

The log bundle is uploaded and analyzed.

View Analysis Reports

After the VMware Skyline Health Diagnostics analyzes an uploaded/collected log bundle it generates a detailed report with all findings. You can immediately see it or save it for a later use. UI provides access 50 most recent reports.

As an operator you might want to compare the before and after a remediation the resolution status of the issue.

Prerequisites

Verify that you have a valid user account credential with VMware Skyline Health Diagnostics.


Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 Click **Show Reports** on the top navigation menu.
- 3 The left menu showing following four filters,
 - a Diagnostics Report : Shows the reports that have Diagnostics plug-ins selected at the time of analysis.
 - b Security Reports : Shows the reports that have Security plug-ins selected at the time of analysis.
 - c vSAN Reports : Shows the reports that have vSAN plug-ins selected at the time of analysis.
 - d VMware Cloud Foundation Reports : Show the reports that have VMware Cloud Foundation plugin selected at the time of analysis.
- 4 Select any one of the above , you are interested in.
- 5 Select a log bundle using the filter against the **Bundle Name , Analysis Type , Tags, User Name** or **Start Time**. You can use the **Tags** to search quickly the issues base on the keyword that you provided while starting the analysis.



- 6 Click  **(View)** in the right most column to see the details of the report .



- 7 To download the report , click  in the right most column.
- 8 To view the details of report in the same window, click expand > available on left side of the bundle selected.

Results

Selected Report is downloaded locally or opened in a new window depending on the action

Deleting Single Analysis Report

In default configuration all analysis reports are saved perpetually. You can configure a default retention period or manually delete the reports. (This feature is available version 2.5.0 on wards). An operator can delete the analysis reports created by self. Admin user (shd-admin) can delete analysis reports created by any user.

Deleting Analysis Report using UI

Prerequisites


Verify that you have a valid user account credential with VMware Skyline Health Diagnostics.

Note The delete action irreversible. Deleted reports are not recoverable.

Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 Click **Show Reports** on the main menu.
- 3 Click on the report you want delete.



- 4 Click on the  icon in the last column of the report display row
- 5 In the confirmation dialog box click OK to delete the report.

Results

Report is successfully deleted.

Saving or Deleting Multiple Analysis Reports

You can select multiple reports and choose one of the actions from Delete or Save for selected reports.

As an operator you might want to compare the before and after a remediation the resolution status of the issue.

Prerequisites

Verify that you have a valid user account credential with VMware Skyline Health Diagnostics.

Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 Click **Show Reports** on the main menu.
- 3 Select the reports you want to Delete or Save using the checkbox in the first column.

- 4 Option to delete or save gets enabled.



- 5 Choose the action you want to perform

- a If you want to download all selected reports to your workstation, Click Save Multiple



- b If you want to delete all selected reports, DeleteMultiple Bundles



. Click Proceed in the confirmation dialog.

Results

Selected reports are either Saved or Deleted depending on the action.

Configuring Auto Delete for Analysis Reports from User Interface

In default configuration all the Analysis Reports are saved perpetually. You can configure automatic deletion of past reports after a fixed retention period using Skyline Health Diagnostics User Interface.

Prerequisites

- Verify that you have **shd-admin** user credentials for the VMware Skyline Health Diagnostics.
- Verify that you can login to VMware Skyline Health Diagnostics HTML user interface.

Procedure

- 1 Log in to the **VMware Skyline Health Diagnostics** UI.
- 2 Click the **Settings** tab in the top-menu.
- 3 Click the **Configuration** in the left pane.
- 4 Select the property **Report Retention Period** to modify.

- 5 Click on the edit button  to update the property value.

- 6 You can directly input the desired value or use the up or down arrow to increment or



decrement the value.

7 Click OK button  to save the value.

8

Results

Auto Deletion of Analysis Reports is enabled. Reports will be deleted automatically post the configured retention period.

Configuring Auto Delete for Analysis Reports using Config File

In default configuration all the Analysis Reports are saved perpetually. You can configure automatic deletion of past reports after a fixed retention period.

Prerequisites

- Verify that you have **root** user credentials for the OS where VMware Skyline Health Diagnostics is installed.
- Verify that you can SSH to a VMware SHD Appliance/VM or open the VM Console from vSphere Client as root user
- For more information about enabling the root user log in on Photon OS, see :https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html (This step is not required for VMware SHD Appliance as by default root login via SSH is enabled)

Procedure

- 1 Open VMware SHD Appliance/VM console using vCenter Server user interface or SSH
- 2 Login as the **root** user.
- 3 To change the current directory, run command `cd /opt/vmware-shd/vmware-shd/app/apiserver/`.
- 4 To back-up the current configuration file, run command `cp vmware-shd.conf vmware-shd.conf.back`.
- 5 To edit the configuration file using **vim** editor, run command `vim vmware-shd.conf`.
- 6 In **vi** editor, press the **Insert** key to switch to the edit mode.
- 7 Change the value for the field *retention* under *[reports]* section.
This value must be entered as number and denotes days of retention
- 8 To save and exit the editor, press **Esc** key and type **:wq**.
- 9 To restart the services run command `systemctl restart vmware-shd`.

Results

Auto Deletion of Analysis Reports is enabled. Reports will be deleted automatically post the configured retention period

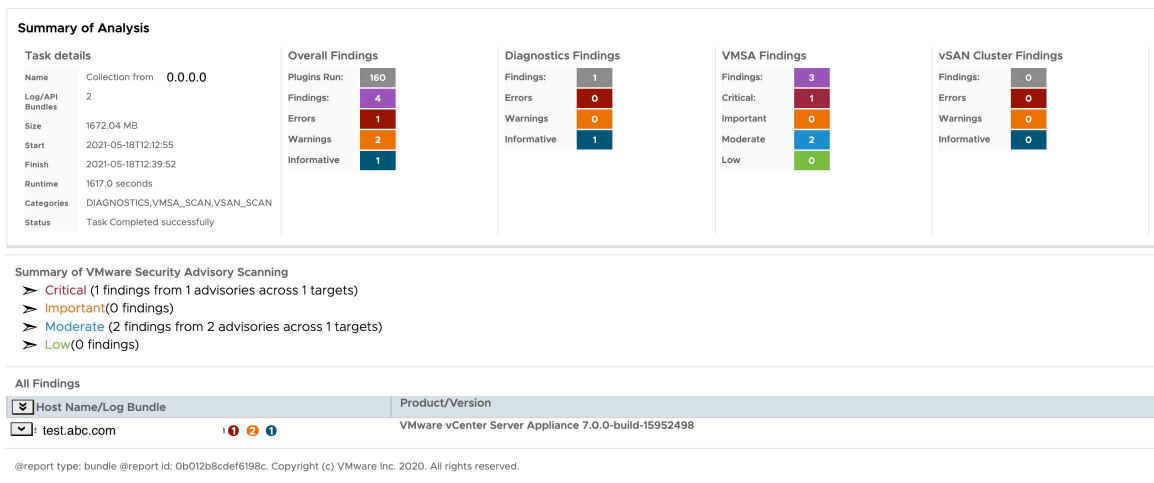
Interpreting the Diagnostics Report

Diagnostics report contains multiple sections with a hierarchical summary of analysis and findings.

View a Summary of Detected Issues

A bundle level report contains multiple sections depending on the types of plug-ins selected for the diagnostics run.

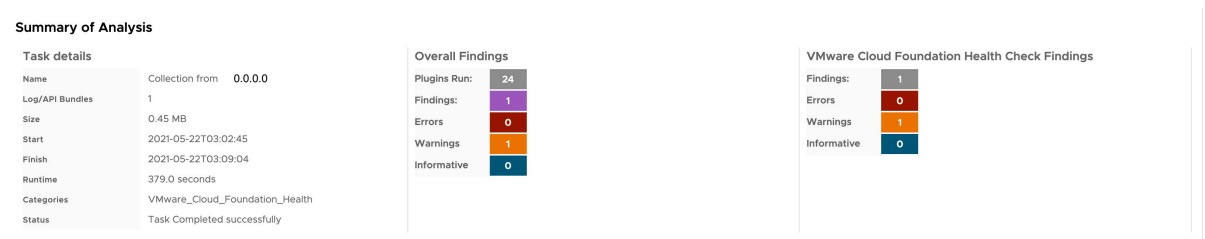
- 1 First section provides a brief summary of task and finding .



a

- VMware Cloud Foundation Summary report will display VMware Cloud Foundation related finding.

Figure 3-3. VMware Cloud Foundation Report Summary



- 2 Second optional section provides the summary of VMware Security Advisory Scanning if the VMware Security Advisory plugin option selected during the diagnostics runs.

Summary of VMware Security Advisory Scanning

- **Critical** (1 findings from 1 advisories across 1 targets)
- **Important**(0 findings)
- **Moderate** (2 findings from 2 advisories across 1 targets)
- **Low**(0 findings)

a

- b The VMware Security Advisory related plug-ins are grouped based on published severity level in the advisory.

- 3 Third Section lists all the findings across all the target ESXi hosts/vCenter included in this run. Each analyzed ESXi host/vCenter has a separate section showing all of the findings across the selected plugin types.

All Findings		
Host Name/Log Bundle	Findings	Product/Version
hostname.domain-name.com	Errors 12 Warnings 25 Info 6	VMware ESXi 6.7.0-build-8169922

Summary of Analysis - Task Details

The task details, from the Summary of Analysis section, displays following

- The details on the analysis task including number of log bundles/hosts.
- Start/end time of the task.
- The total size of all log bundles processed.
- The task status.

Summary of Analysis

Task details

Name	Collection from hostname.domain-name.com
Log/API Bundles	1
Size	67.85 MB
Start	2020-11-04T08:53:53
Finish	2020-11-04T08:58:50
Runtime	297.0 seconds
Categories	VMSA_SCAN,DIAGNOSTICS
Status	Task Completed successfully

Summary of Analysis - Findings

These finding cards provide details on number of plug-ins run and findings based on the alert/severity levels

Summary of Analysis				
Task details		Overall Findings	Diagnostics Findings	VMSA Findings
Name	Collection from 0.0.0.0	Plugins Run: 160	Findings: 1	Findings: 3
Log/API Bundles	2	Findings: 4	Errors: 0	Critical: 1
Size	1672.04 MB	Errors: 1	Warnings: 0	Important: 0
Start	2021-05-18T12:12:55	Warnings: 2	Informative: 1	Moderate: 2
Finish	2021-05-18T12:39:52	Informative: 1		Low: 0
Runtime	1617.0 seconds			
Categories	DIAGNOSTICS,VMOSA_SCAN,VSA_SCAN			
Status	Task Completed successfully			
		vSAN Cluster Findings		
		Findings: 0		
		Errors: 0		
		Warnings: 0		
		Informative: 0		

Overall findings are sum of all plug-ins run across selected plugin types for this run

Depending on the types of plugin selected, additional cards are show with results from those set of plug-ins.

Diagnostics findings are categorized based on plugin alert Levels (Error/Warning/Informative)

VMOSA findings are categorized based on Severity levels of advisory

VSAN Cluster Findings are categorized based on plugin alert Levels (Error/Warning/Informative)

VMware Cloud Foundation Findings are categorized based on plugin alert Levels (Error/Warning/Informative)

Summary of VMware Security Advisory Scanning

In this section of the report, you find the results from VMware Security Advisory scanning

grouped by the advisory severity. To expand each severity section, click .


Under each section, all the findings are listed with the list of applicable vCenter/Hosts.



Summary of VMware Security Advisory Scanning		
<ul style="list-style-type: none"> Critical (1 findings from 1 advisories across 1 targets) VMOSA-2021-0002 VMOSA-2021-0002.a: VMware vCenter Server - VMware vCenter Server updates address remote code execution vulnerability in the vSphere Client (CVE-2021-21972) 		
Target Host	Product/Version	Desired Patch/Update (Minimum)
hostname.host.com	VMware vCenter Server Appliance 7.0.0-15952498	VMware vCenter Server/Appliance 7.0.1: Update 1c
<ul style="list-style-type: none"> Important (0 findings) Moderate (2 findings from 2 advisories across 1 targets) Low (0 findings) 		

You can click the title of each finding to navigate to the published VMware Security Advisory.

All Findings

In this section, for each of the host/log bundle analyzed, you find one row with the log bundle/host name, number of findings and Product Version details.

Summary of each Host/Log Bundle		
Host Name/Log Bundle	Findings	Product/Version
 localhost.	Info Warnings Errors	VMware ESXi 6.7.0-build-14320388

To expand and view details of the findings, click  at the start of the row. Clicking  expands all rows listed on this section. You can click the same button again to collapse the expanded section.

localhost. Info Warnings Errors VMware ESXi 6.7.0-build-14320388

Log Directory: **esx-localhost-2020-08-02--15.30-2103419**
 Hostname: **localhost**, Log Date: **2020-08-02T15:30:06**
 VMware ESXi 6.7.0-build-14320388 (ESXi 6.7 Update 3 released on 2019-08-20)

Plugins Run Number of Findings Informative Warnings Errors

VCG/vSAN HCL Validation Summary

Device	Description	VCG Status	Driver Status	Current Driver/Version	VCG Driver	Current Firmware	VCG Firmware	Forward Support
Server	HPE ProLiant DL380 Gen10	Supported	N/A	N/A	N/A	U30	HPE U30_2.22 UEFI Mode (Boot Mode:UEFI)	6.7 U3, 7.0
vmnic0	NetXtreme BCM5719 Gigabit Ethernet (network)	Supported	Supported	rtg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
vmnic1	NetXtreme BCM5719 Gigabit Ethernet (network)	Supported	Supported	rtg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
vmnic2	NetXtreme BCM5719 Gigabit Ethernet (network)	Supported	Supported	rtg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
vmnic3	NetXtreme BCM5719 Gigabit Ethernet (network)	Supported	Supported	rtg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
vmnic4	82599 10 Gigabit Dual Port Network Connection (network)	Supported	Not Latest	ixgben 1.7.15-1OEM.670.0.0.8169922	1.8.7	0x8000091d	N/A	6.7 U3, 7.0
vmnic5	82599 10 Gigabit Dual Port Network Connection (network)	Supported	Not Latest	ixgben 1.7.15-1OEM.670.0.0.8169922	1.8.7	0x8000091d	N/A	6.7 U3, 7.0
vmhba0	Lewisburg SATA AHCI Controller (sata)	Supported	Supported	vmw_ahci 1.2.8-1vmw.670.3.73.14320388	1.2.8-1vmw		N/A	6.7 U3, 7.0
vmhba1	HPE P408i-a SR Gen10 (sas)	Supported	Not Latest	smartpqi 1.0.3.2309-1OEM.670.0.0.8169922	1.0.4.3017	1.99	2.92-[0]	6.7 U3, 7.0
vmhba2	QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter (fc)	Supported	Not Latest	qinativefc 3.1.16.1-1OEM.670.0.0.8169922	3.1.31.0-1	8.08.220	8.08.xx	6.7 U3, 7.0
vmhba3	QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter (fc)	Supported	Not Latest	qinativefc 3.1.16.1-1OEM.670.0.0.8169922	3.1.31.0-1	8.08.220	8.08.xx	6.7 U3, 7.0

**Devices used for vSAN are checked against vSAN HCL. vSAN HCL check is currently limited only for the Storage IO Device
 #Firmware and BIOS versions are not validated. Please review the details for compatibility

Plugin Summary

For each of findings against the log bundles, you find a comprehensive report outlining the findings, alert level, resolution, investigation details, and log evidences if available. If any KB is to be associated with the finding, it is included in this section.

Storage.SlowStorageOperations: Possible storage bottleneck detected - slow storage operations

Fix Available In: Please review the environment

Resolution:

Some possible Symptoms:

- Tasks failing/timing-out on the host. E.g. vMotion/snapshot/maintenance-mode/vm-power-on.
- Host disconnects from vCenter as soon as you start one of the above tasks.
- ESXi Embedded Host Client is not accessible.
- esxcli commands unresponsive.

Please check for storage issues including HBA, fabric and backend storage

Evidences from Logs:

Description: Slowness for Storage operations reported by hostd.

Log File Name: var/run/log/hostd.log

```
2020-08-02T15:15:19.094Z warning hostd[2099811] [Originator@6876 sub=IoTracker] In thread 2099224,
open("/vmfs/volumes/5dcd5f45-f6e57b6a-cccc-bbbbbbbbbb/VMA_1/VMA_1.vmx") took over 11 sec.
2020-08-02T15:15:19.094Z warning hostd[2099811] [Originator@6876 sub=IoTracker] In thread 2099076,
open("/vmfs/volumes/5dcd5f45-f6e57b6a-cccc-bbbbbbbbbb/VMA_2/VMA_2") took over 11 sec.
```

The title provides a brief description of the issues identified and is colored based on the severity of the finding.

Error *NN* :- Indicates the issues detected with an error log level. These require immediate attention and user must follow the resolution details provided by the plug-in.

Warning *NN* :- Indicated the issues detected with a warning log level. Warning plug-ins provide the recommendation to avoid a probable issue that might occur in future (Ex: Multi-path configuration, Unreachable Syslog Targets).

Info *NN*:- Indicated the issues detected with an info log level. Informational plug-ins do not represent any functional issues. They just indicate helpful information from the logs (Ex: Host Configuration, BIOS details and so on)

Below the title, you see the knowledge base article number associated with this finding and the availability of the fix available.

Apart from the Title section, a plugin has one or more of following sections

- Resolution: This section provides more context about the issue identified with the resolution path. A resolution path can be in the form of a patch or an upgrade and configuration changes. If a patch or an upgrade is not available , it lists workarounds available for immediate use.
- Investigation Details: This section lists some of the information identified from the logs that provide contextual or companion data related to the identified issues.
- Evidences from Logs: This section lists the log statements used for identifying the root cause with the log filename in which they are found. This help in validating the findings.
- Back-trace: This section displays the stack trace form the ESXi host that crashed.

Interpreting VCG/vSAN HCL Validation Summary.

Diagnostics report includes detailed report related to Hardware Compatibility checks performed on the Server/IO Devices for the ESXi server for which the log bundle has been analyzed.

VCG/vSAN HCL Validation

Server and Storage/Network IO devices are validated against the **VMware Compatibility Guides**. vSAN used Storage I/O devices are validated against the **vSAN HCL**. Currently vSAN validation is limited to Storage I/O devices only. Firmware levels for Server and I/O devices are not validated but included in the report.

































VCG/vSAN HCL Validation Summary

This section has a data grid showing one row of each of the findings. Each row shows the device and validation summary.

Columns

- Device: Device name as it named on ESXi server.
- Description: Description of the device.

- VCG Status: Compatibility Status for the Device.
- Driver Status: Compatibility Status of the Driver being used.
- Current Driver/Version: Driver and the Version being used.
- VCG Driver: Most recent Driver Version as indicated by VCG.
- Current Firmware: Firmware currently being used (May not be available for all devices).
- VCG Firmware: Most recent Firmware Version as indicated by VCG.
- Forward Support: Future upgrade support (Shows current and later versions supported for this device)


VCG/vSAN HCL Validation Summary									
	Device	Description	VCG Status	Driver Status	Current Driver/Version	VCG Driver	Current Firmware	VCG Firmware	Forward Support
	Server	HPE ProLiant DL380 Gen10	 Supported	N/A	N/A	N/A	U30	HPE U30_2.22 UEFI Mode (Boot Mode:UEFI)	6.7 U3, 7.0
	vmnic0	NetXtreme BCM5719 gigabit Ethernet (network)	 Supported	 Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	146	N/A	6.7 U3, 7.0
	vmnic1	NetXtreme BCM5719 Gigabit Ethernet (network)	 Supported	 Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	146	N/A	6.7 U3, 7.0
	vmnic2	NetXtreme BCM5719 gigabit Ethernet (network)	 Supported	 Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	146	N/A	6.7 U3, 7.0
	vmnic3	NetXtreme BCM5719 gigabit Ethernet (network)	 Supported	 Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	146	N/A	6.7 U3, 7.0
	vmnic4	82599 10 Gigabit Dual Port Network Connection (network)	 Supported	 Not Latest	ixgben 1.7.15-10EM.670.0.0.8169922	1.8.7	0x8000091d	N/A	6.7 U3, 7.0
	vmnic5	82599 10 Gigabit Dual Port Network Connection (network)	 Supported	 Not Latest	ixgben 1.7.15-10EM.670.0.0.8169922	1.8.7	0x8000091d	N/A	6.7 U3, 7.0
	vmhba0	Lewisburg SATA AHCI Controller (sata)	 Supported	 Supported	vmw_ahci 12.8-1vmw.670.3.73.14320388	12.8-1vmw		N/A	6.7 U3, 7.0
	vmhba1	HPE P408i-a SR Gen10 (sas)	 Supported	 Not Latest	smartpqi 1.0.3.2309-10EM.670.0.0.8169922	1.0.4.3017	199	2.92-[0]	6.7 U3, 7.0
	vmhba2	QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter (fc)	 Supported	 Not Latest	qlnativefc 3.116.1-10EM.670.0.0.8169922	3.131.0-1	8.08.220	8.08.xx	6.7 U3, 7.0
	vmhba3	QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter (fc)	 Supported	 Not Latest	qlnativefc 3.116.1-10EM.670.0.0.8169922	3.131.0-1	8.08.220	8.08.xx	6.7 U3, 7.0

Status Indicators

ⓘ Not Checked	Device was not checked for compatibility as VCG Database is not updated
⚠ Not Listed	This device was not found on the compatibility guide
✓ Supported	Device is supported for the current version of ESXi running
❗ Not Supported	Device is NOT supported for the current version of ESXi running
⚠ Not Latest	Driver currently being used is not the latest one compared to the one listed on VCG
❗ Not Minimum	Driver currently being used is does not meet the minimum version listed on VCG

VCG Details

Each row in the VCG/vSAN HCL report can be expanded to view further details from the

compatibility guide. Click  to expand the row and view the details. Clicking the same collapses, the details section.

vmnic0

NetXtreme BCM5719 Gigabit Ethernet (network)

Supported

Supported

ntg3 4.1.3.2-1vmw.670.1.28.10302608

4.1.3.2-1vmw

1.46

N/A

6.7 U3, 7.0

Description	NetXtreme BCM5719 Gigabit Ethernet (14e4:1657 103c:22be)				
VCG/HCL Model	HP Ethernet 1Gb 4-port 331i Adapter				
Driver/Firmware	ntg3 - 4.1.3.2-1vmw.670.1.28.10302608, 1.46				
Devices	vmnic0(Down), vmnic1(Up), vmnic2(Down), vmnic3(Up)				
VCG Entry	https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=io&productid=37751				
VCG Status	Found 1 entries for VMware ESXi 6.7.0 Update 3. <div><div></div>[OK]Current Driver ntg3-4.1.3.2-1vmw.670.1.28.10302608 is part of supported list.</div>				
	Release	Driver	Version	Firmware	Features
	ESXi 6.7 U3	ntg3	4.1.3.2-1vmw	N/A	IPv6
VCG Support	ESXi 7.0, ESXi 6.7 U3, ESXi 6.7 U2, ESXi 6.7 U1, ESXi 6.7, ESXi 6.5 U3, ESXi 6.5 U2, ESXi 6.5 U1, ESXi 6.5, ESXi 6.0 U3, ESXi 6.0 U2, ESXi 6.0 U1, ESXi 6.0, ESXi 5.5 U3, ESXi 5.5 U2, ESXi 5.5 U1, ESXi 5.5				
VCG Notes	Firmware versions listed are the minimum supported versions. Refer to http://kb.vmware.com/kb/2030818 for additional information on other supported driver and firmware combinations				
VCG DB Status	IO Device:2020-08-02T05:03:20 CPU Series:2020-08-02T05:04:54 Server:2020-08-02T05:02:23 vSAN HCL:2020-03-01T08:03:00 Last Updated: 2020-08-02T21:32:09				

Interpreting VMware Cloud Foundation Diagnostics Report

A diagnostics report includes detailed information related to VMware Cloud Foundation Health checks performed on the Management and workload domains.

VMware Cloud Foundation Health Diagnostics

The VMware Cloud Foundation Health Check diagnostics report displays information for all the following products that includes

- vCenter Server
- ESXi
- VMware NSX
- VMware Cloud Foundation SDDC Manager
- VxRail Manager
- VMware vRealize Automation
- vRealize Operations
- vRealize Log Insight
- vRealize Life Cycle Manager

The health summary includes, following categories,

- 1 Services Health
- 2 NTP Health
- 3 General Health
- 4 Certificate Health
- 5 Password Health
- 6 Connectivity Health
- 7 Compute Health

- 8 Storage Health
- 9 DNS Health
- 10 Composability Health
- 11 Hardware Compatibility Health
- 12 Hosts IPs
- 13 Inventory Info

VMware Cloud Foundation Health Summary

The **Summary** section provides following details

- plug-ins Run
- Number of findings
- Errors
- Warnings
- Informative

The **Analysis Result** section provides summary base on the criticality of the health issue. Health issues are categorized into

- Error
- Warning
- Info

Figure 3-4. VMware Cloud Foundation Health Summary



VMware Cloud Foundation Health Details

This section has a data grid showing one row of each of the findings. Each row shows the Issues and cause summary with host details.

The **Health Checker** includes following categories,

- 1 Services Health

- 2 NTP Health
- 3 General Health
- 4 Certificate Health
- 5 Password Health
- 6 Connectivity Health
- 7 Compute Health
- 8 Storage Health
- 9 DNS Health
- 10 Composability Health
- 11 Hardware Compatibility Health
- 12 Hosts IPs
- 13 Inventory Info

Columns

- Hostname: The name / IP of the host.
- Area: The type of the host, e.g. ESXi, vCenter, etc..
- Status: Health status (Red, Yellow, Green of the host).
- Reason: The reason for the status.
- Analysis Status: The time of the analysis done.

Figure 3-5. Report Details

All Findings

Host Name/Log Bundle	Product/Version
hostname,company.com 0 1 0	VMware Cloud Foundation 4.2.0.0-build-17559673

Log Directory: **healthcheck-2021-05-22-03-02-46-2404**
 Hostname: hostname,company.com
 VMware Cloud Foundation 4.2.0.0-build-17559673(VMware Cloud Foundation 4.2 released on 2021-02-09)

Plugins Run 24 Number of Findings 1 Errors 0 Warnings 1 Informative 0

Analysis Results

Y Plugin Category:VMware_Cloud_Foundation_Health
 ➤ Warn (1)

Figure 3-6. Categorywise health details

VMware_Cloud_Foundation_Health.HealthCheck.NTPHealthChecker: Issues observed in the NTP configurations validations.

Investigation Details:

Following NTP are reported as incorrectly configured:

Hostname	Area	Status	Reason	Analysis Time
st-114-244.eng.vmware.com	ESXi	YELLOW	ESXi NTP is NOT configured as expected. Actual NTP: ['time1.vmware.com'], Valid NTP: ['ntp3-sjc05.vmware.com', 'time2.oc.vmware.com', '10.166.1.120']	Sat May 22 03:1
st-114-241.eng.vmware.com	ESXi	YELLOW	ESXi NTP is NOT configured as expected. Actual NTP: ['time1.vmware.com'], Valid NTP: ['ntp3-sjc05.vmware.com', 'time2.oc.vmware.com', '10.166.1.120']	Sat May 22 03:1
st-114-243.eng.vmware.com	ESXi	YELLOW	ESXi NTP is NOT configured as expected. Actual NTP: ['time1.vmware.com'], Valid NTP: ['ntp3-sjc05.vmware.com', 'time2.oc.vmware.com', '10.166.1.120']	Sat May 22 03:1
st-114-242.eng.vmware.com	ESXi	YELLOW	ESXi NTP is NOT configured as expected. Actual NTP: ['time1.vmware.com'], Valid NTP: ['ntp3-sjc05.vmware.com', 'time2.oc.vmware.com', '10.166.1.120']	Sat May 22 03:1
st-114-245.eng.vmware.com	vCenter	YELLOW	VC NTP is not configured as expected. Configured: ['time1.vmware.com', 'time1.vmware.com'], Expected: ['ntp3-sjc05.vmware.com', 'time2.oc.vmware.com', '10.166.1.120']	Sat May 22 03:1

Interpreting VMware vSAN Storage Report

A diagnostics report includes detailed information related to VMware vSAN Storage Health checks performed on the vSAN enabled clusters in vCenter Server.

VMware vSAN Storage Health Diagnostics

The VMware vSAN Storage Health Check diagnostics report displays information for all the vSAN enabled clusters selected.

VMware vSAN Storage Health Summary

The **Summary** section provides following details

- plug-ins Run
- Number of findings
- Errors
- Warnings
- Informative

The **Analysis Result** section provides summary base on the criticality of the health issue. Health issues are categorized into

- Error
- Warning
- Info

All Findings

Host Name/Log Bundle	Product/Version
hostname.company.com -vSAN-Test-Infra	VMware vCenter Server 7.0.0-build-15952599

Log Directory: **domain-c8-Test-Infra**
 Hostname: hostname.company.com -vSAN-Test-Infra Log Date: 2021-07-19T08:37:22
 VMware vCenter Server 7.0.0-build-15952599(vCenter Server 7.0 GA released on 2020-04-02)
 Analysis Status: Completed Run Plugins

Plugins Run (63) Number of Findings (6) Errors (1) Warnings (3) Informative (1)

Analysis Results

Y Plugin Category:VSAN_SCAN

- Error (1)
- Warn (3)
- Info (1)

VMware vSAN Storage Health Details

This section has a data grid showing one row of each of the findings. Each row shows the Issues and cause summary with host details.

The **Health Checker** includes vSAN Health category. It provides following details,

- 1 Issue Summary : The issue detected by vSAN Health Check plug-in
- 2 Description : Provides description of the issue.
- 3 KB : The VMware Knowledge Base article id that can describe the issue in details, and provide resolution or workaround if available.
- 4 Resolution : KB link for the issue identified.
- 5 Investigation details : Provides investigation details for the analysis done and impacted hosts.

Analysis Results

Y Plugin Category: VSAN_SCAN

Y Error (1)

VSAN_SCAN.VSAN_HEALTH.KB2150916: vCenter state is authoritative check
 Checks if vCenter Server state is pushed to ESXi, and the host membership is not out of sync.
 KB Number: [2150916](#)

Resolution:
 Please read KB: <https://kb.vmware.com/s/article/2150916> for more details/resolution.

Investigation Details:
 Test Name: vCenter state is authoritative: Hosts that are out of sync

Host	Last Update by VC	Last Update Time	Recommendation
hostname.company.com	Different VC (0c92021b-4a65-4109-be37-9c6dec5560b8)	2020-01-31 10:27:55 UTC	If vCenter Server was replaced/recovered from backup, and current host list in vCenter Server is correct, th
hostname.company.com	Different VC (0c92021b-4a65-4109-be37-9c6dec5560b8)	2020-01-31 10:27:55 UTC	If vCenter Server was replaced/recovered from backup, and current host list in vCenter Server is correct, th
hostname.company.com	Different VC (0c92021b-4a65-4109-be37-9c6dec5560b8)	2020-01-31 10:27:55 UTC	If vCenter Server was replaced/recovered from backup, and current host list in vCenter Server is correct, th

> Warn (3)

> Info (1)

Adding and Removing Tags for the Analysis Report

You can add or remove the tag for the report for quick reference and search, post completion of the analysis run.

As an operator you might want to quickly search the report base on some tags.





Prerequisites

Verify that you have a valid user account credential with VMware Skyline Health Diagnostics.

Procedure

- 1 Log in the VMware Skyline Health Diagnostics UI using the supported browser.
- 2 Click **Show Reports** on the top navigation menu.

3 The left menu showing following four filters,

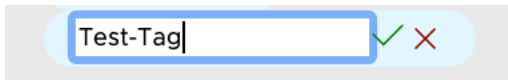
- a **Diagnostics Report**  : Lists the reports that have diagnostics plug-ins selected at the time of analysis.
- b **Security Reports**  : Lists the reports that have security plug-ins selected at the time of analysis.
- c **vSAN Reports**  : Lists the reports that have vSAN plug-ins selected at the time of analysis.
- d **VMware Cloud Foundation Reports**  : Lists the reports that have VMware Cloud Foundation plug-ins selected at the time of analysis.

4 Select any one of the above , you are interested in.

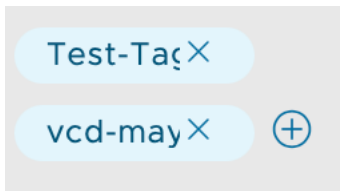
5 Select a log bundle using the filter against the **Bundle Name** , **Analysis Type** , **Tags**, **User Name** or **Start Time**. You can use the **Tags** to search quickly the issues base on the keyword that you provided while starting the analysis.

6 Click  in the Tags column for the selected report.

7 Input the name of the tag and click **OK** button.



8 The newly added tag name appears under the Tags Columnn



9 To remove the tag click on the delete icon, .

Results

The tag will be delete for the analysis report.

Help and Support

You can get help on problems related to the install or operation.

You can download the support bundle for VMware Skyline Health Diagnostics , you may want to share with the VMware support.

Prerequisites

Verify that you have an operator user account to access the UI of VMware Skyline Health Diagnostics.

Procedure

- 1 You can collect the log bundle from VMware Skyline Health Diagnostics UI by following steps :
 - a Log in to VMware Skyline Health Diagnostics UI, navigate to **SettingsHelp and Support**
 - b Click **Collect SHD Bundle**
- 2 Or in the absence of UI, from Photon VM console
 - a SSH to the Photon VM with **root** user credentials and run `shd-support`
 - b Download the log bundle **vmware-shd-support-YYYY-MM-DDThh_mm_ss.tgz** from **/opt/vmware-shd/vmware-shd/log**
- 3 For any install issue, take the screenshot and collect the details from console.
- 4 Send an email to **shd-support@vmware.com** with issue details, screenshots along with log bundle attached.

Results

VMware starts looking into issue and will reach out to you.

View the CEIP Data Collected for Reporting and Analytics

The VI-Admins or the security teams in your organization might be interested to know the data getting collected by VMware Skyline Health Diagnostics as part of CEIP. The **TOOL USAGE REPORT** provides insight into the data collected.

Prerequisites

- Verify that you have an operator user account to access the HTML5 user interface of **VMware Skyline Health Diagnostics**.
- Verify that you can open the HTML5 user interface of **VMware Skyline Health Diagnostics** in the browser window.

Procedure

- 1 Log in to VMware Skyline Health Diagnostics UI, Click **Settings > Help and Support > Tool Usage Report**
- 2 Click **Tool Usage Report** .
- 3 The download of the report starts.

- 4 Once download complete, open the report to see the data collected by **VMware Skyline Heath Diagnostics**, that you will be sharing with VMware.

Results

The report having the details about the data collected by **VMware Skyline Heath Diagnostics** .

Updating VMware Skyline Health Diagnostics

4

It is highly recommended to keep the VMware Skyline Health Diagnostics updated as new patches or updates as they are released. Patches and Updates bring in new signatures (increased analytic capabilities) and new features/product coverage.

This chapter includes the following topics:

- [Update or Upgrade VMware Skyline Health Diagnostics Using Online Mode](#)
- [Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful](#)
- [Update or Upgrade the VMware Skyline Health Diagnostics Offline.](#)
- [Revert to Last Working Set-Up If Update or Upgrade Operation Fails.](#)

Update or Upgrade VMware Skyline Health Diagnostics Using Online Mode

if VMware Skyline Health Diagnostics connected to Internet, you can update or upgrade to the latest version with simple steps and ease.

Prerequisites

- Verify that you have an **shd-admin** user account to access the HTML5 user interface of **VMware Skyline Health Diagnostics**.
- Verify that you can open the HTML5 user interface of **VMware Skyline Health Diagnostics** in the browser window.
- Verify that **VMware Skyline Health Diagnostics** is connected to Internet.
- Verify that you have the **Virtual machine.Snapshot management.Create** snapshot **privilege** on the virtual machine.
- Verify that you have **Virtual machine.Snapshot management.Remove** Snapshot privilege on the virtual machine.

Procedure

- 1 Log in to vCenter HTML5 Client.

- 2 Take the snapshot of the Appliance/VM running **VMware Skyline Health Diagnostics**. Refer [Take Snapshot of Virtual Machine](#) for more information.
- 3 Log in to VMware Skyline Health Diagnostics UI as **shd-admin**.
- 4 Click the **Settings** tab in the top menu.
- 5 Click the **Upgrade & History** in the left pane.
- 6 Click the **Tool Update** tab.
- 7 To check whether new updates are available, click the **CHECK TOOL UPDATES**. If new updates are available, a download option is enabled.
- 8 To download the update, click the **DOWNLOAD UPDATES** (This option is available only for the **shd-admin** user)
- 9 Confirm that the version is visible in **Download History Summary**.
- 10 After the confirmation, restart the VMware Skyline Health Diagnostics appliance.

Results

VMware Skyline Health Diagnostics updated or upgraded to the latest version.

What to do next

- 1 Verify that the operation is successful using the steps mentioned in [Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful](#)

Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful

You can verify the VMware Skyline Health Diagnostics update/upgrade is successful with few simple checks.

Prerequisites

- Verify that you have an **shd-admin** user account to access the HTML5 user interface of VMware Skyline Health Diagnostics.
- Verify that you can open the HTML5 user interface of VMware Skyline Health Diagnostics in the browser window.
- Verify that VMware Skyline Health Diagnostics is connected to Internet.

Procedure

- 1 On-Successful upgrade, log in to VMware Skyline Health Diagnostics HTML5 user interface as **shd-admin**.
- 2 Click **Settings** -> **About** tab and take the note of version information. It should display the version you downloaded to upgrade to.

- 3 Click **Tool Update** and navigate to section **Download History Summary & Upgrade History Summary** . You can ensure these sections are displaying latest version you downloaded. If the version information is consistent , it means that the update or upgrade is successful.
- 4 If **Upgrade version Summary** or **About** section information is not updated with latest downloaded or intended version, it means that the update or upgrade operation has failed. Please collect the log bundle and send email to **shd-support@vmware.com**.
- 5 If the update or upgrade is successful, Delete the snapshot of the VM if the above validation is successful.
- 6 If the update or upgrade fails, revert to the snapshot taken before the upgrade and then delete the snapshot.

Results

You have successfully verified the update or upgrade of VMware Skyline Health Diagnostics.

Update or Upgrade the VMware Skyline Health Diagnostics Offline.

Due to the security policies in your organization, you may not want VMware Skyline Health Diagnostics to have the Internet connectivity. You can still install the new patches/updates for VMware Skyline Health Diagnostics following the offline method.

Prerequisites

- Verify that you have an **shd-admin** user account to access the HTML5 user interface of **VMware Skyline Health Diagnostics**.
- Verify that you have valid user credentials and privileges to vSphere infrastructure where you want to update or upgrade the VMware Skyline Health Diagnostics.

Required privileges:

- **Datastore.Browse datastore** on the datastore.
- **Datastore.Low level file operations** on the datastore.
- **Virtual machine.Snapshot management.Create** snapshot **privilege** on the virtual machine.
- **Virtual machine.Snapshot management.Remove** Snapshot privilege on the virtual machine.
- Verify that you can access vSphere Infrastructure with privileges required for managing the virtual machine settings and interacting with virtual machine using console.
- Verify that you can open the HTML5 user interface of **VMware Skyline Health Diagnostics** in the browser window.

- Verify that you have downloaded the **VMware Skyline Health Diagnostics** latest version ISO , see [Downloading VMware Skyline Health Diagnostics ISO Image for Offline Updates](#)

Procedure

- 1 Log in to the vCenter HTML5 client.
- 2 Identify the VM/Appliance running **VMware Skyline Health Diagnostics** and power off the VM.
- 3 Take the snapshot of the VM using VMware vSphere client having **VMware Skyline Health Diagnostics** installed. See [Take Snapshot of Virtual Machine](#) for further help.
- 4 In the vCenter HTML5 Client, select the Storage tab in the left pane of vSphere Client.
- 5 Select the datastore to which you upload the files from the datastore inventory.
- 6 (Optional) On the Files tab, click the New Folder icon to create a folder.
- 7 Select a folder and click the Upload Files icon.
- 8 Browse to the downloaded VMware Skyline Health Diagnostics ISO image, select it, and click **Open** . The ISO upload time vary, depending on file size and network upload speed.
- 9 Refresh the datastore file browser and verify that the uploaded files are present.
- 10 In vSphere Client, right-click the VMware SHD Appliance/VM, select Edit Settings.
- 11 Click the arrow next to the CD/DVD drive 1 device to expand the section. Click Browse to select the uploaded VMware Skyline Health Diagnostics ISO Image file.
- 12 If the Connect at Power On check box is not selected, click to select it. Then click OK to close the Edit Settings window.
- 13 Power on the virtual machine and open VMware Skyline Health Diagnostics Appliance/VM console using vCenter Server user interface or SSH
- 14 Login as the **root** user.
- 15 To mount the attached ISO, run `mount /dev/cdrom /mnt/cdrom`.
- 16 To start the upgrade process by executing install script, run `sh /mnt/cdrom/install.sh`.
- 17 After the installation process competes, you can log out from the shell and verify the installation by logging into HTML5 UI

Results

The VMware Skyline Health Diagnostics updated or upgraded to the version as specified by the ISO Image

Revert to Last Working Set-Up If Update or Upgrade Operation Fails.

If an update or upgrade of the **VMware Skyline Health Diagnostics** fails, you might want to restore your environment to the previous working state.

Prerequisites

- Verify that you have an **shd-admin** user account to access the HTML5 user interface of **VMware Skyline Health Diagnostics**.
- Verify that you have valid user credentials and privileges to vSphere infrastructure where the update or upgrade of the VMware Skyline Health Diagnostics failed.
- Required privileges:
 - **Virtual machine.Snapshot management.Revert** snapshot **privilege** on the virtual machine.
 - **Virtual machine.Snapshot management.Remove** snapshot **privilege** on the virtual machine.
 - for managing the virtual machine settings and interacting with virtual machine using console.
- Verify that you have credential for the **root** user, set at the time of the install.

Procedure

- 1 SSH to the **VMware Skyline Health Diagnostics** Appliance/VM and log in with **root** user credentials.
- 2 To collect the log bundle run the command **shd-support** on the shell. This command collects the log bundle.
- 3 Download the log bundle to your system using **winSCP** or **SCP**.
- 4 Log out from the VM console.
- 5 Log in to vCenter and select the VM VMware Skyline Health Diagnostics.
- 6 To revert a snapshot, select the Appliance/VM running VMware Skyline Health Diagnostics and click the **Snapshots** tab. See [Revert a Virtual Machine Snapshot](#) for details.
- 7 Navigate to a snapshot taken before the upgrade in the snapshot tree, click **Revert**, and click the **Revert** button.
- 8 Delete the snapshot taken before the upgrade. See [Delete a Snapshot](#) for further details.
- 9 Power on the VM.
- 10 Write to **shd-support@vmware.com** with issue details along with the log bundle attached.

Results

The **VMware Skyline Health Diagnostics** instance is reverted to earlier working version.

Scale Limits for VMware Skyline Health Diagnostics

5

This section defines the scale and max configurable limits supported by VMware Skyline Health Diagnostics to function effectively.

This chapter includes the following topics:

- [Scale Limits](#)

Scale Limits

This section provides the maximum limits for analyze operation in Skyline Health Diagnostics.

Maximum Limits for Analyze Operation

- 1 The maximum number of ESXi hosts allowed to select during the analyze operations are sixty-four (64). You can select vCenter along with ESXi host limit.
- 2 The maximum number of parallel analysis runs allowed are four, across Skyline Health Diagnostics. This means if five (5) users want to run the analysis in parallel, only four will be executed and other analyze operations will error out. Once one of the analyze operations are completed, the user can start the new analysis operation.
- 3 You can submit four (4) parallel analyze operations with maximum sixty-four (64) ESXi hosts in each request.

Maximum Limits for all the Activities

Maxium Upgrade Summary	Last five upgrade activities will be displayed.
Download History Summary	Last five download activities will be displayed.
View Analysis Report	UI provides access to fifty most recent reports.
Maximum Tasks displayed	Recent Task View displays ten most recent tasks.

**Maximum number of host
allowed to select in a
analyze operation**

You can select maximum sixty-four ESXi hosts for and one vCenter Server in a analyze operation run.

**Maximum number of
parallel runs across SHD**

The maximum number of parallel analysis run allowed are four across the Skyline Health Diagnostics.

Interaction of Skyline Health Diagnostics with Services

6

VMware Skyline Health Diagnostics provides user interface over the network. Also, if internet connectivity is available can perform online update/upgrade and VCG database updates. It also communicates to VMware CEIP Data collection if CEIP is opted.

This chapter includes the following topics:

- [Inbound Interaction](#)
- [Outbound Interaction](#)

Inbound Interaction

The VMware Skyline Health Diagnostics client can interact with VMware Skyline Health Diagnostics Server on the secure port, using the secure protocol.

VMware Skyline Health Diagnostics allows following protocols and ports for inbound connections.

- 1 The VMware Skyline Health Diagnostics HTML5 user interface is accessible on port 443 over https.
- 2 You can connect to the VMware Skyline Health Diagnostics Appliance console over the SSH protocol on the port 22.

Outbound Interaction

The VMware Skyline Health Diagnostics Server interacts with VMware Services hosted in the VMware environment, outside of the Customer on-premise infrastructure to download updates, and signatures, and share the CEIP data. The VMware Skyline Health Diagnostics Server also interacts with vCenter Server and ESXi hosts in the on-premise environment to collect logs, and product version, and build number to perform its tasks.

VMware Skyline Health Diagnostics makes following outbound Interaction to receive or send the data to successfully perform its tasks.

Purpose	Destination URL	Protocol	Destination Port
Download the new patches and updates.	https://shd-download.vmware.com	HTTPS	443
Download the VMware Compatibility Guide updates	https://vmware.com	HTTPS	443

Purpose	Destination URL	Protocol	Destination Port
vSAN Hardware Compatibility	http://partnerweb.vmware.com	HTTP/HTTPS	80/443
Customer Experience Improvement Program	https://vcsa.vmware.com	HTTPS	443