control up

ControlUp Analyzer User Guide

September 2019

Contents

1 Installation and Setup

1.1 System Requirements

The following section details the capacity and configuration requirements for deployment of the pre-packaged ControlUp Analyzer appliance:

- VMware vSphere infrastructure should already be deployed. ESX/ESXi hosts must be v5.x and above, and these must be managed by vCenter v5.x or v6.x.
- NSX-V is supported by connecting to an NSX Manager when paired with a vCenter instance. ControlUp Analyzer supports NSX Manager v6.2 and above.
- VMware Horizon is supported by connecting to a Connection Server. For Connection Servers that are part of a single replication group, it is required to establish the connection to only one Connection Server which belong to the group. Also, if there is a Load Balancer configured with **session persistence**, it can be used to connect to a Connection Server in a replication group. ControlUp Analyzer supports Horizon v6.x and above.
- HW Compatibility checks are performed on ESXi v6.0 and above.
- The ControlUp Analyzer appliance is normally deployed into an existing vSphere infrastructure. Appropriate resource allocation for the appliance is selected during the deployment process. The standard sizing options are small/medium/large with resources allocated as follows:
  - Small (use this configuration for small environments: up to 25 Hosts)
    - 2 vCPU
    - 4 GB RAM
    - 120GB Storage
    - 100Mbit network (1GBit or above recommended)
  - Medium (use this configuration for medium deployments: up to 150 Hosts)
    - 4 vCPU
    - 8 GB RAM
    - 120GB Storage
    - 100Mbit network (1GBit or above recommended)
  - Large (use this configuration for large deployments: up to 400 Hosts)
    - 8 vCPU
    - 32 GB RAM
    - 120GB Storage
    - 100Mbit network (1GBit or above recommended)

- A user with the following privilege **at vCenter level** is needed:

  Minimum required:
  - Read Only

[Note] The minimum required permission for the Analyzer to perform scanning is **Read Only.** However, in this case collection will not be fully comprehensive and it will not be possible to report issues related to some areas of the configuration (such as device-specific info from ESXi hosts (driver, firmware)).

In order to provide a fully comprehensive analysis, the additional privileges provided below will ensure that sufficient information is collected for 100% of the checks performed by ControlUp Analyzer:

Required for CIM collection:

- Host > CIM > CIM interaction

Required for VSAN configuration collection:

- Global > Settings

Required for files collection:

- Host > Configuration > Firmware

Required for Kernel modules collection:

- Host > Configuration > Change settings

Required for auto ESXi syslog configuration:

- Host > Configuration > Advanced settings
- Host > Configuration > Change settings
- Host > Configuration > Security profile and firewall

Required for auto VM syslog configuration:

- Virtual Machine > Configuration > Advanced

Required for auto Web Client registration:

- Extension > Register extension
- Extension > Update extension

Required for HW Compatibility:

- Host > Configuration > Change settings
- Global > Settings

➢ For connection to NSX-V a user with the following privileges in NSX Manager is needed:

Minimum requirement:

- Auditor

Recommended:

- Security administrator – required to leverage the NSX Custom Dashboard Widget for ControlUp.

[**Note**] Due to constraints in NSX Manager prior to v6.3.3 ControlUp Analyzer is unable to automatically validate that an NSX Manager is registered to a specific vCenter. You'll be asked to provide confirmation during the connection process.

Authentication source:

- **Local** - local CLI user can be created following the below procedure:

  1. Open console session to NSX Manager and log in with the Administrator account
  2. Switch to Privilege mode using the *"enable"* command
  3. Switch to Configuration mode using the *"configure terminal"* command
  4. Add a CLI user account using the *"user <username> password (hash | plaintext) <password>"* command

     Example: *user cliuser password plaintext abcd1234*

  5. Save the configuration with *"write memory"* command
  6. Allow the created CLI user to run the REST API calls using the "*user <username> privilege web-interface"* command
  7. Issue POST request to *"https://<NSX-IP>/api/2.0/services/usermgmt/role/<username>?isCli=true"* endpoint with user having administrator privileges to assign a role to the newly created CLI user. Example of the body content assigning *"auditor"* privilege:

```
<accessControlEntry>
    <role>auditor</role>
    <resource>
        <resourceId>globalroot-0</resourceId>
    </resource>
</accessControlEntry>
```

  8. Now you'll be able to use the new CLI user for connection to NSX Manager

- **Domain** - domain users are supported on NSX-v 6.4 and later

➢ For connection to a Connection Server a user with the following privileges in Horizon is needed:

Recommended:

- Administrators (Read only).

➢ Required ports:

Source	Destination	Protocol	Port	Description	Comment
RCA	vCenter	TCP	443	Collection of data using vSphere SDK (vCenter, ESXi, VMs configuration settings)	required for core product functionality
RCA	ESXi	TCP	443	Collection of data from ESXi servers (file-level configuration settings)	needed for file-level checks
RCA	ESXi	TCP	5988, 5989	CIM data collection from ESXi servers	needed for CIM data (will be replaced by

					beginning of 2019-Q1)
RCA	NSX Manager	TCP	443	Collection of data using NSX-v REST API (NSX configuration settings)	required for core product functionality (in case NSX-v functionality is required)
RCA	Horizon	TCP	443	Collection of data using Horizon API (Horizon configuration settings)	required for core product functionality (in case Horizon functionality is required)
ESXi	RCA	UDP	514	Syslog data collection	needed for log analysis
RCA	updates.runecast.com	TCP	443	Application and rules definition updates	needed for online updates only
User browser	RCA	TCP	80, 443, 31415	RCA web interface	HTTP always redirects to HTTPS
vSphere Web Client	RCA	TCP	443	Web client plugin communication to RCA	needed for displaying results in WebClient
REST API client	RCA	TCP	443	ControlUp Analyzer API clients communication	needed for REST API
SPOG	RCA	TCP	443	Single pane of Glass to RCA communication	needed for displaying results from multiple analyzers
User browser	SPOG	TCP	443	Single pane of glass web interface	user access to SPOG
RCA	LDAP	TCP	389	RCA communication to AD	needed for connection to a DC on a regular LDAP port
RCA	LDAP SSL	TCP	636	RCA communication to AD	needed for connection to a DC on a protected LDAPS port
RCA	DNS	TCP	53	RCA communication to DNS	required for core product functionality

- Internet Connectivity:
  ControlUp Analyzer is packaged as a virtual appliance in OVA format that is deployed into your

virtual infrastructure. All data and logic necessary for full operation is contained in the appliance. No data is transmitted from the ControlUp Analyzer outside of your data center. Optionally, the ControlUp Analyzer can be connected to the Internet to download zero-touch updates for knowledge definitions and application updates. A fully off-line update mechanism is provided using files (.ISO and .bin). You can download the offline update iso file here: https://updates.runecast.com/runecast-analyzer-vmware/rcupdate.iso. You can download the knowledge definitions update here: https://updates.runecast.com/definitions/kbupdates.bin.

- Supported browsers to access the ControlUp Analyzer Web Interface: Chrome v68.0.3440.106 and newer, Firefox v50.0.2 and newer, MS Edge v38.14393.0.0 and newer.

1.2 Deployment

1. Download the ControlUp Analyzer OVA file and deploy from your download location. You can download the file from https://updates.runecast.com/RunecastAnalyzer/ControlUpAnalyzer.ova
2. **Accept** the license agreement.
3. Select the **VM name and folder**, select the destination **host**, **datastore** and **network** on your environment.
4. In **Customize template**, configure the **network configuration** for the ControlUp Analyzer appliance.
5. Review the settings and click **Finish**.
6. Power on the appliance. After the boot process has finished, you should see the appliance console displaying the URL to the application and how to access the **ControlUp Console Interface**.
7. If you need to change the settings of the appliance itself (network configuration, update settings), you can login to the **Console Interface** of the ControlUp Analyzer appliance (**default user**: rcadmin / **password**: admin)

1.3 Initial Configuration

This section describes the initial configuration steps for the ControlUp Analyzer appliance including connections to the vSphere environment and NSX Manager (if available) or Horizon Connection Server. It includes adding settings for vCenter, NSX Manager, Horizon Connection Server, Web Client Plug-in, licensing, log forwarding, and performing an initial analysis.

1.3.1 Connect to a System and Analyze

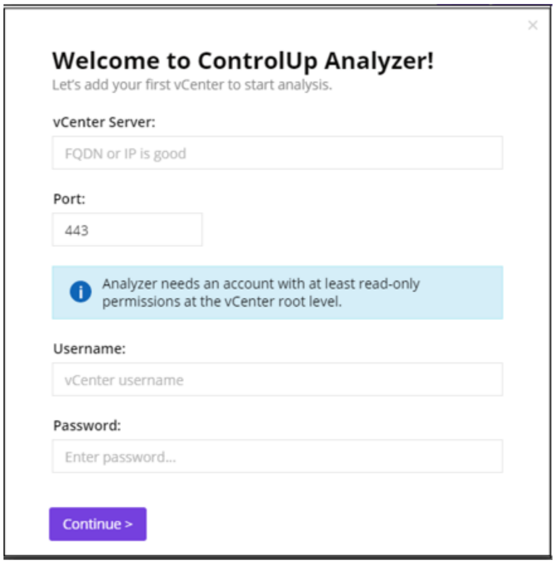
1. From a browser, navigate to the ControlUp Analyzer Web Interface url: https://*applianceIP* and login with default credentials:

   user: rcuser

   password: ControlUp!

2. During the first login no vCenter connections will exist so you will be prompted to configure a

connection to your vCenter server. Enter the vCenter connection info (see **System requirements** section above for required privileges) and **Continue** to the next step.



Welcome to ControlUp Analyzer!

Let's add your first vCenter to start analysis.

vCenter Server: FQDN or IP is good

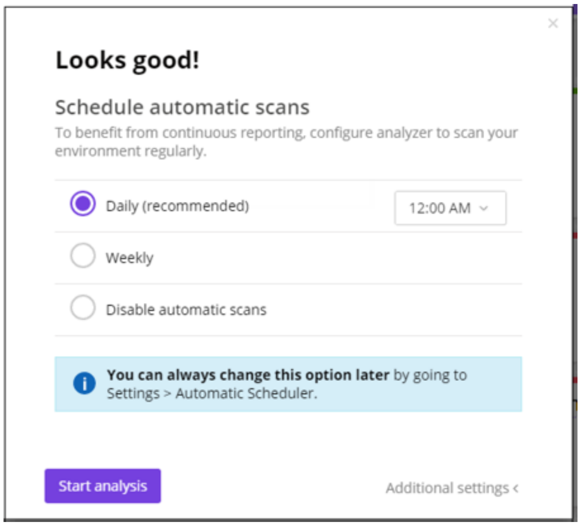
Port: 443

Analyzer needs an account with at least read-only permissions at the vCenter root level.

Username: vCenter username

Password: Enter password...

3. Confirmation of successful connection is displayed. You now have the option to configure automatically scheduled scans. We encourage you to schedule them to benefit from continuous reporting. From this screen you are able to trigger the first analysis using the **Start analysis** button.



Looks good!

Schedule automatic scans

To benefit from continuous reporting, configure analyzer to scan your environment regularly.

● Daily (recommended) 12:00 AM

○ Weekly

○ Disable automatic scans

You can always change this option later by going to Settings > Automatic Scheduler.

4. Optionally, you can help to improve ControlUp Analyzer by sending limited anonymous usage data.

   The telemetry data contains the following information:

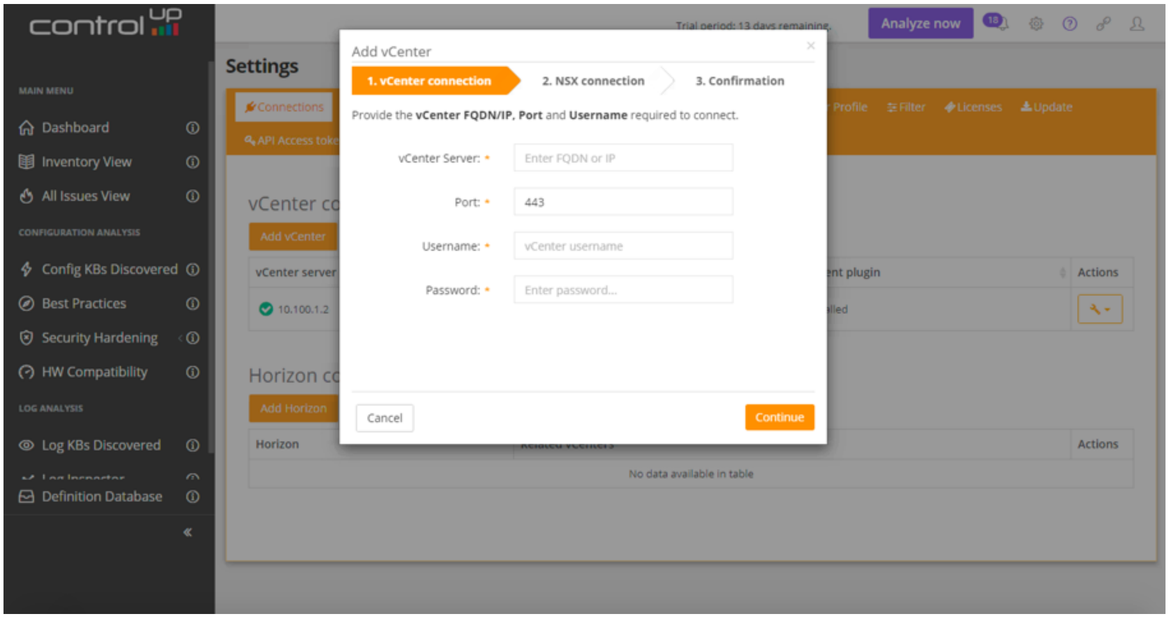
   - Version of ControlUp Analyzer.

- Number of Systems (NOT their IP or name).
- Issues discovered and their severity (NOT the objects affected).
- % of best practice adoption and security compliance (NOT the objects affected).
- Preferences in settings like activation of DISA STIG, PCI DSS, HIPAA, Automatic Scheduler and the total number of CPUs (NOT the objects affected).
- User actions like display dashboard, display settings, add System, remove System and start the analysis (NOT the objects affected).
- Hardware details like manufacturer, description, disks, bios/firmware/driver versions (NOT their IP or hostname).
- Browser used and version.

[Note] You always have the option to change your preference from the **User profile** tab under **Settings**. Once a license has been applied, the data collection will turn off automatically. If you would like to continue sending information to improve ControlUp Analyzer, you can turn it on from **User profile** under **Settings**.

5. To connect additional vCenter servers navigate to **Settings** and select **Connections** tab. Click **Add vCenter** button and follow these steps:

   - Enter the vCenter connection information and click **Continue** to the next step.



Add vCenter

1. vCenter connection | 2. NSX connection | 3. Confirmation

Provide the **vCenter FQDN/IP, Port** and **Username** required to connect.

vCenter Server: * Enter FQDN or IP

Port: * 443

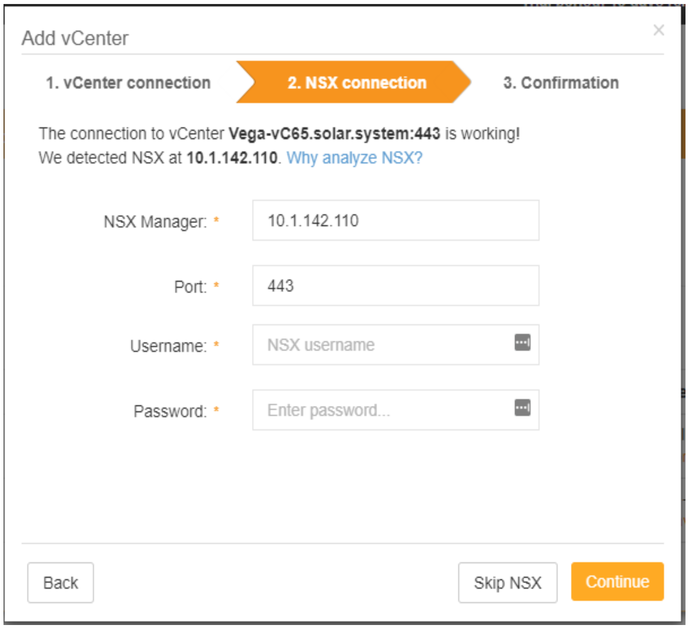
Username: * vCenter username

Password: * Enter password...

   - Validate the successful connection to vCenter. During validation an attempt to automatically detect NSX will be in process. If no NSX Manager is detected, this step will be skipped. If a NSX manager is detected then the connection settings will be shown. Enter the username and password of an account with at least auditor permissions to add NSX to

ControlUp Analyzer and benefit from the same functionality ControlUp Analyzer offers for vSphere. If you skip setting up the NSX connection at this point it can be established later.

- Click **Continue** to proceed to the last step.



The connection to vCenter **Vega-vC65.solar.system:443** is working!
We detected NSX at **10.1.142.110**. Why analyze NSX?

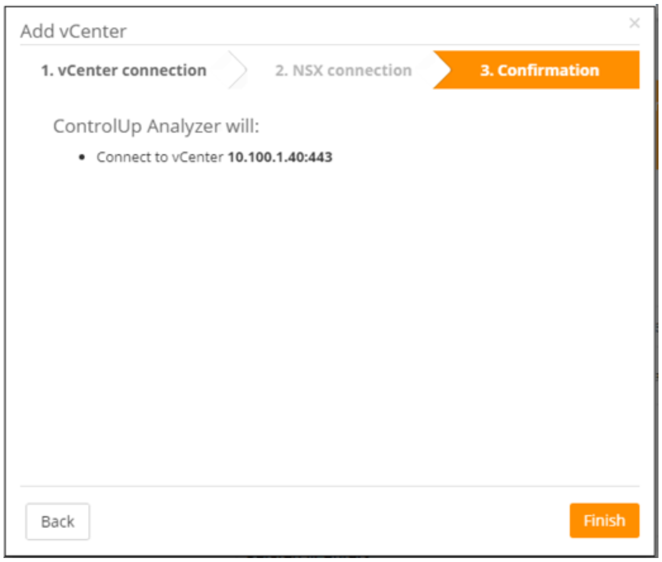
NSX Manager: * 10.1.142.110

Port: * 443

Username: * NSX username

Password: * Enter password...

- The last step will summarize the actions to be performed by ControlUp Analyzer after clicking the **Finish** button.



ControlUp Analyzer will:

- Connect to vCenter **10.100.1.40:443**

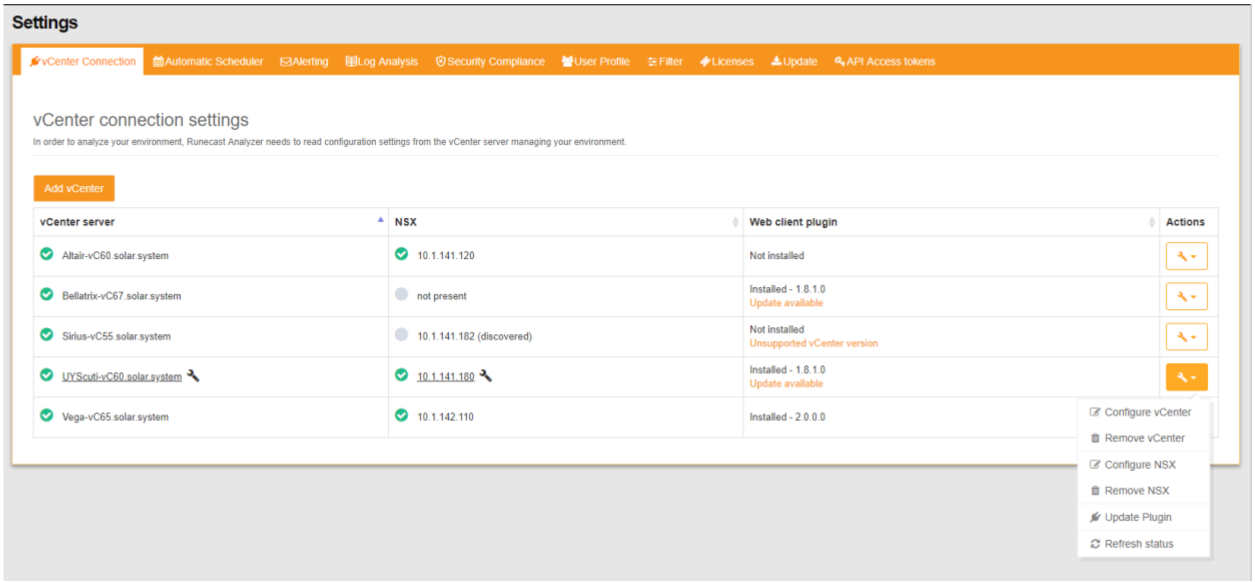
Once you have added one or more vCenters (and optionally, NSX Managers) an overview of all connections will be presented including the status of NSX and also the Web Client Plug-in installation status:

- The NSX column will display one of these states:
  - **Not present:** if no NSX was found to be connected to vCenter server.
  - **Discovered:** if NSX was discovered but it was not added to ControlUp Analyzer.
  - If **NSX** has been added it will be marked with the symbol ✓.
- The Web client plugin column will display one of the states:
  - **Not installed**
  - **Installed**

  Additional operations for Web Client Plug-in can be triggered from the **Actions** button. For more detail about the plug-in please read the section Registering the Plug-in with vCenter server.

Both vCenter and NSX can be reconfigured by using the 🔧 button, made available on hover.

Multiple actions can be performed from the dropdown **Actions** button located on the right side.



Settings

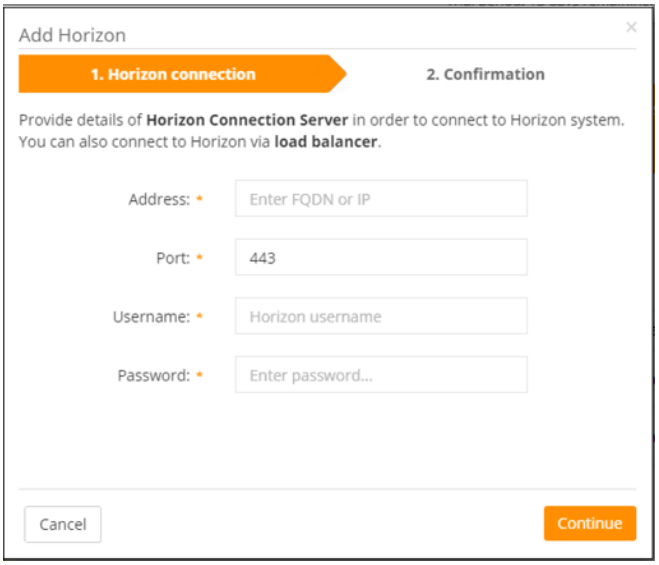
vCenter connection settings

In order to analyze your environment, Runecast Analyzer needs to read configuration settings from the vCenter server managing your environment.

vCenter server	NSX	Web client plugin	Actions
✓ Altair-vC60.solar.system	✓ 10.1.141.120	Not installed	🔧
✓ Bellatrix-vC67.solar.system	○ not present	Installed - 1.8.1.0 Update available	🔧
✓ Sirius-vC55.solar.system	○ 10.1.141.182 (discovered)	Not installed Unsupported vCenter version	🔧
✓ UYScuti-vC60.solar.system 🔧	✓ 10.1.141.180 🔧	Installed - 1.8.1.0 Update available	🔧
✓ Vega-vC65.solar.system	✓ 10.1.142.110	Installed - 2.0.0.0	

6. To connect to Horizon Connection Server (or Load Balancer) click **Add Horizon** button and follow these steps:

   - Provide the Horizon information and click **Continue** to the next step.



Add Horizon

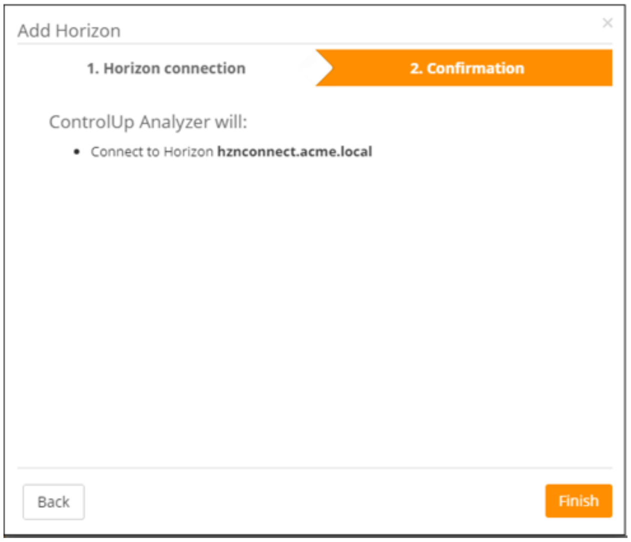
Provide details of **Horizon Connection Server** in order to connect to Horizon system. You can also connect to Horizon via **load balancer**.

Address: * Enter FQDN or IP

Port: * 443

Username: * Horizon username

Password: * Enter password...

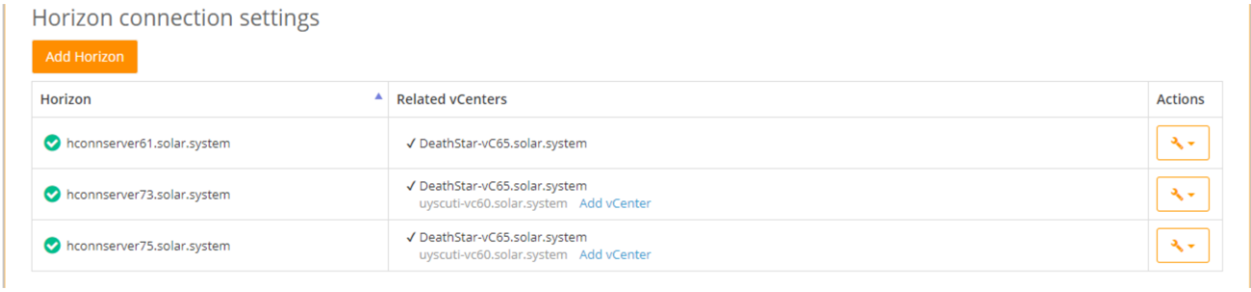


Add Horizon

ControlUp Analyzer will:

- Connect to Horizon **hznconnect.acme.local**

- Under the **Related vCenters** tab of the Horizon connection are listed all vCenter Servers which are configured for the particular Horizon environment. For complete and more relevant results it is recommended to add all Horizon vCenter Servers to ControlUp Analyzer. The vCenters marked with a checkbox are already connected to ControlUp Analyzer. The ones which are missing have an **Add vCenter** link that will open the interactive dialog to add the vCenter to ControlUp Analyzer.



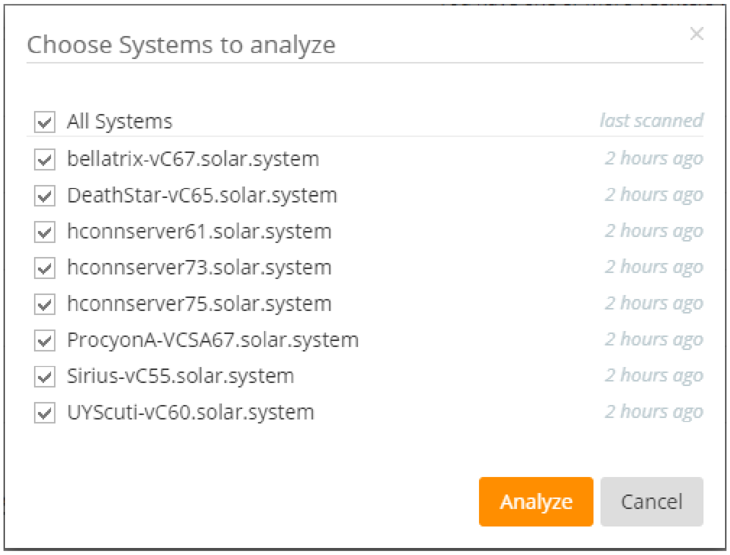
Horizon connection settings

Horizon	Related vCenters	Actions
hconnserver61.solar.system	✓ DeathStar-vC65.solar.system	
hconnserver73.solar.system	✓ DeathStar-vC65.solar.system uyscuti-vc60.solar.system Add vCenter	
hconnserver75.solar.system	✓ DeathStar-vC65.solar.system uyscuti-vc60.solar.system Add vCenter	

[Note] It is not possible to compare the vCenter Servers UUID prior to Horizon v7.4. If you're using Horizon v7.4 or older, please ensure you add the vCenter Servers in ControlUp Analyzer with the same name as added in Horizon.

7. Click the **Analyze Now** button on the top navigation bar to perform an initial analysis.

8. If only one System is configured it will be scanned. If multiple Systems (vCenters or Horizon Connection Servers) are connected you can choose which Systems to analyze (you can select them all or choose specific ones).



Choose Systems to analyze

	last scanned
☑ All Systems	
☑ bellatrix-vC67.solar.system	2 hours ago
☑ DeathStar-vC65.solar.system	2 hours ago
☑ hconnserver61.solar.system	2 hours ago
☑ hconnserver73.solar.system	2 hours ago
☑ hconnserver75.solar.system	2 hours ago
☑ ProcyonA-VCSA67.solar.system	2 hours ago
☑ Sirius-vC55.solar.system	2 hours ago
☑ UYScuti-vC60.solar.system	2 hours ago

9. After the analysis process has completed (the time taken can vary depending on number of Systems selected to be scanned and the size of environments) you can navigate to the dashboard and various views to see the results.

1.3.2 Licensing ControlUp Analyzer

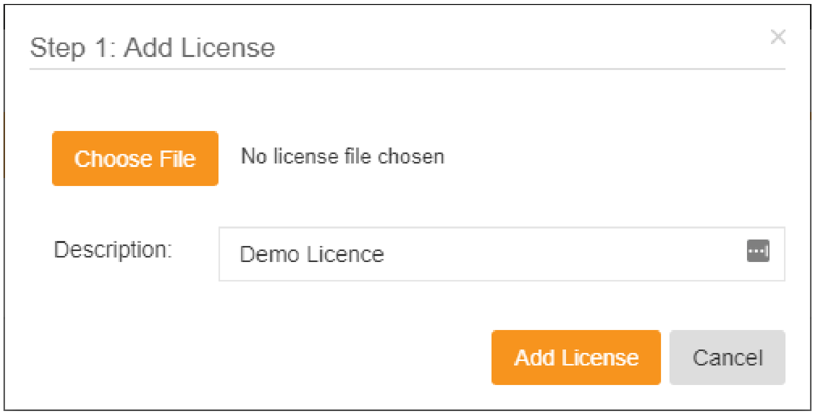
ControlUp Analyzer is licensed based on the number of CPU sockets in your environment. It comes with a 14 day evaluation period without needing to add a license. During the trial evaluation period full functionality is provided in the application, although detail is not provided for all issues. In order to add and assign a valid license to your hosts, follow the steps below.

1. Click the **Settings** icon located on the right side of the top navigation bar.

2. Click the **Licenses** tab.

3. Click **Add License** to start the two step wizard for adding and assigning a license.

4. In Step 1 of the wizard, select a valid license file you obtained from ControlUp and write a license description. Click **Add License**.



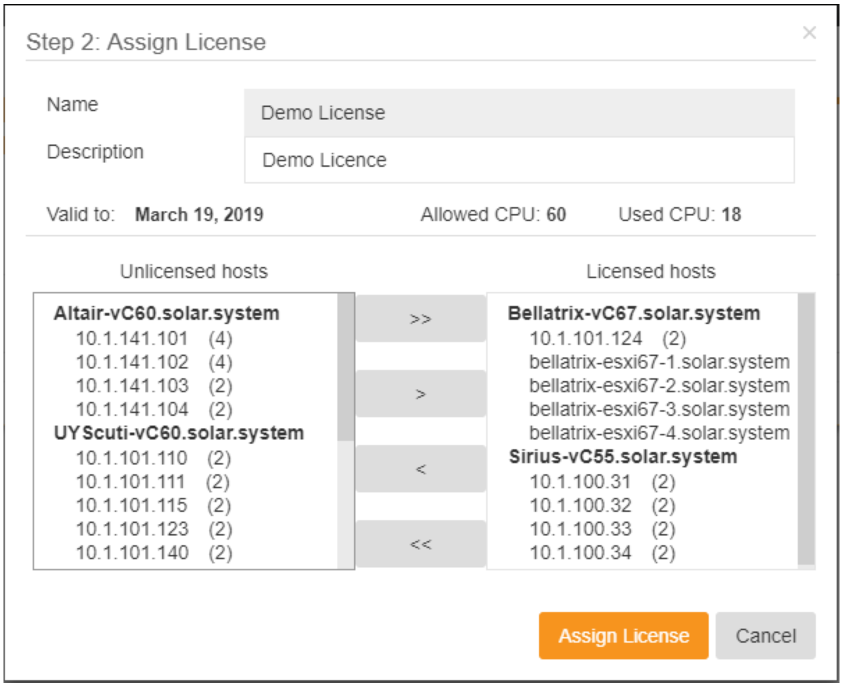
Step 1: Add License

No license file chosen

Description: Demo Licence

[Note] This action will add the license to your ControlUp Analyzer appliance but will not assign it to any specific hosts. Proceed to the next step.

5. In Step 2 of the wizard, you can select specific hosts to license. Select the hosts from the **Unlicensed hosts** column and click on **>** to move them under **Licensed hosts** on the right-hand side. If the hosts have already been licensed, they will not appear under **Unlicensed hosts**. Click **Assign License** once you are done.



Step 2: Assign License

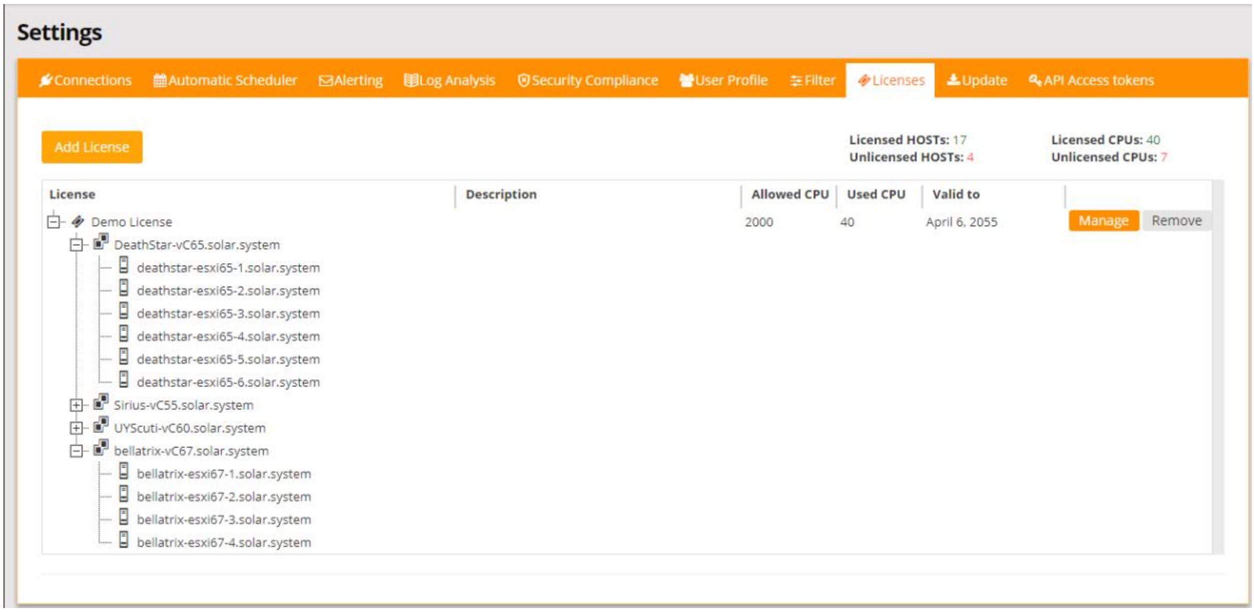
Name: Demo License

Description: Demo Licence

Valid to: **March 19, 2019** Allowed CPU: **60** Used CPU: **18**

Unlicensed hosts	Licensed hosts
Altair-vC60.solar.system	**Bellatrix-vC67.solar.system**
10.1.141.101 (4)	10.1.101.124 (2)
10.1.141.102 (4)	bellatrix-esxi67-1.solar.system
10.1.141.103 (2)	bellatrix-esxi67-2.solar.system
10.1.141.104 (2)	bellatrix-esxi67-3.solar.system
UYScuti-vC60.solar.system	bellatrix-esxi67-4.solar.system
10.1.101.110 (2)	**Sirius-vC55.solar.system**
10.1.101.111 (2)	10.1.100.31 (2)
10.1.101.115 (2)	10.1.100.32 (2)
10.1.101.123 (2)	10.1.100.33 (2)
10.1.101.140 (2)	10.1.100.34 (2)

The license you specified at Step 1 of the wizard was added to your ControlUp Analyzer appliance and it was assigned to the host you specified in Step 2. Once added, the license appears in the licenses list:



Licensed HOSTs: 17
Unlicensed HOSTs: 4

Licensed CPUs: 40
Unlicensed CPUs: 7

License	Description	Allowed CPU	Used CPU	Valid to
Demo License		2000	40	April 6, 2055
DeathStar-vC65.solar.system				
deathstar-esxi65-1.solar.system				
deathstar-esxi65-2.solar.system				
deathstar-esxi65-3.solar.system				
deathstar-esxi65-4.solar.system				
deathstar-esxi65-5.solar.system				
deathstar-esxi65-6.solar.system				
Sirius-vC55.solar.system				
UYScuti-vC60.solar.system				
bellatrix-vC67.solar.system				
bellatrix-esxi67-1.solar.system				
bellatrix-esxi67-2.solar.system				
bellatrix-esxi67-3.solar.system				
bellatrix-esxi67-4.solar.system				

Click **Manage** to change the license assignment or description. You can click **Remove** to remove the license from the list and disassociate it from hosts.

1.3.3 Configure Log Collection

ControlUp offers real-time analysis of logs received from the vSphere hosts and VMs. Your hosts may already be forwarding their logs to a standard syslog collector. ControlUp Analyzer can be configured as an additional syslog destination; logs will continue to be sent to your other syslog server(s) and you do not need to delete any current syslog server addresses. ControlUp will retain only the relevant log entries that may indicate a potential issue.

Configure log settings for all **ESXi hosts** and **VMs** in order to maximize the data being analyzed for issues.

[Note] The log configuration can be carried out at any time. ControlUp Analyzer will start analyzing the logs immediately after they are forwarded to the appliance. If you would like to setup log collection later, you can skip this step.

1.3.3.1 ESXi Log Forwarding – Automatic Setup

1. Ensure that the vCenter user you have configured has the following privileges:

    - Host > Configuration > Advanced settings

    - Host > Configuration > Network configuration

2. Click the **Settings** icon located on the right-hand side of the top navigation bar and select the **Log Analysis** tab.

3. Click the **Edit** button to configure log retention. This can be set according to the number of days retained and maximum size of logs retained on disk.

4. Observe the list of vCenters connected to ControlUp Analyzer appliance. Clicking on each one will expand the list of hosts belonging to the selected vCenter and will display whether they are configured to send their logs to the ControlUp Analyzer appliance (either a green checkmark or a red cross).

5. Click the wrench icon located on the right-hand side of the **Host syslog settings** section.

6. Select the hosts that are not configured and click **Configure**. Confirm the changes by clicking **OK**.

[Note] Some checkboxes may appear in grey – this means they are not selectable due to insufficient privileges for the vCenter user configured. Refer to **Step 1** for more information.

7. The **Reload** button is used for fetching the syslog settings from all connected vCenters. To fetch a specific vCenter server use the ⟳ icon located to the right-hand side of the selected vCenter.

1.3.3.2 ESXi Log Forwarding – PowerCLI Script Setup

Alternatively, you can use a PowerCLI script to configure ESXi logging:

1. Click the help ring icon located to the right-hand side of the **Host syslog settings** section in the **Log Analysis** tab.

2. Expand the section and click to download the PowerCLI script.

3. You can review the script before execution and make changes if needed.

4. Execute the script using PowerCLI.

1.3.3.3 ESXi Log Forwarding – Manual Setup

If you prefer to configure the ESXi syslog settings manually then follow the steps provided in this section. For each ESXi host in you environment, perform the following:

Navigate to the **Syslog.global.logHost** setting:

1. (*Web Client*) select the **ESXi host > Manage > Settings > Advanced System Settings**

2. (*vSphere Client*) select the **ESXi host > Configuration > Advanced Settings > Syslog**

3. Add udp://*applianceIP*:514 to the value of **Syslog.global.logHost** (if you already have another remote syslog configured, append the value and separate it with a comma). Click **OK**.

4. Navigate to **Security profile > Firewall > Properties**.

5. Make sure that **syslog** is enabled. Click **OK**.

[Note] You can read more about enabling remote syslog in the VMware KB article 2003322.

1.3.3.4 Enable VM Log Forwarding to Syslog – Automatic Setup

VM log forwarding is only effective if you have configured ESXi log forwarding (see above).

By default, a VM will log to files located in the VM directory. In order to forward the VM logs to syslog automatically, follow these steps:

1. Ensure that the vCenter user you have configured has the following privileges:

- Virtual Machine > Configuration > Advanced

2. Click the **Settings** icon located on the right side of the top navigation bar and select the **Log Analysis** tab.
3. Observe the list of vCenters connected to the ControlUp Analyzer appliance. Clicking on each one will expand the list of VMs belonging to the selected vCenter and whether they are configured to send their logs to the ControlUp Analyzer appliance (either a green checkmark or a red cross).
4. Click the wrench icon located on the right-hand side of the **VM log settings** section.
5. Select the VMs that are not configured and click **Configure**.
6. Perform either a **vMotion** or **Power Cycle** for each VM. This ensures that the configuration is applied and thereafter logs will be sent from the VM.

[Note] Some checkboxes may appear in a grey color – this means that they are not selectable due to insufficient privileges for vCenter user you have configured. Refer to **Step 1** for more information.

1.3.3.5 VM Log Forwarding – PowerCLI Script Setup

Alternatively, you can use a PowerCLI script to configure VM logging:

1. Click the help ring icon located on the right side-hand of the **VM log settings** section of the **Log Analysis** tab.
2. Expand the Scripted section and download the PowerCLI script.
3. You can review the script before execution and make any changes if needed.
4. Execute the script using PowerCLI.
5. Perform either a **vMotion** or **Power Cycle** for each VM. This ensures that the configuration is applied and thereafter logs will be sent from the VM.

1.3.3.6 Enable VM Log Forwarding to Syslog - Manual

If you prefer to configure the VM log settings manually then follow the steps in this section. VM log forwarding will only be effective if you have previously configured ESXi log forwarding.

By default, a VM will log to files located in the VM directory. In order to forward the VM logs to syslog, follow these steps for each VM:

1. Power off/Shutdown the VM.
2. In the VM Hardware panel, click **Edit Settings > VM Options**.
3. Click the **Advanced** triangle to expand the advanced virtual machine options.

4. Select **Enable logging**.
5. Click **Configuration parameters**.
6. Click **Add Row**.
7. In **name** column insert: **vmx.log.destination**, In **value** column insert: **syslog-and-disk**
8. Click **Add Row**.
9. In **name** column insert**: vmx.log.syslogID**
10. In **value** column insert the specific VM name. Click **OK** twice.

2 Working with ControlUp Analyzer

2.1 What is an Issue?

In ControlUp Analyzer, an **Issue** represents a discovered problematic combination of infrastructure values such as configuration settings, log patterns, software and hardware type and versions, etc. The discovered combination of values is considered problematic based on information from various sources including VMware Knowledge Base articles, official VMware Security Hardening Guide and industry Best Practices.

An issue in ControlUp Analyzer has several fields:

- **Severity**: This grades the estimated importance of the issue based on its general impact and importance. Depending on the specifics of your environment, it is possible that certain issues may have a different importance than the suggested severity.
- **AppliesTo**: The virtual infrastructure layer the issue affects – Compute, Network, Storage, VM, Management.
- **Affects**: The infrastructure quality the issue affects – Availability, Manageability, Performance, Recoverability, Security.
- **Products**: Supported products by ControlUp Analyzer (vSphere, NSX-V, vSAN, Horizon)
- **Objects**: The number of objects (e.g. VMs, Hosts, Datastores) affected by this issue.
- **Title**: A short description of the issue.
- **Count**: *This field is applicable only to log related KBs*. The number of problematic log pattern occurrences within the specified period of time.
- **Last seen date:** *This field is applicable only to log related KBs*. The last date and time when the problematic log pattern was detected.
- **Result**: *This field is applicable only to Security hardening section*. Presents the status of security rule based on the findings results: Pass or Fail.
- **Vulnerability id**: *This field is applicable only to DISA STIG*. The identification id set by Information Assurance Support Environment on their rules list.
- **Control id**: *This field is applicable only to PCI DSS*. The identification id set by Payment Card Industry Security Standards Council on their documentation list.
- **Milestone**: *This field is applicable only to PCI DSS*. Milestones are defined in the PCI DSS standard to enable you to use the “Prioritized Approach” to prioritize higher risk issues.
- **Rule ID**: *This field is applicable only to HIPAA*. The identification id set by Health Insurance Portability and Accountability Act on their documentation list.

Once you expand an issue in the ControlUp Analyzer interface, you can view additional fields:

- **Source:** The source describing the issue – Knowledge Base, Security Hardening Guide, Best Practice.
- **Reference:** A link to online resources further describing the issue.
- **Date of last update:** The date when the issue definition was last updated in the ControlUp Analyzer database.
- **Impact:** The relative potential impact of the issue – 1 is low and 3 is high.
- **Importance:** The importance of this issue – 1 is low and 3 is high. The issue importance depends on the infrastructure quality it relates to (Availability, Manageability, Performance, Recoverability, Security) and the infrastructure layer it impacts (Compute, Storage, Network, VM, Management). For example, if the issue is Security- or Availability-related and applies to the Compute layer then the Importance will be higher. If the issue impacts Manageability of individual VMs then the Importance will be lower.
- **Risk rating:** The sum of Impact and Importance.
- **Findings:** This is an important tab that shows the list of affected objects (e.g. VMs, Hosts, Datastores). For each object, the settings that were found to be problematic or the log messages that need to be reviewed are displayed. Click on an object from the affected objects list on the left to see the list of findings listed on the right. The findings list displays the description and current value of each finding that needs to be reviewed. In case of log-related KBs, you can see the exact log messages associated with the described issue.
- **Note:** Here you can add a note to any Knowledge Base article, Best Practice or Security Hardening check. The notes are not linked to the actual check (not to a detected issue) – so even if you have a Security Hardening check which is with **Pass** status, you can still add a note to it.
- **Ignore:** You will be able to filter out the current KB/SH/BP against infrastructure objects based on your selection.

2.2 What is an Object?

An **Object**, also referred to as *configuration item* is an inventory object from the virtual infrastructure. Objects can be vCenter, hosts, VMs, datastores, virtual switches, resource pools, farms, security servers etc.

2.3 Context

Gives the possibility to select a single System (vCenter Server or Horizon Connection Server) or all. Depending on the selection made the rest of the interface will show the appropriate information on **MAIN MENU** and **CONFIGURATION ANALYSIS**. This is not applicable to **LOG ANALYSIS** which is general for all Systems**.**

2.4 MAIN MENU

Contains three subsections presenting an overview of the environment, issues discovered and history trend.

2.4.1 Dashboard

The ControlUp Analyzer dashboard is the central page that provides a summary of your virtual environment and detected issues. Navigate to the ControlUp Analyzer Web Interface url: ***https://applianceIP*** and login with valid credentials. By default, the local user credentials are:

User: rcuser

Password: ControlUp!

If you have configured ControlUp Analyzer to use Active Directory then you can use an Active Directory account. Make sure to specify the username in one of the following formats:

- username
- username@domain.com

Based on number of Systems configured (one or multiple), and the selection done on the **CONTEXT,** the Dashboard will provide slightly different views:

Components displayed when **only one System (vCenter Server)** is connected:

- Analyze now button
- Configuration Issues by Severity
- Configuration Issues by Layer
- Log Issues
- KBs Applicable
- Security Compliance
- Best Practice Adoption
- Issues History
- Hosts with Most Issues
- Analysis Detail

Components displayed when **only one System (Horizon Connection Server)** is connected:

- Analyze now button
- Configuration Issues by Severity
- KBs Applicable
- Best Practice Adoption
- Issues History
- Analysis Detail

Components displayed when **multiple Systems** are connected (**All Systems**):

- Analyze now button
- Configuration Issues by Severity
- Configuration Issues by Layer
- Log Issues

- KBs Applicable
- Security Compliance
- Best Practice Adoption
- Issues History
- Hosts with Most Issues
- My Systems

2.4.1.1 Analyze now button

Click this button to initiate a scan and perform an analysis of all configuration data in your virtual infrastructure. It is recommended that you enable and configure automated scheduled scans – see Automatic scheduler (for more information about Analyze now button please check section 1.3.1 Connect to a System and Analyze).

2.4.1.2 Configuration Issues by Severity

The widget located at the top-left corner of the dashboard provides a quick summary on the number of issues found in the environment, grouped by severity. In the All Systems view it provides the summary across all Systems connected.

2.4.1.3 Configuration Issues by Layer

The widget is located in the left side of the dashboard, below **Configuration Issues by Severity.** It provides a quick summary of the number of issues found in the environment, grouped by layer and severity. Each severity has a related icon (● - Critical, ⚠ - Major, ● - Medium, ● - Low). In the All Systems view it provides the summary across all vCenters connected.

2.4.1.4 Four Key-metric Badges

- **Log Issues:** Number of Knowledge Base related issues discovered in logs. In the All Systems view this is the number of Knowledge Base related issues discovered across all Systems connected.

- **KBs Applicable:** Number of Knowledge Base related issues discovered in the Systems configuration. The number of current issues found will be accompanied by an arrow representing the average of the last five scans. Its direction will indicate a trend factoring the current value and average historical values. The historical trending will also be displayed by a sparkline. In the All Systems view this is the number of Knowledge Base related issues discovered across all Systems connected.

- **Security Compliance:** The level of security compliance based on all security checks performed as part of the Security Hardening view. The compliance percentage will be accompanied by an arrow representing the average of the last five scans. Its direction will indicate a trend factoring the current value and average historical values. The historical trending will also be displayed by a sparkline. In the All Systems view this is the level of security compliance across all vCenters connected.

- **Best Practice Adoption:** The level of Best Practice adoption, based on all best practices enabled as part of the Best Practices view. The Best Practice percentage will be accompanied by an arrow representing the average of the last five scans. Its direction will indicate a trend factoring the current value and average historical values. The historical trending will also be displayed by a sparkline. In the All Systems view this is the level of Best Practice adoption across all Systems connected.

2.4.1.5 Issues history

The bar chart provides an overview of the issue count evolving over time.

If the **Days** view is selected, then each day will be represented by a bar along the x-axis. When hovering over a bar, it will display the number of issues (this is also shown for each severity, represented with the corresponding color) of the last scan during that day. Where no scans were performed during the day, the bar color will be less vivid and on hover the message **No analysis on this day** will be shown.

If the **Weeks** view is selected, then each week will be represented by a bar along the x-axis. When hovering over a bar, it will display the number of issues (this is also shown for each severity, represented with the corresponding color) calculated as an average for the entire week. Where no scans were performed during the entire week, the bar color will be less vivid and on hover the message **No analysis on this week** will be shown.

2.4.1.6 Hosts with Most Issues

A list displayed below the **Issue History** shows the hosts having the highest number of issues. The hosts included in the analysis will depend which vCenter(s) are selected in the **CONTEXT**. The issue count will be accompanied by corresponding severity icons.

2.4.1.7 My Systems / Analysis Detail

At the bottom of the Dashboard more detailed information concerning Systems scan results is available.

When **All Systems** is selected in the **CONTEXT**, then a list of all Systems connected to ControlUp Analyzer will be shown. The number of issues found in Logs, KBs and also the percentage for Security Compliance and Best Practice Adoption are visible for each System row. Expanding any row will show further details about the checks performed and objects analyzed. The “Analyze now” button is also available in each row providing a quick way to trigger a scan for the selected System.

When a **single System** is selected in the **CONTEXT**, a Dashboard widget is shown at the bottom entitled “Analysis Detail”. This will show further lower-level details for the System selected about the checks performed and objects analyzed.

2.4.1.8 Generate Report button

A PDF report will be generated reproducing the full dashboard overview (as displayed in the user interface). This provides a colorful and graphical management report that includes the standard badges and statistics showing the overall system health. Additionally, a list of the top 50 Issues is also included.

2.4.2 Inventory View

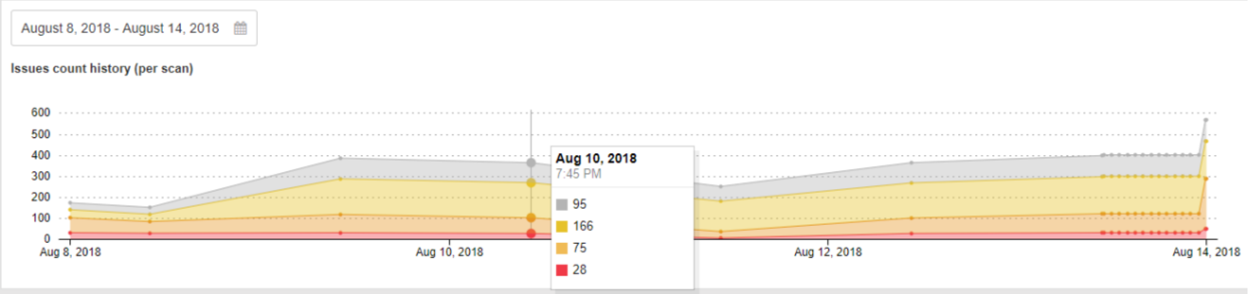
Browse through your virtual infrastructure objects hierarchically using the Inventory feature. The number of detected issues is shown alongside inventory objects in the tree-view shown. Click on an object to open a detailed list of associated issues.

2.4.3 All Issues View

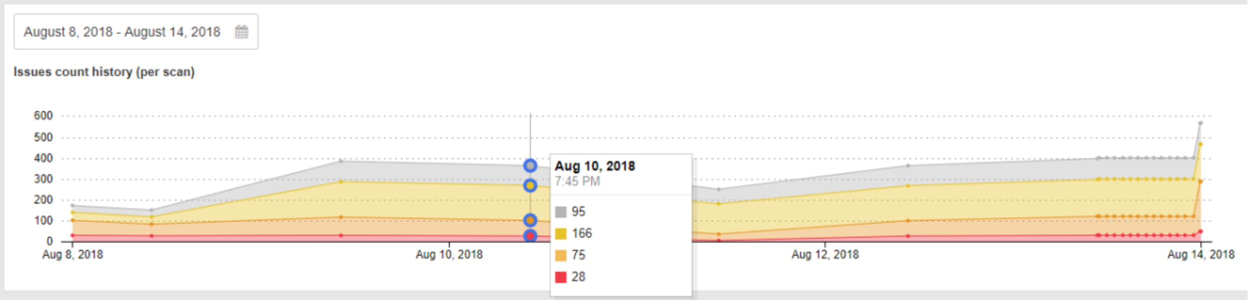
This view combines all types of detected issues into a single chart and table – Configuration KB issues, Best Practice, Security Hardening checks and Log KB issues. By default the list of current issues (at the last scan) is displayed. This view is easy customized by using filters and/or selecting historical points in time.

At the top of the view, six dropdown buttons (vCenters, Severity, Source, Applies to, Affects, Products) provide the possibility to filter the data displayed. The list of filters applied is shown directly under the dropdown buttons. Filters are applied to the history chart and also to the list of results. Two other features are found at the top-right. The **Search** bar gives the possibility to search for text in **Title**. The **Export** button provides the option to export the **Result** table in different formats (.pdf, .csv). If selected, the option ***include affected objects*** will output each affected object together with low-level results for their specific findings.

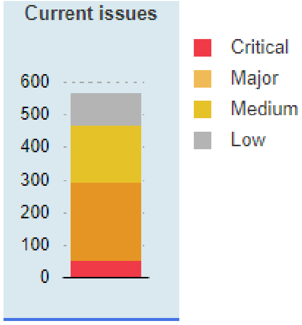
The history chart is provided to visualize issue levels or objects number over the time period shown. Use one of the two buttons **Objects/Issues** to switch to the desired view. The time period can be selected by using the calendar control. Each scan is represented using dots, which will display additional information (date/hour of the scan and the number of issues found) when the user hovers over them.



If a specific point in time is selected when clicking on the selected date, this is confirmed with blue edges being shown around the dots. This selection will modify the **Results** table and the issues found will be relevant to the date selected. Remember that any dropdown filters selected will also affect the results based on their selection.

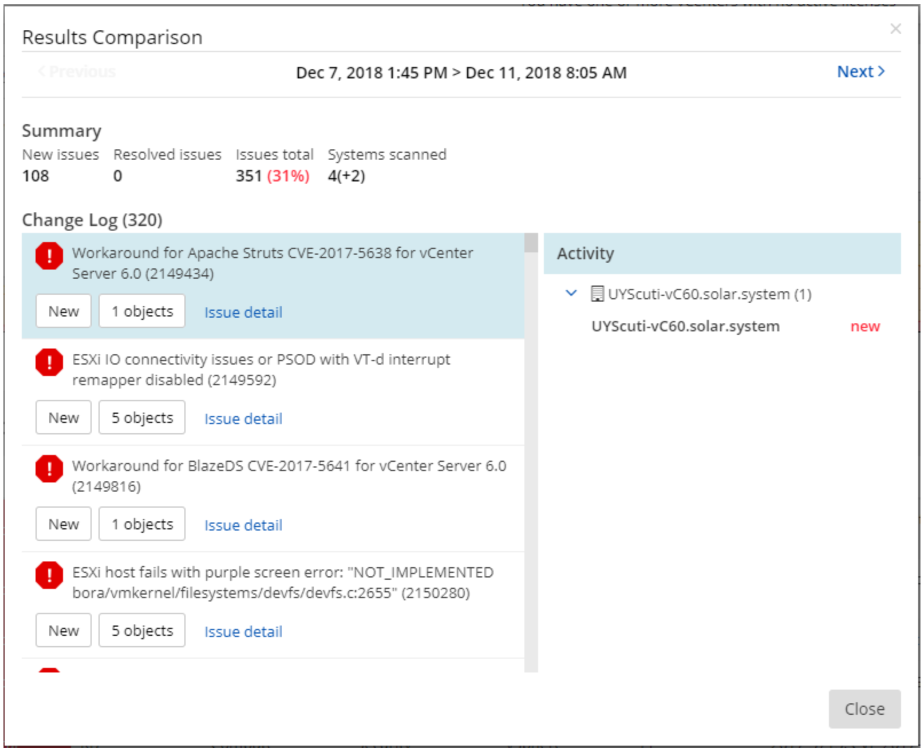


A widget is shown on the right-hand side of the chart providing the count of **Current Issues** found during the last scan. The number of issues displayed is affected by any filters applied from the dropdown buttons found at the top of this page. This is also affected by any filters applied using the **Ignore** button within a specific issue, or Filters applied in the **Settings** -> **Filter** page.



If the **Results** table has been modified to display issues from a specific date or selected using the chart and point in time dots, just click on the **Current Issues** widget so that the table provides the current results.

An important feature allows you to understand changes between two consecutive scans. This is found on the right-hand side of the **Results** table and is named **Compare with previous result**. Once you click on it, a popup window will open showing a summary of changes.



Results Comparison

‹ Previous Dec 7, 2018 1:45 PM > Dec 11, 2018 8:05 AM Next ›

Summary

New issues	Resolved issues	Issues total	Systems scanned
108	0	351 (31%)	4(+2)

Change Log (320)

Workaround for Apache Struts CVE-2017-5638 for vCenter Server 6.0 (2149434)
New 1 objects Issue detail

ESXi IO connectivity issues or PSOD with VT-d interrupt remapper disabled (2149592)
New 5 objects Issue detail

Workaround for BlazeDS CVE-2017-5641 for vCenter Server 6.0 (2149816)
New 1 objects Issue detail

ESXi host fails with purple screen error: "NOT_IMPLEMENTED bora/vmkernel/filesystems/devfs/devfs.c:2655" (2150280)
New 5 objects Issue detail

Activity

UYScuti-vC60.solar.system (1)

UYScuti-vC60.solar.system new

Close

[**Note**] If any filters have been applied using the drop-down buttons in the **All Issues** View, this will also be applied to the popup and so will affect the Systems and issues displayed.

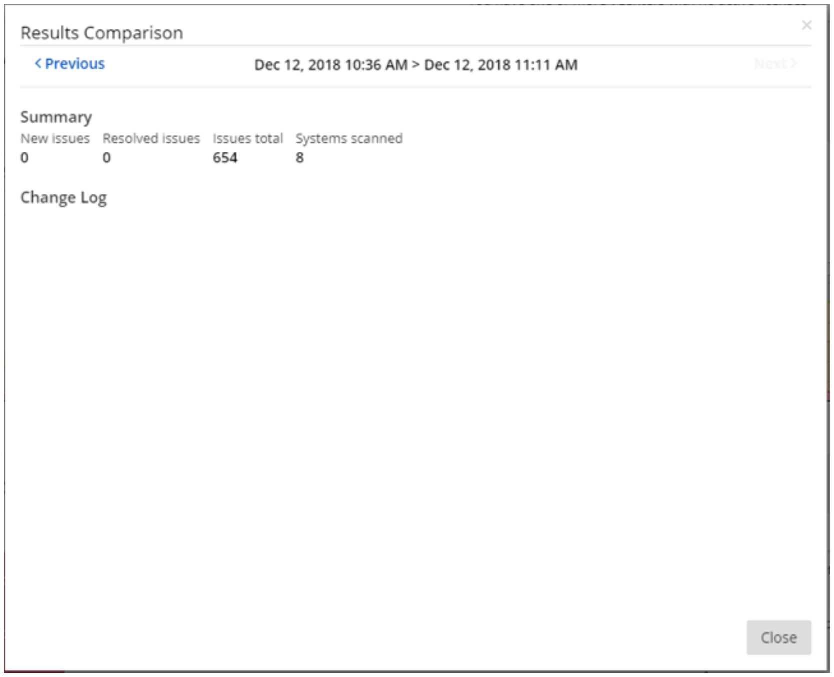
The time range for the comparison is shown at the top of the pop-up. The dates/hours refer to the points in time when the scans being compared were triggered. You can navigate to **Previous** or **Next** to move between consecutive scans and quickly show a comparison for the newly selected scans.

Summary offers an overview of new, resolved and total numbers of issues. It also shows the number of Systems scanned.

Change Log will show the **New issues** found. Each one will display these attributes:

- Title of issue and severity (represented by the specific icon).
- The type of change is shown using one of the following statuses:
  - **New** – the issue was not found in the previous scan.
  - **Resolved** – the issue was present in the previous scan but it was not found in the next one.
  - **Partially resolved** – the number of objects affected is less than in the previous scan.
  - **Increased** – the number of objects affected is higher than in the previous scan.
- Number of objects affected by the issue.
- Issue detail – on click this will open an additional tab containing the full issue description.
- Activity table showing the objects affected by the changed status between two consecutive scans.

If there are no changes between two consecutive scans then just the total issues and Systems scanned will be displayed.



New issues	Resolved issues	Issues total	Systems scanned
0	0	654	8

[**Note**] To improve performance and reduce storage usage, historical data older than twelve months will be displayed in a simplified view. The changes are reflected in the following areas:

- A historic issue's results are no longer available for comparison with other results and the button used for this action will be replaced with a **Simplified Results** label.
- The Findings tab within historic issues will no longer contain the affected objects and their values.
- When generating reports via the **Export** button, located in the top right corner of the screen, the option to include the affected objects is not available anymore.

2.5 CONFIGURATION ANALYSIS

This section includes several views of configuration issues that were detected from scanning the entire virtual infrastructure and by analyzing the configuration settings. Each view provides the capability to Export (at the top-right of the screen) the issues shown in the table. You also have the option to ***include affected objects*** which will output each affected object and the objects' findings values.

2.5.1 Config KBs Discovered

This view lists all detected issues within the scanned virtual infrastructure that were derived from VMware Knowledge Base articles.

2.5.2 Best Practices

This view includes industry best practices related to VMware's recommendations. Each best practice is checked against the configuration items from the scanned virtual infrastructure. If a specific best practice is followed for all related objects, the best practice item is marked as **Pass**. If it is not followed for at least one of the affected objects, then it is marked as **Fail**. Expanding the best practice section will show details on affected objects and provide the settings that do not align with the best practice.

2.5.3 Security Hardening

This section contains security and compliance policies related to VMware's guidelines, DISA STIG and PCI DSS.

2.5.3.1 VMware Guidelines

The security rules displayed in this view are taken from the official VMware Security Hardening guides. Their severity differs based on the type of security check:

- **Low Severity:** Security hardening that is intended for highly secure environments only.
- **Medium Severity:** Security hardening that relates to common environments.
- **Major Severity:** Security hardening that can relate to any environment and is related to a host or a network configuration item.

Regardless of the original severity, some security rules may not be required for your organization's security policy. You might need to customize the displayed security checks by filtering those that are not included in your organization's security policy. For more information, see Filters.

Every security check can either **Pass** or **Fail**. In cases where there is at least one object in your infrastructure that is not compliant with a specific security check, this check will be marked as **Fail**. The list of non-compliant objects can be viewed in the details of the affected objects section.

2.5.3.2 DISA STIG 6

The security rules displayed in this view are taken from the official Information Assurance Support Environment (IASE) website. Their severity differs based on the type of security check:

- **Low Severity:** Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

- **Medium Severity:** Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
- **High Severity:** Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.

Regardless of the original severity, some security rules may not be required for your organization's security policy. You might need to customize the displayed security checks by filtering those that are not included in your organization's security policy. For more information, see Filters.

Analysis results can display the following states:

- **Fail:** will be displayed where there is at least one object in your infrastructure that is not compliant with a specific security check. The list of non-compliant objects can be viewed in the details of the affected objects section. **No Manual** check is involved.
- **Pass:** will be displayed in case that no object is found to be non-compliant. **No Manual** check is involved.
- **Manual:** An answer to **Manual** check is required.
- **Fail (M):** will be displayed where there is at least one object in your infrastructure that is not compliant with a specific security check. The list of non-compliant objects can be viewed in the details of the affected objects section. A **Manual** check is involved.
- **Pass (M):** will be displayed where no object is found to be non-compliant. A **Manual** check is involved.

2.5.3.3 PCI DSS

The requirements and controls cited in the profile are taken from PCI DSS v3.2.1 (May 2018). The milestones displayed in this view are taken from the PCI DSS "Prioritized Approach". The Prioritized Approach provides six security milestones that help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance. Milestones range from 1-6, with 1 being the highest priority and 6 being the lowest:

- 1 - Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised.
- 2 - Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromises – the network or a wireless access point.
- 3 - Secure payment card applications. This milestone targets controls for applications, application processes, and application servers.
- 4 - Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning and who is accessing your network and cardholder data environment.
- 5 - Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protections mechanisms for that stored data.

- 6 - Finalize remaining compliance efforts and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

Regardless of the original severity, some security rules may not be required for your organization's interpretation of the security policy. You might need to customize the displayed security checks by filtering those that are not required. For more information, see Filters.

PCI DSS contains two types of rules (**Customizable** and **Non-customizable**). The main difference between them is that Customizable rules allows the user to change the parameters default values, used by the checks, to the desired ones. Additional filter tab named Customizable can be used to quickly select one of the two types. To change the default values, expand the rule marked as Customizable and navigate to Customize tab. A short note describing the setting purpose and its default value is available. Click on the Add Custom Value button, insert the custom value on the dedicated field and select an inventory object which will be evaluated against new value. By selecting a parent object, the value will be propagated to its children. After pressing the Save button you will be able to see a new line presenting the object in scope, the custom value, the user name and the time when he updated the value. Multiple values can be added to different inventory objects. A value set to children object will rewrite the value set on parent level. After customization is done don't forget to Analyze the environment so the new values are taken into account. Each one of the customized rules will be flagged with a **C** mark in the Result status column.

Every security check can either return a result of **Fail** or **Configured**. In cases where there is at least one object in your infrastructure that is not compliant with a specific security check, this check will be marked as **Fail**. The list of non-compliant objects can be viewed in the details of the affected objects section. A result of **Configured** means there are no objects failing for the specific check, but this does not mean you are fully compliant against the whole PCI DSS requirement or control.

2.5.3.4 HIPAA

This profile relates to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) published by the Secretary of the U.S. Department of Health and Human Services (HHS).

Organizations (called "covered entities") must put in place technical safeguards to secure individuals' "electronic protected health information" (e-PHI). The profile lists relevant technical safeguards in the virtual infrastructure that are automatically checked and compared against the requirements of the HIPAA Security Standards for the Protection of Electronic Protected Health Information (the Security Rule).

Every security check can either return a result of **Fail** or **Configured**. In cases where there is at least one object in your infrastructure that is not compliant with a specific security check, this check will be marked as **Fail**. The list of non-compliant objects can be viewed in the details of the affected objects section. A result of **Configured** means there are no objects failing for the specific check.

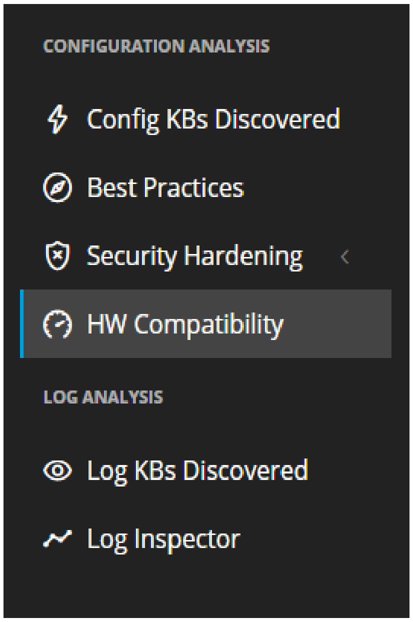
Regardless of the original severity, some security rules may not be required for your organization's interpretation of the security policy. You might need to customize the displayed security checks by filtering those that are not required. For more information, see Filters.

2.5.4 HW Compatibility

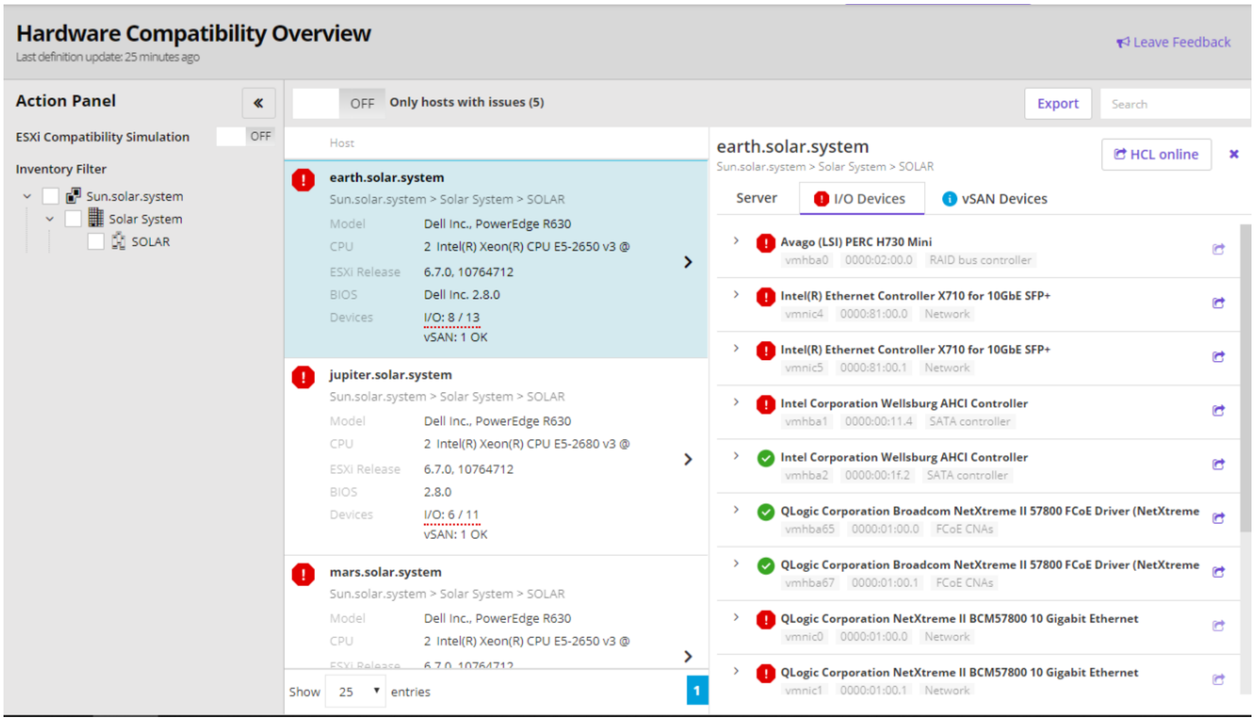
In this section the Analyzer shows you the compliance status of your hardware against VMware Hardware Compatibility List (HCL). Keeping your vSphere hardware aligned with VMware HCL is critical for the health and support of your virtual environment.

N.B. ESXi 6.0 and above are supported for this feature. Ensure you have the minimum required permissions specified in **System Requirements.**

The feature is accessed by clicking the **HW Compatibility** button from the sidebar:



On selection, the **Hardware Compatibility Overview** screen will be shown in the main panel:



earth.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2650 v3 @
ESXi Release	6.7.0, 10764712
BIOS	Dell Inc. 2.8.0
Devices	I/O: 8 / 13 vSAN: 1 OK

jupiter.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2680 v3 @
ESXi Release	6.7.0, 10764712
BIOS	2.8.0
Devices	I/O: 6 / 11 vSAN: 1 OK

mars.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2650 v3 @
ESXi Release	6.7.0, 10764712

earth.solar.system
Sun.solar.system > Solar System > SOLAR

❗	Avago (LSI) PERC H730 Mini	vmhba0	0000:02:00.0	RAID bus controller
❗	Intel(R) Ethernet Controller X710 for 10GbE SFP+	vmnic4	0000:81:00.0	Network
❗	Intel(R) Ethernet Controller X710 for 10GbE SFP+	vmnic5	0000:81:00.1	Network
❗	Intel Corporation Wellsburg AHCI Controller	vmhba1	0000:00:11.4	SATA controller
✓	Intel Corporation Wellsburg AHCI Controller	vmhba2	0000:00:1f.2	SATA controller
✓	QLogic Corporation Broadcom NetXtreme II 57800 FCoE Driver (NetXtreme	vmhba65	0000:01:00.0	FCoE CNAs
✓	QLogic Corporation Broadcom NetXtreme II 57800 FCoE Driver (NetXtreme	vmhba67	0000:01:00.1	FCoE CNAs
❗	QLogic Corporation NetXtreme II BCM57800 10 Gigabit Ethernet	vmnic0	0000:01:00.0	Network
❗	QLogic Corporation NetXtreme II BCM57800 10 Gigabit Ethernet	vmnic1	0000:01:00.1	Network

- On the left-hand side, the **Action Panel** contains two main components:

  - The **ESXi Compatibility Simulation** component is offering the ability to show if your current hardware would have compatibility with other ESXi versions available (6.0 and above), simulating possible upgrade/downgrade based on the version selected. To enable the simulation turn on the button located at its right-hand side. You can then choose the desired version from the revealed drop-down list. Initiate the compatibility analysis by pressing the **Simulate** button. The results are displayed on the right-hand side. The icons︽, ︾ or = located before the ESXi Release indicate if your selected ESXi version for simulation will be an upgrade or downgrade from the present version. A detailed description of the right-hand side panel is described in the next paragraph.

  - The **Inventory Filter** component provides an inventory tree, showing all vCenter Servers, and includes nested Datacenters and Clusters (N.B. Hosts that are not part of any cluster are grouped into an area entitled **Standalone Hosts**). This allows you to select appropriate objects as desired. By default, all vCenters monitored by the Analyzer and their licensed hosts are displayed. If you want to focus attention on specific Datacenter(s) or Cluster(s) you can tick the corresponding checkboxes which will filter the view based on your selection.

- On the right-hand side of the main panel all Hosts are presented in a table offering a breakdown of configuration and the compatibility evaluation. Cross-checks between the Host's system Data and the HCL industry knowledge will produce an overall state for the host (Compatible ✓ or Possibly Incompatible❗). In case of incompatibility, the parameter that contributed to this status will be underlined by a red dotted line.

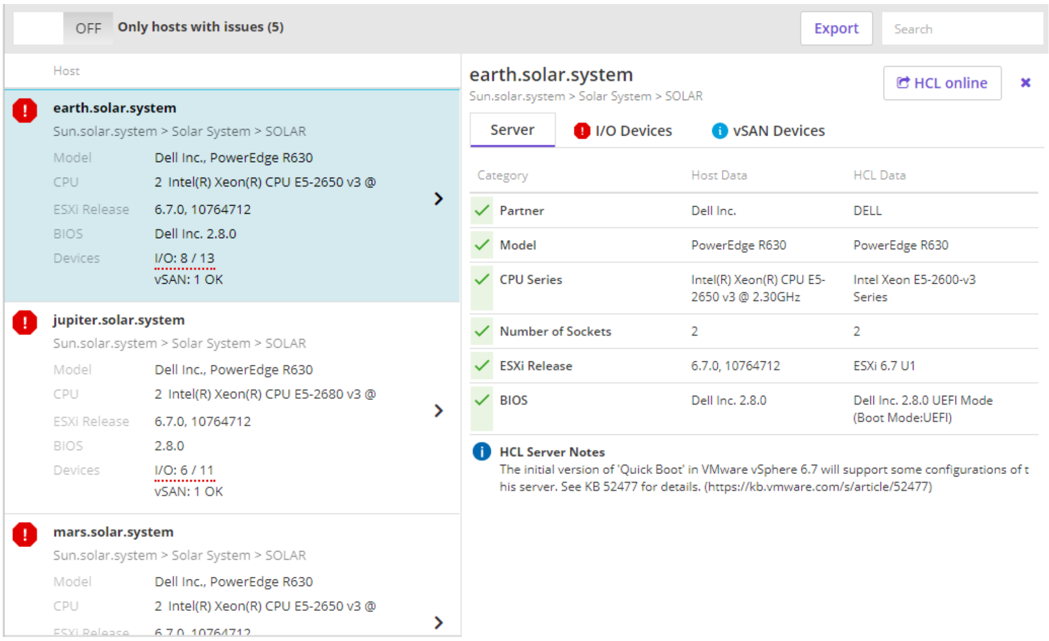
Optionally, you can switch between views of all Hosts or just those with issues by toggling the **ON/OFF** button found in the top bar.

The option to export the report in .csv format is available by using the **Export** button.

For each Host, the name, inventory location, version and build number, model, CPU, BIOS and number of I/O devices are each displayed in separate columns. By clicking on a row, an additional detail panel will appear providing more data. If you want to see detail directly from the VMware HCL webpage you can click on the button labelled **HCL online** which will open a new browser tab linked to the specific server selected (if an internet connection is not available a message will be displayed).

The detail panel is divided into tabs:

- Server - contains a summary of the data retrieved from the ESXi host (Host Data) and data found in the HCL (HCL Data) against multiple categories. Evaluation is done sequentially starting with Partner data and continuing with Model, CPU series, down to BIOS. On a mismatch between Host Data and HCL Data the evaluation process will stop, and a red exclamation symbol will be displayed to indicate a possible incompatibility. The data also provides other known/supported options if these are available from the HCL. Information collected from the Host will still be shown for all categories.



Host

earth.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2650 v3 @
ESXi Release	6.7.0, 10764712
BIOS	Dell Inc. 2.8.0
Devices	I/O: 8 / 13 vSAN: 1 OK

jupiter.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2680 v3 @
ESXi Release	6.7.0, 10764712
BIOS	2.8.0
Devices	I/O: 6 / 11 vSAN: 1 OK

mars.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2650 v3 @
ESXi Release	6.7.0, 10764712

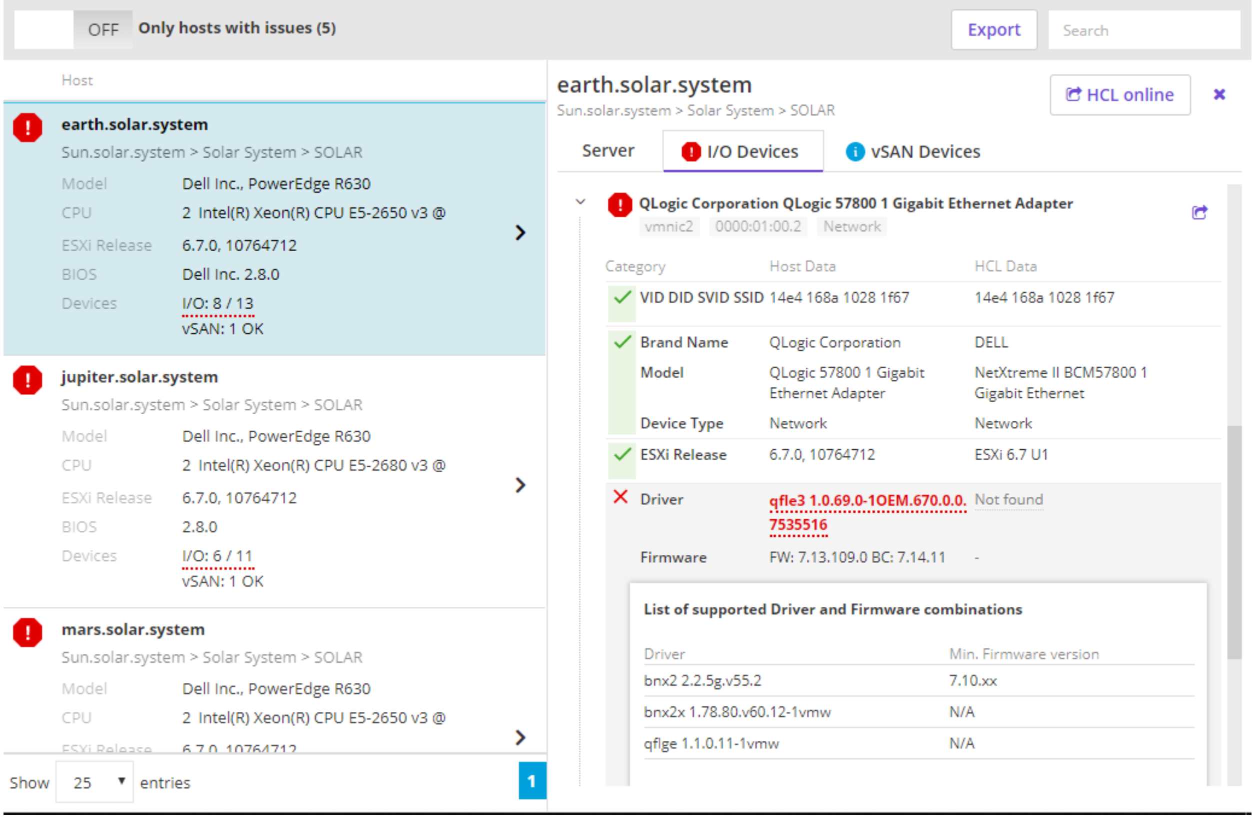
earth.solar.system
Sun.solar.system > Solar System > SOLAR

	Category	Host Data	HCL Data
✓	Partner	Dell Inc.	DELL
✓	Model	PowerEdge R630	PowerEdge R630
✓	CPU Series	Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz	Intel Xeon E5-2600-v3 Series
✓	Number of Sockets	2	2
✓	ESXi Release	6.7.0, 10764712	ESXi 6.7 U1
✓	BIOS	Dell Inc. 2.8.0	Dell Inc. 2.8.0 UEFI Mode (Boot Mode:UEFI)

HCL Server Notes
The initial version of 'Quick Boot' in VMware vSphere 6.7 will support some configurations of t his server. See KB 52477 for details. (https://kb.vmware.com/s/article/52477)

- I/O Devices – contains a list of all I/O devices present on the server selected. Compatibility states are shown using a green (compatible) or red (possibly incompatible) symbol. For each device, specific information about the PCI address and other technical IDs are shown. If you want to see the detail on the VMware HCL webpage you can click on the button ↗ to open a new browser tab linked specifically for the device.

To expand a specific device to view its detail, click on the name or › symbol. You will be shown evaluation results concerning the HCL Data. The evaluation sequence uses categories starting with IDs, Brand Name, Model, Device Type and continuing with ESXi Release and Driver, Firmware. If there is a mismatch between Host Data and HCL Data the evaluation will stop, showing a red symbol to indicate a possible incompatibility. You will also be shown known/supported options if these are available (information collected from the Host will still be shown for all categories).



earth.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2650 v3 @
ESXi Release	6.7.0, 10764712
BIOS	Dell Inc. 2.8.0
Devices	I/O: 8 / 13 vSAN: 1 OK

jupiter.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2680 v3 @
ESXi Release	6.7.0, 10764712
BIOS	2.8.0
Devices	I/O: 6 / 11 vSAN: 1 OK

mars.solar.system
Sun.solar.system > Solar System > SOLAR

Model	Dell Inc., PowerEdge R630
CPU	2 Intel(R) Xeon(R) CPU E5-2650 v3 @
ESXi Release	6.7.0, 10764712

earth.solar.system
Sun.solar.system > Solar System > SOLAR

QLogic Corporation QLogic 57800 1 Gigabit Ethernet Adapter
vmnic2 0000:01:00.2 Network

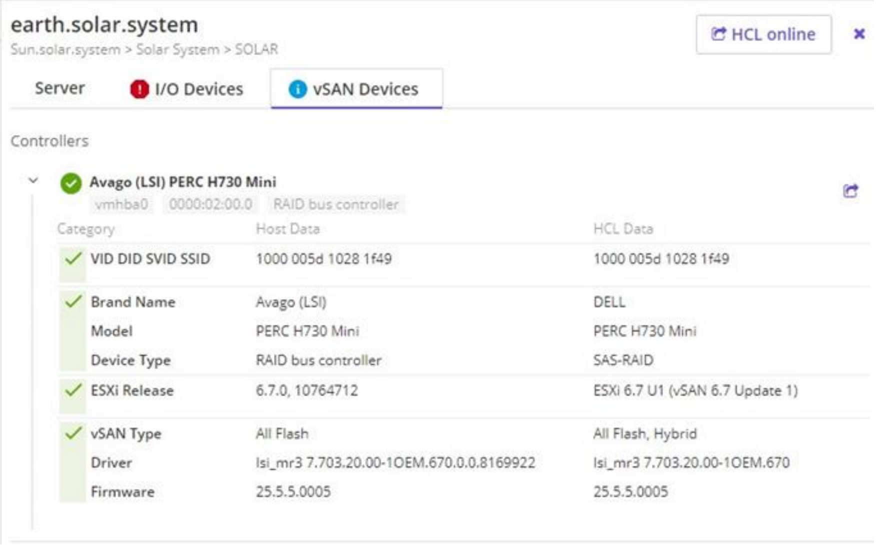
	Category	Host Data	HCL Data
✓	VID DID SVID SSID	14e4 168a 1028 1f67	14e4 168a 1028 1f67
✓	Brand Name	QLogic Corporation	DELL
	Model	QLogic 57800 1 Gigabit Ethernet Adapter	NetXtreme II BCM57800 1 Gigabit Ethernet
	Device Type	Network	Network
✓	ESXi Release	6.7.0, 10764712	ESXi 6.7 U1
✗	Driver	qfle3 1.0.69.0-1OEM.670.0.0.7535516	Not found
	Firmware	FW: 7.13.109.0 BC: 7.14.11	-

List of supported Driver and Firmware combinations

Driver	Min. Firmware version
bnx2 2.2.5g.v55.2	7.10.xx
bnx2x 1.78.80.v60.12-1vmw	N/A
qflge 1.1.0.11-1vmw	N/A

- vSAN Devices – this tab will be available only when vSAN is configured. Contains two sections, one displaying the **Controllers** and the second one presenting information related to **Disk Groups**.
    - Controllers - compatibility states are shown using a green (compatible) or red (possibly incompatible) symbol. For each controller, specific information about name, type and other technical IDs are shown. If you want to see the detail on the VMware HCL webpage you can click on the button ↗ to open a new browser tab linked specifically for the device.

      To expand a specific device to view its detail, click on the name or symbol. You will be shown evaluation results concerning the HCL Data. The evaluation sequence uses categories starting with IDs, Brand Name, Model, Device Type and continuing with ESXi Release and vSAN Type, Driver, Firmware. If there is a mismatch between Host Data and HCL Data the evaluation will stop, showing a red symbol to indicate a possible incompatibility. You will also be shown known/supported options if these are available (information collected from the Host will still be shown for all categories).



earth.solar.system

Sun.solar.system > Solar System > SOLAR

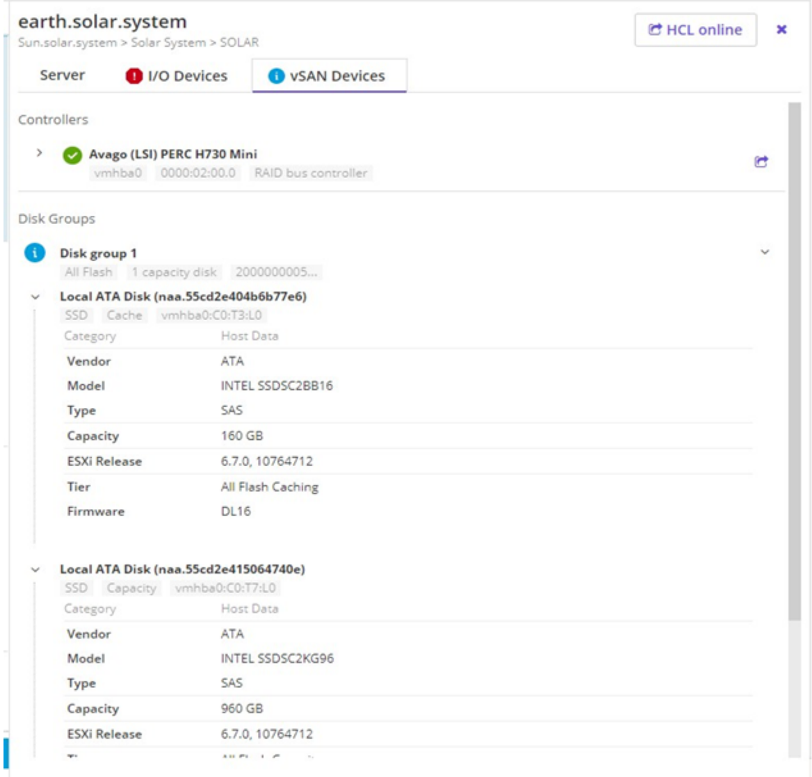
Controllers

✓ Avago (LSI) PERC H730 Mini

vmhba0 | 0000:02:00.0 | RAID bus controller

Category	Host Data	HCL Data
✓ VID DID SVID SSID	1000 005d 1028 1f49	1000 005d 1028 1f49
✓ Brand Name	Avago (LSI)	DELL
Model	PERC H730 Mini	PERC H730 Mini
Device Type	RAID bus controller	SAS-RAID
✓ ESXi Release	6.7.0, 10764712	ESXi 6.7 U1 (vSAN 6.7 Update 1)
✓ vSAN Type	All Flash	All Flash, Hybrid
Driver	lsi_mr3 7.703.20.00-1OEM.670.0.0.8169922	lsi_mr3 7.703.20.00-1OEM.670
Firmware	25.5.5.0005	25.5.5.0005

- Disk Groups – are displayed without any compatibility evaluation and are providing informative data ⓘ about each group and its disks.



earth.solar.system

Sun.solar.system > Solar System > SOLAR

Controllers

✓ Avago (LSI) PERC H730 Mini

vmhba0 | 0000:02:00.0 | RAID bus controller

Disk Groups

Disk group 1

All Flash | 1 capacity disk | 2000000005...

Local ATA Disk (naa.55cd2e404b6b77e6)

SSD | Cache | vmhba0:C0:T3:L0

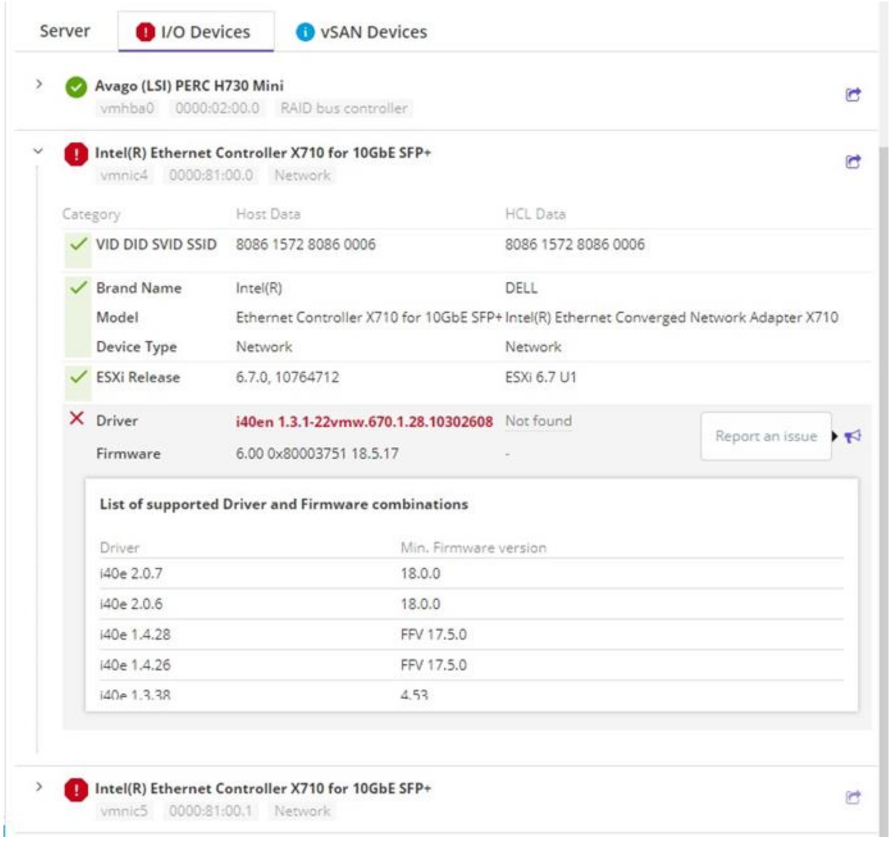
Category	Host Data
Vendor	ATA
Model	INTEL SSDSC2BB16
Type	SAS
Capacity	160 GB
ESXi Release	6.7.0, 10764712
Tier	All Flash Caching
Firmware	DL16

Local ATA Disk (naa.55cd2e415064740e)

SSD | Capacity | vmhba0:C0:T7:L0

Category	Host Data
Vendor	ATA
Model	INTEL SSDSC2KG96
Type	SAS
Capacity	960 GB
ESXi Release	6.7.0, 10764712

On all detail tabs, the far right-hand side of each category contains a button showing a loud-speaker icon 📢 which appears on hover:



Avago (LSI) PERC H730 Mini
vmhba0 0000:02:00.0 RAID bus controller

Intel(R) Ethernet Controller X710 for 10GbE SFP+
vmnic4 0000:81:00.0 Network

Category	Host Data	HCL Data
✓ VID DID SVID SSID	8086 1572 8086 0006	8086 1572 8086 0006
✓ Brand Name	Intel(R)	DELL
Model	Ethernet Controller X710 for 10GbE SFP+	Intel(R) Ethernet Converged Network Adapter X710
Device Type	Network	Network
✓ ESXi Release	6.7.0, 10764712	ESXi 6.7 U1
✕ Driver	i40en 1.3.1-22vmw.670.1.28.10302608	Not found
Firmware	6.00 0x80003751 18.5.17	-

List of supported Driver and Firmware combinations

Driver	Min. Firmware version
i40e 2.0.7	18.0.0
i40e 2.0.6	18.0.0
i40e 1.4.28	FFV 17.5.0
i40e 1.4.26	FFV 17.5.0
i40e 1.3.38	4.53

Intel(R) Ethernet Controller X710 for 10GbE SFP+
vmnic5 0000:81:00.1 Network

The button is available for both states – compatible or possibly incompatible and gives you the option to report an issue if a match was not made as expected, or a mismatch occurred. If an internet connection is available, clicking the loud-speaker icon will present a window showing the (anonymized) data collected. The button to send the data can then be used to submit. If an internet connection is not available, the window will provide steps to download the file and e-mail to the support team. We very much welcome any feedback.

2.6 LOG ANALYSIS

This section contains views related to log analysis. It provides the log collection status and log issues detected based on the correlation of log entries with KB articles. It also provides more general dashboards displaying common error logs.

2.6.1 Log KBs Discovered

ControlUp Analyzer continuously monitors the logs it receives and is searching for log patterns that are described in various VMware KB articles. The **Log KBs Discovered** view displays a table of issues discovered in the logs within a period of time. The time period is configurable at the top of the page.

It is our recommendation to attend to these issues as a matter of priority, because your environment is already exhibiting symptoms of a particular known issue.

2.6.2 Log Inspector

Along with the documented issues in VMware KBs, ControlUp Analyzer filters and tags common error messages from the logs that may indicate a problem. The tagged log entries are represented in a historical chart that can be examined by the administrator. A smaller navigation chart is located under the main log chart. The navigation chart can be used to change the time range of the displayed logs.

Initially, the chart displays the occurrence frequency of log strings that could indicate a problem, such as **Unableto**, **CouldNot**, **FailedTo**, **Error**, etc. Use the drop-down menu on the left-hand side of the search bar to explore deeper the log messages for that string. Another graph appears that includes the most common predicates containing the selected log string.

Select **shell** to see detailed chart and table listing the shell commands executed on the monitored ESXi hosts.

Use the search bar to filter for log entries based on their syslog-message field (case sensitive).

Use the magnifier icon next to Hostname and Program to filter for specific hostname or program.

Click on the colored square located on the left of **Unableto**, **CouldNot** and other predicates, to exclude the respective log entries from the chart and table.

The filters you create will appear under the top search bar. Use the filter checkbox to enable/disable a filter or use the ***red cross*** to remove it.

2.7 Definition Database

This view shows current knowledge which is used to perform the configuration analysis – Knowledge Base articles, Best Practice checks and Security Hardening checks. This view does not show the actual issues detected in your environment, just the knowledge used for analysis.

2.8 Settings Page

The ControlUp Analyzer settings icon (cog icon) is located on the right-hand side of the top navigation bar. Use this page to configure connections to the virtual infrastructure, scheduled analysis, alerting, logs, filters, licensing and ControlUp Analyzer appliance users.

2.8.1 Connections

Within the Connections tab, you can specify the connection details for vCenter servers (and optionally, NSX Managers) or Horizon Connection Servers in the environment that ControlUp Analyzer will analyze. Server address, port number, username and password are mandatory fields. The account you specify should have the minimum required permissions specified in **System Requirements**. To connect to multiple Systems, add them one by one. For more details please check **Connect to a System and analyze.**

2.8.2 Automatic Scheduler

You can configure automatic scheduling by clicking the **Edit** button. Once automatic scanning is selected, the scanning frequency can be chosen. The **Analyze now** button can be used even when Automated scans are scheduled.

2.8.3 Alerting

The Alerting page can be used to enable email alerting. After each analysis, either manual or automatic, an email containing a report of findings will be sent to the configured recipient(s). SMTP server and port, as well as sender and recipient email addresses are mandatory fields. Multiple recipient email addresses separated by a comma can be added (For example: email1@domain1.com, email2@domain2.com, email3@domain3.com).

2.8.4 Log Analysis

The Log Analysis page can be used to configure log retention and syslog settings for Hosts and VMs. For more information – see 1.3.3 Configure Log Collection.

Use the **Reload** button, located on right-hand side of **Syslog settings on the Hosts and VMs of configured vCenters** to re-fetch the current configuration from all vCenters. A timestamp will indicate when the last fetch was triggered. Also, a re-fetch can be performed individually for each vCenter by clicking the specific ⟳ icon.

2.8.5 Security Compliance

In this section you can choose which security profiles to use for your environment's security compliance.

By default, VMware Security Hardening Guide for vSphere is enabled and active. You can select additional profiles if you need to adhere to other security standards.

2.8.6 User Profile

The User Profile tab can be used to manage the ***Local user*** accounts or to connect ControlUp Analyzer to Active Directory.

2.8.6.1 Local user

The default local user that has access to the ControlUp Analyzer web interface is:

- username: rcuser
- password: ControlUp!

By default **rcuser** is granted with **Admin** role which cannot be changed. Click **Edit user** in the **Actions** column in order to change the default password. N.B. **rcuser** is the only account which cannot be deleted.

An unlimited number of **Local User** accounts can be added. For each user, one of two roles can be selected: **Admin** or **Read-only**.

The **Admin** role has no restrictions – it is able to manage the ControlUp Analyzer without any limitations. It has also permission to create/remove other users with the exception of **rcuser**.

The **Read-only** role has restrictions - it is not able to change any settings or configuration and not able to scan or create/remove other users. This role can *Generate an API access token* with read-only privileges.

2.8.6.2 Active Directory

You can use Active Directory accounts to login to the ControlUp Analyzer web interface. Click **Edit** within the Active Directory section and provide information about your Active Directory setup:

a. **Active Directory (*Enable/Disable*)**

b. **Domain (for example *company.com*)**

c. **Domain Groups – any user/group in the specified domain group will get the specified access (Admin or Read-only) to the ControlUp Analyzer web interface.**

Optionally, you can configure advanced options by clicking on the **Advanced options** link:

d. Use SSL (*Enable/Disable*)

e. URL (the address and port of a domain controller, for example *ldap://dc.company.com*)

f. PORT number

g. Root DN (for example *ou=test,dc=company,dc=local*)

When an AD user is member of both **Admin** and **Read-Only** groups, as configured in ControlUp Analyzer, his privilege level will be set to **Admin**.

[Note] Make sure that DNS is configured. The ControlUp Analyzer should be able to resolve the domain controller name. Make sure that the group you specify for the Domain Group exists in your Active Directory domain. The user **MUST** be able to read members of the group.

2.8.7 Filters

Filters can be used to disable a combination of configuration items and issues from showing in the reports and statistics. Without filters, ControlUp Analyzer will include all configuration items it has access to for all possible issues and best practices. Typically, these are all inventory objects within vCenter and (optionally) NSX Manager or Horizon Connection Server.

There are many use cases for using filters, for example:

- Some of the Security Hardening checks are not part of your specific security policy and you need to exclude them from reports.
- You have several test ESXi hosts that you want to exclude from all reports, or perhaps you want to see only Critical issues detected for those hosts.

Click **Add Filter** to create a new filter. A new filter called **New Filter** appears in the list. Expand **New Filter** and edit its name and description. The filter configuration includes two hierarchical trees:

- The left-hand tree displays the vCenter (and optionally NSX) or Horizon Connection Server inventory with all inventory objects underneath. Select which object this filter will apply to.
- The right-hand tree displays all possible issues organized by type (Knowledge Base, Best Practices, Security Hardening) and severity (Low, Medium, Major, Critical). Select a group of issues the filter will apply to.

Click **Update** once finished. The filter is applied to all views.

Click **Export/Import** button on the top right corner of the Filters view to Export and Import all filters. Choose one of the following options:

- **Export Filters** exports all filters in a downloadable .dat file. This function will not export the inventory objects specified in the filters. Once you import the filters, you would need to specify the objects this filter applies to.
- **Export Filters including objects** exports all filters and objects they apply to in a downloadable .dat file. This function can be used in case you plan to import the filters to a ControlUp Analyzer appliance that is connected to the exact same System.
- **Import Filters** imports filters from a .dat file. Filters have an OFF status once imported. N.B. In the case where the .dat file contains inventory objects, they will be added to the filters only if the System object ID and other object IDs match.

2.8.8 Licenses

In this tab you can add and assign a valid license to your hosts. For more information – see 1.3.2 Licensing ControlUp Analyzer.

2.8.9 Update

Within this tab the update status of ControlUp Analyzer is shown. It is divided into two parts, **Application** and **Knowledge Definition**.

- **Application** (full appliance consisting of updates to the OS, component, application, and also database definitions like KB, BP, SH, etc): The version of the ControlUp appliance currently deployed is displayed. This view differs based on the online/offline update state of the appliance:
  - If the appliance has an internet connection (online) then the application will check if there are any updates available. It will display one of two states: ***Up to date*** or ***Update available***. If the status is ***Update available,*** you can perform manually the update by accessing the ControlUp Analyzer Console Interface (check Note) and navigate to the **Update** section. Otherwise ControlUp Analyzer will automatically apply the updates during the night.
  - If the appliance doesn't have an internet connection (offline) then the status ***You are offline*** is displayed together with a link to the *Customer portal*. When accessing the portal through an internet connected device, expanding the ***Offline updates*** provides access to an *.ISO* file.

Download the file from https://updates.runecast.com/runecast-analyzer-vmware/rcupdate.iso and attach it to you ControlUp Analyzer VM. You can perform manually the update by accessing ControlUp Analyzer Console Interface and navigate to the **Update** section.

[Note] To access the ControlUp Analyzer Console Interface open ControlUp Analyzer VM console and press F1 key to login. Check section **ControlUp Analyzer Console Interface** for additional details.

- **Knowledge Definition (contains only data definition updates for knowledge such as KBs, BPs, SH, etc.):** The last update release date is displayed. The view differs based on the online/offline state of the appliance:
  - If the appliance has an internet connection (online) then the application will check if there are any updates available. It will display one of the following two states: ***Up to date*** or ***Update now***.
  - If the appliance doesn't have internet connection (offline) then ***You are offline*** is displayed together with a link to the ***Customer portal***. When accessing the portal through an internet connected device, expanding the ***Offline updates*** provides access to the *.bin* file. To perform an update, Download the file and then import it into the appliance using the ***Choose File*** button.

[Note] Online application and knowledge definition updates require access to *https://updates.runecast.com*

2.8.10 API Access tokens

ControlUp Analyzer offers a full REST API for custom integration, configuration and reporting.

In order to use the API, an access token is required. The token can be generated in the graphical interface of the ControlUp Analyzer or by sending a POST request to /api/v1/users/local/{username}/tokens

Once generated, the access token needs to be included in the Authorization header of each request. For example, to retrieve data about the vCenters registered in your ControlUp Analyzer appliance, you can use a call similar to:

```
curl -H "Authorization: your_token_here" -X GET https://appliance_IP/rc2/api/v1/vcenters
```

The API reference documentation can be accessed by clicking the API link.

2.9 Tool Tips

Click on the question mark on the right-hand side of the top navigation bar to enable/disable tool tips. Once enabled, question mark icons will appear next to some of the main interface elements. If you hover over an icon you will see a help tip to describe the respective item.

2.10 About ControlUp Analyzer

General information are displayed, such as current version and contact information. If troubleshooting of ControlUp Analyzer is required, you can download a support bundle which contains configuration setting and logs of ControlUp Analyzer and send it to email: AnalyzerSupport@ControlUp.com .

3 ControlUp Analyzer Console Interface

Configuration changes to ControlUp Analyzer appliance can be perform through the ControlUp Analyzer Console Interface. You can re-configure network settings, change the administrative user password and perform updates.

To access the ControlUp Analyzer Console Interface, select the **ControlUp Analyzer VM** and use the vSphere client to open a console from within the Summary tab**.** Within the console, use the **F1** key to login. The default credentials are:

- Username: rcadmin
- Password: admin

Once logged in you will find the following options:

- Network Settings: control the network configuration of the appliance. If DHCP is required set its value to **true.**
- User Settings: administrative user password can be changed in this section.
- Remote Access: control the SSH service status (Enable/Disable).
- Updates: ControlUp Analyzer can be updated in both **Online** and **Offline** mode. The appliance checks for updates every night and applies them automatically if there are available.
    - Online – updates are installed from the online repository.
    - Offline – updates are installed from an offline update bundle (.iso file) by attaching it to the ControlUp Analyzer VM's CD/DVD drive and ensuring it is connected. You can download the latest .iso here: https://updates.runecast.com/runecast-analyzer-vmware/rcupdate.iso.

  The **Check for update and install** button will check and apply updates from the selected repository.

- Logout: ends the current user session and returns to previous menu.

4 Advanced Configuration

This section includes the advanced configuration settings of ControlUp Analyzer and may require console access to the virtual appliance. ControlUp Analyzer runs in a virtual appliance running Ubuntu OS. For security purposes, SSH is disabled by default. You will need to use your vSphere Web Client to navigate to the ControlUp Analyzer VM and open the VM console.

4.1 How to change the rcadmin password

To change the rcadmin password follow the steps below:

1. Open the **ControlUp Analyzer appliance console**
2. Press **F1** and login with **rcadmin** user (default password: **admin**)
3. Navigate to **User Settings** and press **Enter**
4. Set new password and confirm.

4.2 How to replace the self-signed SSL certificate

By default, the connection to the ControlUp Analyzer web interface is encrypted using a self-signed SSL certificate. In case your company policy requires CA signed certificates, you can replace the default one following the steps below:

1. If **SSH** is already **Enabled** on ControlUp Analyzer, please continue with step 7
2. Open the **ControlUp Analyzer appliance console**
3. Login with **rcadmin** user (default password: **admin**)
4. Navigate to **Remote Access** and press **Enter**
5. Select **Enable SSH** and press **Enter**
6. Navigate to **Logout** and press **Enter** to return to previous menu
7. Initiate **SSH session** to ControlUp Analyzer
8. Login with **rcadmin** user (default password: **admin**)
9. In the directory /etc/runecast/cert, rename the existing certificates:

   sudo mv rc2.crt orig.rc2.crt

   sudo mv rc2.key orig.rc2.key

10. Copy the new certificate and key to */etc/runecast/cert*.
    - from the appliance initiate file transfer:

      sudo scp username@remoteHost:/location/your-file.crt /etc/runecast/cert/your-file.crt

      sudo scp username@remoteHost:/location/your-file.key /etc/runecast/cert/your-file.key

    - As an alternative you can copy the certificate files to ControlUp Analyzer using SCP client. Is this case, you will not be able to upload them directly to */etc/runecast/cert/* directory. Initially, they can be placed in the */tmp* directory and then moved with elevated privileges.

      sudo mv /tmp/your-file.crt /etc/runecast/cert/your-file.crt *sudo mv /tmp/your-file.key /etc/runecast/cert/your-file.key*

11. In the directory */etc/runecast/cert* rename the new certificate and key to *rc2.crt* and *rc2.key*

    ```
    sudo mv your-file.crt rc2.crt
    sudo mv your-file.key rc2.key
    ```

12. The copy process of the certificate files to ControlUp Analyzer may not assign the proper permissions. Please review them by using the following command:

    ```
    ls -la /etc/runecast/cert/
    ```

13. If the permissions on your new certificate files are not root:rctomcat run the commands below:

    ```
    sudo chown root:rctomcat cert-file.crt
    sudo chown root:rctomcat key-file.key
    sudo chmod 640 cert-file.crt
    sudo chmod 640 key-file.key
    ```

14. If your key is password-protected (recommended) add rc2.key password into *etc/rctomcat9/server.xml* using following commands:

    ```
    sudo nano /etc/rctomcat9/server.xml
    ```

    ```
    SSLCertificateFile="/etc/runecast/cert/rc2.crt"

    SSLCertificateKeyFile="/etc/runecast/cert/rc2.key"

    SSLPassword="key_password"
    ```

15. Restart the appliance after you install the new certificate

[Note] ControlUp Analyzer supports X.509 certificates to encrypt session information sent over SSL connection.

4.3 How to Use with Proxy Server

ControlUp Analyzer can be configured to use a proxy server facilitating external connectivity. To achieve this, follow one of the two methods described below.

Method 1 - Proxy configuration using script:

1. If **SSH** is already **Enabled** on ControlUp Analyzer, please continue with step 7
2. Open the **ControlUp Analyzer appliance console**
3. Login with **rcadmin** user (default password: **admin**)
4. Navigate to **Remote Access** and press **Enter**

5. Select **Enable SSH** and press **Enter**
6. Navigate to **Logout** and press **Enter** to return to previous menu
7. Initiate **SSH session** to ControlUp Analyzer
8. Login with **rcadmin** user (default password: **admin**)
9. Run the *rcproxy.sh* script:

   ```
   sudo /opt/runecast/scripts/rcproxy.sh
   ```

10. Follow the instructions on the screen

Method 2 - Proxy configuration using REST API.

You can configure proxy via the REST API. One convenient way to do it is via the built-in API browser:

- Navigate to Settings -> API Access tokens.
- Access the API reference link and expand the Configuration list. Select the desired method (PUT, GET, DELETE) for /api/v1/config/system/proxy
- To configure the proxy you need to provide proxy server address, port, user and password. Sample:

  ```
   {
    "authenticated": true,
    "configured": true,
    "password": "password",
    "port": 3128,
    "server": "proxy.example.com",
    "user": "user"
  }
  ```

4.4 How to disable the session timeout for the web interface of ControlUp Analyzer

The web interface of ControlUp Analyzer has a default session timeout value of 15 minutes. For security reasons, it is advised to keep the default. To disable the session timeout, follow the steps below:

1. If **SSH** is already **Enabled** on ControlUp Analyzer, please continue with step 7
2. Open the ControlUp Analyzer appliance console
3. Login with **rcadmin** user (default password: **admin**)
4. Navigate to **Remote Access** and press **Enter**
5. Select **Enable SSH** and press **Enter**
6. Navigate to **Logout** and press **Enter** to return to previous menu
7. Initiate **SSH session** to ControlUp Analyzer
8. Login with **rcadmin** user (default password: **admin**)
9. Edit */etc/runecast/runecast.ini* and uncomment the following line and set also the desired value (true / false):
   session_expires=false

10. Restart the Tomcat service:
    sudo systemctl restart rctomcat9

[Note] Alternatively, you can reboot the appliance, instead of restarting the Tomcat service.

4.5 How to change vCenter heartbeat period configuration of ControlUp Analyzer

Every minute a heartbeat request is sent to each vCenter to check if connection is still available. If the vCenter connection becomes unavailable for any reason it will be reported. The heartbeat is required to determine which vCenters are available for licensing, to show current status and is need also for syslog configuration. If you find the heartbeat to be occurring too frequently you can modify the interval of time to desired value. To change vCenter heartbeat period, follow the steps below:

1. If **SSH** is already **Enabled** on ControlUp Analyzer, please continue with step 7
2. Open the ControlUp Analyzer appliance console
3. Login with **rcadmin** user (default password: **admin**)
4. Navigate to **Remote Access** and press **Enter**
5. Select **Enable SSH** and press **Enter**
6. Navigate to **Logout** and press **Enter** to return to previous menu
7. Initiate **SSH session** to ControlUp Analyzer
8. Login with **rcadmin** user (default password: **admin**)
9. Edit */etc/runecast/runecast.ini* and uncomment the following line and set also the desired value (value is limited to interval 1-30):
   #hb_minutes=1

10. Restart the Tomcat service:
    sudo systemctl restart rctomcat9

[Note] Alternatively, you can reboot the appliance, instead of restarting the Tomcat service.

4.6 How to change ControlUp Analyzer network configuration

Network configuration can be set during .ova deployment. If later changes are needed, they can be performed following one of the next steps:

1. From vApp Options
   - Shut down the ControlUp Analyzer appliance VM
   - Using the vSphere Web Client, right click on the VM and select **Edit Settings**
   - From the newly opened window select **vApp Options**
   - Expand **Networking properties** and edit the **DNS** field to the desired value

- Confirm the changes by clicking **OK** button on the **Edit Settings** window
- Power On the ControlUp Analyzer VM

2. From ControlUp Console Interface
   - Open the **ControlUp Analyzer appliance console**
   - Login with **rcadmin** user (default password: **admin**)
   - Navigate to **Network Settings** and configure the parameters as desired. If **DHCP** is required set its value to **true**

[Note] Once the network properties are reconfigured through the ControlUp Console Interface the network configuration is marked as **Internally managed** and further changes via **vApp Options** will be discarded.

4.7 How to change address of Knowledge updates via config file

To create your own repository and use it as download location for Knowledge updates follow the steps below:

1. If **SSH** is already **Enabled** on ControlUp Analyzer, please continue with step 7
2. Open the **ControlUp Analyzer appliance console**
3. Login with **rcadmin** user (default password: **admin**)
4. Navigate to **Remote Access** and press **Enter**
5. Select **Enable SSH** and press **Enter**
6. Navigate to **Logout** and press **Enter** to return to previous menu
7. Initiate **SSH session** to ControlUp Analyzer
8. Login with **rcadmin** user (default password: **admin**)
9. Create/Edit *runecast.ini* at */etc/runecast* and add the following lines:
   updates_url=https://your_repository_IP/
   updates_file_version=version.txt
   updates_file_updates=kbupdates.bin
   Both files *version.txt* and *kbupdates.bin* should be placed in your repository.
   - *version.txt* – requires the following format (example):
     ```
     appversion=1.8.0.0
     defversion=1.7.7.0
     defdate=2018-06-13
     appdate=2018-06-25
     ```
   - *kbupdates.bin* – can be downloaded from your profile

[Note] If the files are not properly configured the updates will behave as in offline mode.

10. Restart the Tomcat service:
    sudo systemctl restart rctomcat9

4.8 How to enforce support of TLSv1.2 protocol

By default ControlUp Analyzer supports following TLS protocols: TLSv1, TLSv1.1 and TLSv1.2

In case you require TLSv1.2 only, please verify your VMware infrastructure against the KB: *https://kb.vmware.com/s/article/2148819*

If your VMware infrastructure fully support TLSv1.2, you can disable TLSv1 and TLSv1.1 in ControlUp Analyzer using following steps:

1. If **SSH** is already **Enabled** on ControlUp Analyzer, please continue with step 7
2. Open the **ControlUp Analyzer appliance console**
3. Login with **rcadmin** user (default password: **admin**)
4. Navigate to **Remote Access** and press **Enter**
5. Select **Enable SSH** and press **Enter**
6. Navigate to **Logout** and press **Enter** to return to previous menu
7. Initiate **SSH session** to ControlUp Analyzer
8. Login with **rcadmin** user (default password: **admin**)
9. Modify */etc/rctomcat9/server.xml* as follows:
   replace *SSLProtocol="all"* with *SSLProtocol="TLSv1.2"*
10. Restart the Tomcat service:
    sudo systemctl restart rctomcat9

After these actions ControlUp Analyzer will accept only TLSv1.2 connections.

4.9 How to configure remote audit logging

For security purposes you can enable ControlUp Analyzer audit logging. These additional log messages contain information about the user interaction with ControlUp Analyzer such as sign in, sign out, filter creation and more.

You can configure audit login via the REST API. One convenient way to do it is via the built-in API browser:

- Navigate to Settings -> API Access tokens.
- Access the API reference link and expand the Configuration list. Select the desired method (PUT, GET, DELETE) for /api/v1/config/system/audit/syslog
- To configure the remote audit logging you need to provide syslog server address, port and protocol type .
  Sample:

```
 {
  "host": "10.0.0.1",
  "port": 514,
  "protocol": "UDP"
}
```

[Note] Once a remote syslog server is configured the logs are also available locally on the appliance.

5 ControlUp Analyzer vSphere Web Client Plug-in

The ControlUp Analyzer Plug-in is compatible with both **Flex** and **HTML5** versions of vSphere Web Client. The current version of the plug-in displays results triggered from ControlUp Analyzer. Future releases of the plug-in will include even more integration, allowing you to perform additional actions directly from the plug-in's interface.

Prerequisites:

- ControlUp Analyzer 1.6.3.0 .
- vCenter Server 6.0 and later versions.

5.1 Registering the plug-in with vCenter server

ControlUp Analyzer Web Client plug-in is deployed directly from ControlUp Analyzer appliance. The steps required for initial registration or update of the plug-in are provided below:

1. Log in to ControlUp Analyzer
2. Navigate to **Settings** > **vCenter Connection**
3. For each added vCenter Server there is a Web Client plug-in section. Depending on the current status, the plug-in can be either **Not installed, Installed (Update available)** or **Installed**.
4. By expanding the **Action** button from the right side, you can choose the one of the available options. Follow the instructions in the pop-up window. It provides the option to initiate the registration or update process directly from ControlUp Analyzer or to download a customized PowerCLI script

5.2 Plug-in Configuration

After registration, please login to vSphere Web Client, navigate to Administration section and select *Settings* under *Runecast: Software-Defined Expertise*.

Provide the FQDN or IP address of ControlUp Analyzer and provide an API Access Token, then update settings using the dedicated button.

[Note] In order to use the plug-in from both Flex and HTML5 versions of vSphere Web Client, configuration should be performed on each of them.

5.3 Working with the ControlUp Analyzer plug-in

The plug-in introduces an additional tab named **Runecast** under the **Monitor** section of each inventory object (e.g. Host, VM, port group). The issues grid will show all issues related to the object along with their relevant finding values. It will also show detail directly in the interface (such as the relevant VMware KB article).

A view showing all issues for the inventory can be obtained from the main page of the plug-in. From the Flex Web Client the **Runecast** icon is accessible from the **Home** screen and on HTML5 Web Client it is located under **Menu**.

5.4 Unregistering the extension from vCenter Server and cleaning up its files

Unregistering the extension from vCenter Server stops it from being active in the Web Client, but does not clean up its files. This is because of a known VMware limitation.

To unregister the plug-in run the following script:

```
Write-Host ''
Write-Host "Please enter vCenter Server address and login credentials"
Write-Host ''
###Setting up###
$vcenter = Read-Host 'vCenter Server address'
$user = Read-Host 'Username'
$pswd = Read-Host 'Password' -AsSecureString
$creds = New-Object System.Management.Automation.PSCredential($user,$pswd)
Set-PowerCLIConfiguration -InvalidCertificateAction Prompt -Scope Session -Confirm:$false | Out-Null
#Connect to vCenter
Write-Host "Connecting to $vcenter..." -ForegroundColor yellow
$vc = Connect-VIServer -Server $vcenter -Credential $creds
if (!$vc) {
  Write-Host "Connection to $vcenter failed" -ForegroundColor red
} else {
  Write-Host "Successfully connected to $vcenter"
  Write-Host "Runecast Web Client plugin is about to be unregistered from $vcenter" -ForegroundColor
yellow
  do {
    Write-Host "Do you want to continue? (y/n): " -ForegroundColor yellow -NoNewline
    $answer = Read-Host
  } until (($answer -eq 'y') -Or ($answer -eq 'Y') -Or ($answer -eq 'n') -Or ($answer -eq 'N'))
  if (($answer -eq 'y') -Or ($answer -eq 'Y')) {
    Write-Host 'Unregistering Runecast plugin...' -ForegroundColor yellow
    $em = Get-View ExtensionManager
    try {
        $em.UnRegisterExtension("biz.runecast.rc2plugin")
        Write-Host 'Runecast plugin unregistered. Please, log out and log back in to vSphere Web Client'
    } catch { Write-Host $_.Exception.Message -ForegroundColor red }
  }
#Disconnect from vCenter
Write-Host "Disconnecting from $vcenter..." -ForegroundColor yellow
Disconnect-VIServer -Server $vc -Confirm:$false }
```

To clean up the files, and completely remove the plug-in, follow the steps below:

1. Stop vSphere Web Client service(s). For flex, stop the vsphere-client process and for HTML5, stop the vsphere-ui process.
2. Directory clean up
   - For Windows based vCenter Server navigate to:

For version 6.0:
%VMWARE_CFG_DIR%\vsphere-client\vc-packages\vsphere-client-serenity and remove the *biz.runecast.** folder
%VMWARE_DATA_DIR%\vspherewebclientsvc\ and remove the *runecast* folder

For version 6.5 and later:
%VMWARE_CFG_DIR%\vsphere-client\vc-packages\vsphere-client-serenity and remove the *biz.runecast.** folder
%VMWARE_DATA_DIR%\vsphere-ui\ and remove the *runecast* folder

- For VCSA navigate to:

  For version 6.0:
  /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity and remove the *biz.runecast.** folder
  $VMWARE_DATA_DIR/vsphere-client and remove the *runecast* folder

  For version 6.5 and later:
  /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity and remove the *biz.runecast.** folder
  /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity and remove the biz.runecast.* folder
  $VMWARE_DATA_DIR/vsphere-client and remove the *runecast* folder
  $VMWARE_DATA_DIR/vsphere-ui and remove the *runecast* folder

3. Start vSphere Web Client service(s). For flex, start the vsphere-client process and for HTML5, start the vsphere-ui process.

Thank you for using ControlUp Analyzer!