VMware vSphere and Entrust CloudControl

Integration Guide

2024-12-20

Table of Contents

Chapter 1. Introduction

Entrust CloudControl integrates with VMware vSphere by protecting your vCenters and ESXi hosts. CloudControl organizes your vSphere inventory into categories to help you find information about your vSphere deployment. With vSphere, you must keep insiders such as virtual administrators in their “swim lanes.” CloudControl uses role and asset-based access control to help you define who can do what to which objects. It also uses workflows supporting secondary approval for sensitive and high impact operations. Entrust CloudControl identifies configuration errors in VMware vSphere hosts using pre-built assessment frameworks. It uses active remediation and proactive monitoring ensuring ongoing compliance.

1.1. Product configurations

Entrust has successfully tested the integration of Entrust CloudControl with VMware vSphere in the following configurations:

System	Version
VMware vSphere	7.0.3 and 8.0.0
Entrust CloudControl	6.6.0

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- The documentation and setup process for VMware vSphere.
- The documentation and setup process for Entrust CloudControl. The online documentation contains everything needed to successfully install and deploy CloudControl.

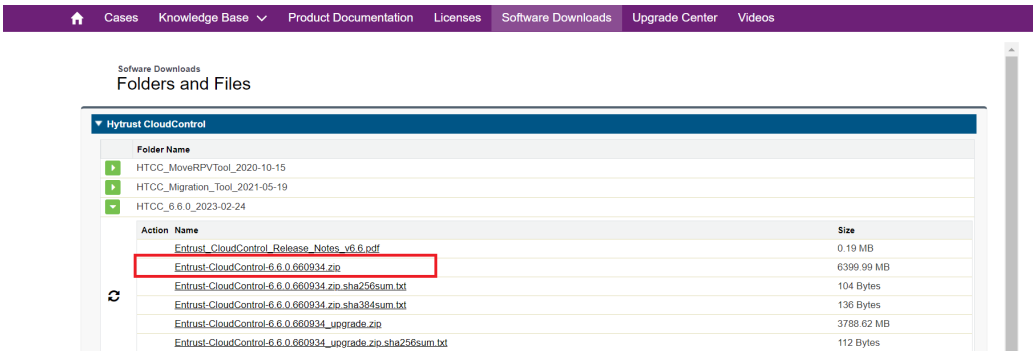
Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Procedures

It is important to note that this guide uses a standalone CloudControl deployment and does not use Active Directory. Users are local to the system. CloudControl was not configured to use Active Directory. CloudControl also supports a cluster environment and this will be documented in the installation guide.

2.1. Download the CloudControl software

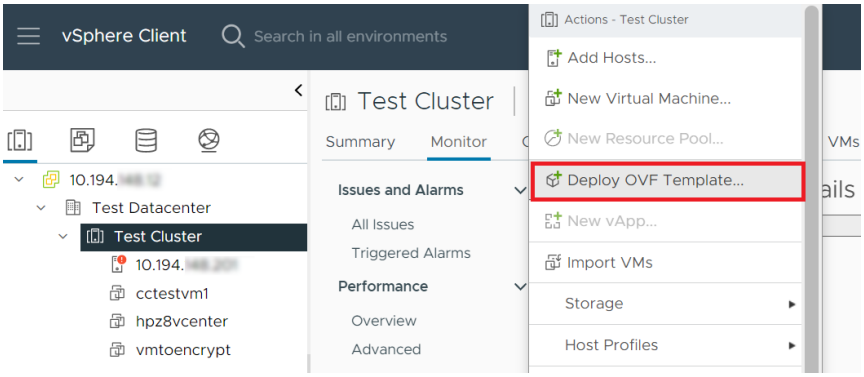
1. Go to https://my.hytrust.com/s/software-downloads.
2. Log in and select **HyTrust CloudControl**.
3. Open the folder `HTCC_6.6.0_2023-02-24`. This folder contains version 6.6.0 that was used in this guide.
4. Select the `Entrust-CloudControl-6.6.0.660934.zip` link to download the file.



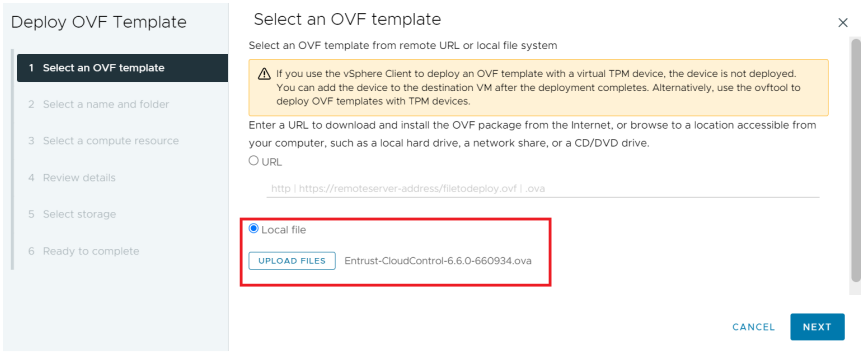
5. Once the file has been downloaded, open the ZIP file to access to the OVA file.

2.2. Deploy the CloudControl VM from the OVA

1. Log in to vCenter.
2. Navigate to **Inventories** > **Hosts and Clusters**.
3. Select the resource pool where you plan to deploy CloudControl.
4. Select **Actions** > **Deploy OVF Template** from vSphere Web Client.



5. On the Select an OVF Template page, select **Local File** and upload the `Entrust-CloudControl-6.6.0-660934.ova` file.



Follow the instructions on Deploying CloudControl as required.

For more information refer to Installing CloudControl from an OVA in the online documentation.

2.3. Power on the appliance

1. Log in to the vSphere Client.
2. Locate the Entrust CloudControl virtual machine in the inventory.
3. Right-click the CloudControl virtual machine and select **Power > Power On**.

2.4. Configure the CloudControl virtual appliance

This guide uses a Standalone Node setup. Follow the online documentation for instructions for Creating a Standalone Node.

2.5. Set up the CloudControl GUI

Once the standalone node has been configured, you must finish the setup using the GUI. Follow the online documentation instructions on Setting Up the CloudControl GUI.

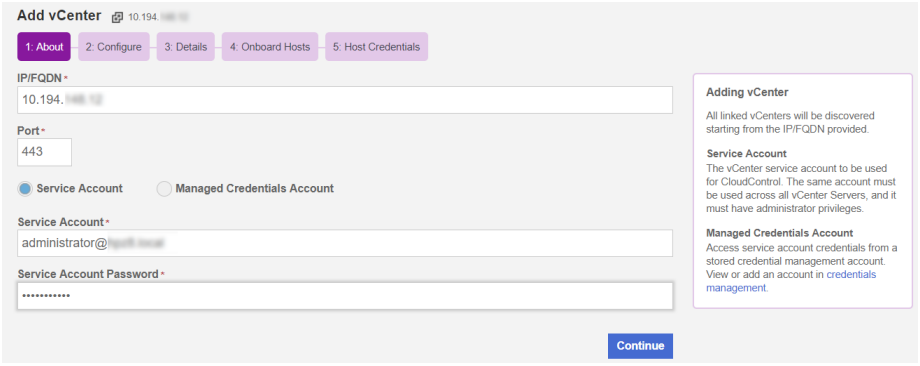
2.6. Add vCenters to CloudControl

You can now add the VMware vSphere inventory into CloudControl.

2.6.1. Add a vCenter to CloudControl

To add a vCenter to CloudControl:

1. From the Home tab, select **Inventory > vSphere**.
2. On the vSphere page, select **Actions > Add vCenter**.



2.6.2. Configure CloudControl after adding a vCenter

To configure CloudControl after adding a vCenter:

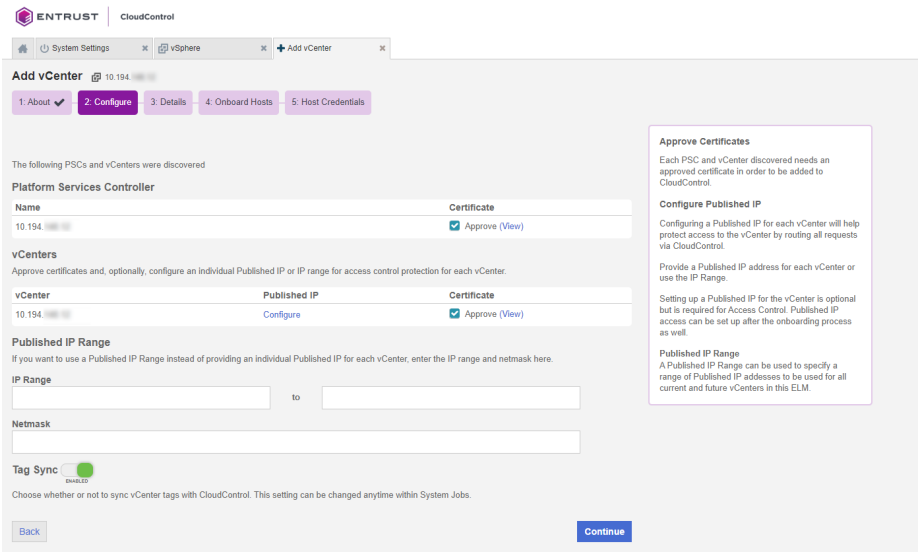
1. On the **Configure page**, view and approve the certificates for the Platform Services Controller (PSC) and all vCenters that were discovered.
2. The **Approve** checkbox must be checked for all certificates before you can add the vCenter.
3. Certificates from a trusted source have the **Approve** checkbox checked automatically.
4. Select the **Certificate** link to view the certificate details.

   Certificates without a certificate authority are displayed with a warning icon. Select the link in the tool tip to add a CA. You can manually approve these certificates by checking the **Approve** checkbox. Certificates that are invalid or expired are displayed with an error icon. These certificates cannot be approved. All vCenter and PSC certificates are displayed on the **Certificate Authorities** tab on the **Certificates** page.

5. Select **Approve** to populate the approve checkbox for the certificate, or select the **x icon** to close the window.
6. Determine if you want to use a single Published IP for each vCenter or a Published IP Range to be used for all current and future vCenters in this ELM.

   If you plan to use Access Control, you must have a Published IP address or range.

7. For a Published IP, select the **Configure** link in the **Published IP** column of the vCenter table, enter the Published IP Address and Netmask, and select **Apply**.
8. For a Published IP Range, enter the **Published IP Address** and **Netmask** in the **Published IP Range** section.
9. Enable **Tag Sync** if you want vCenter Tags in CloudControl.



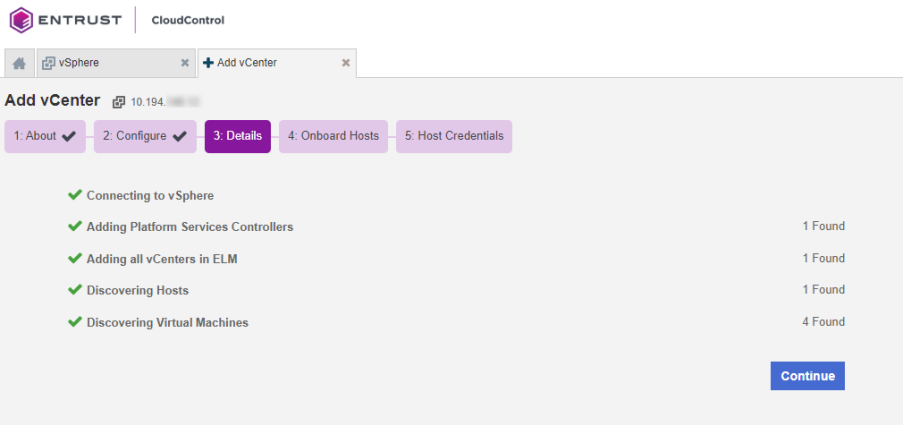
10. When all certificates are approved, select **Continue**.

> You cannot select **Continue** until all of the Approve checkboxes are checked.

Check the online documentation instructions for more detail on Adding vCenters to CloudControl.

2.6.3. View Details

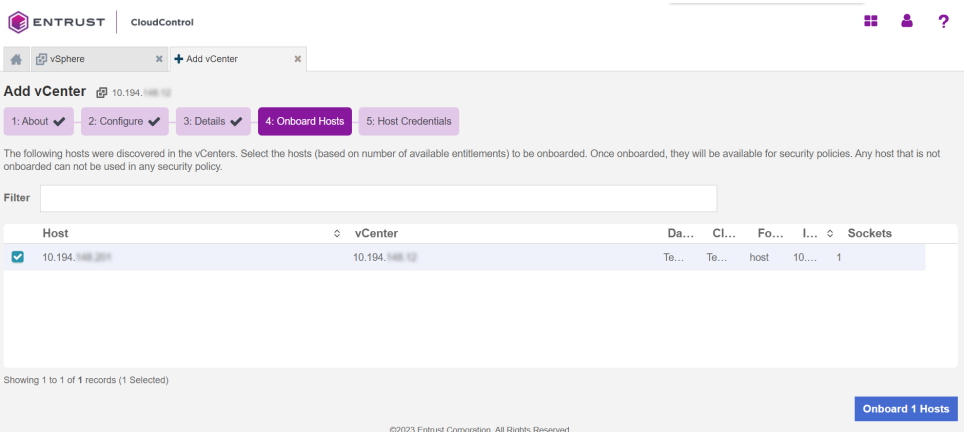
On the **Details** page, you can monitor the process as all of your vSphere information is collected.



2.6.4. Onboard the hosts

On the **Onboard Hosts** page, you can view the hosts that were discovered, remove hosts, or add additional hosts to be added to CloudControl. Select the hosts that you want to add and select **Onboard Hosts**.

You must add hosts before you can run Configuration Hardening policies (assessment and remediation) against your hosts.



2.6.5. Host credentials

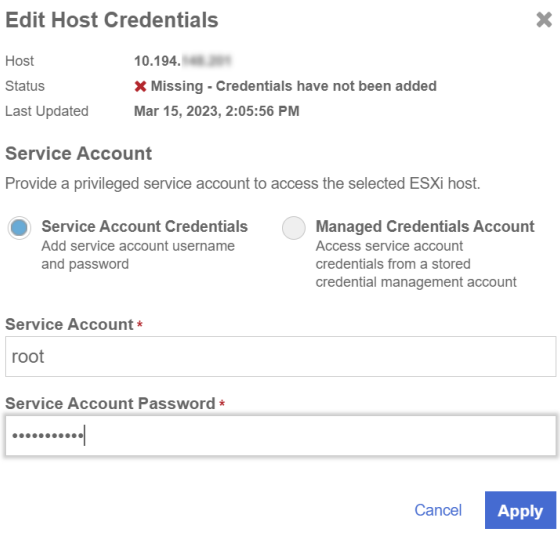
On the **Hosts Credentials** page, you can add or import the credentials for your ESXi hosts.

2.6.5.1. Add credentials

To add credentials:

1. Select one or more ESXi hosts that share the same credentials and select the **Missing** link in the Credentials column.

2. In the **Add Host Credentials** window, enter the User Name and Password for the ESXi hosts and select **Apply**.



The **Credentials** column for each host shows the host status. This can be one of the following:

- Missing
- Valid
- Invalid

> You may encounter an Invalid Certificate when adding the Host Credentials. To resolve this issue, the vCenter root CA must be imported into the CloudControl's Certificate Authorities. Check [procedures:::certificate-invalid] for troubleshooting.

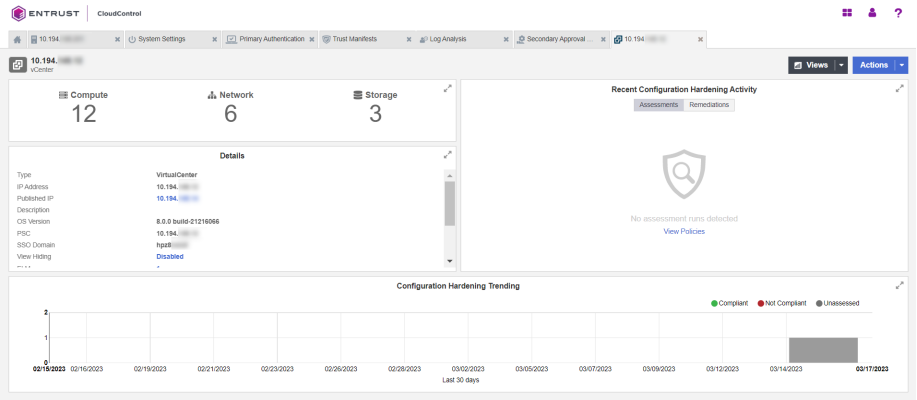
2.6.5.2. Import credentials

To import credentials, you must upload a CSV file in the following format: ESXINAME FQDN, PASSWORD, USERNAME:

1. Select one or more ESXi hosts that share the same credentials and select **Import Credentials**.
2. Select the file that you want to import and select **Continue**.
3. Review the summary on the **Discovered** page.
4. Select **Apply**.

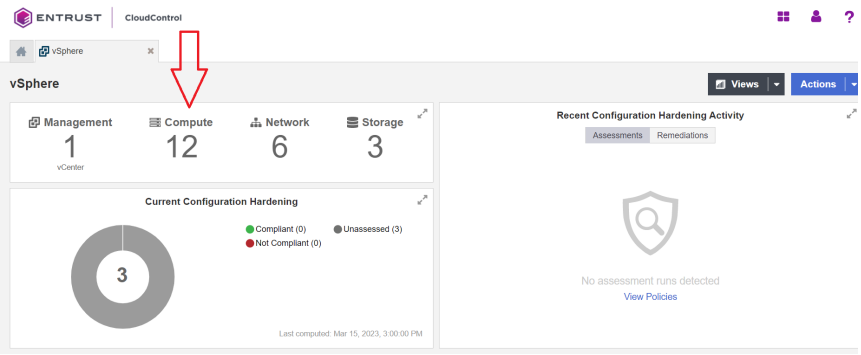
> If you do not add the credentials, then you cannot run Configuration Hardening policies (assessment and remediation) against your hosts.

5. After you have added the credentials, you can enable Global PIP. Global PIP is disabled by default. For more information, see Enable Global PIP.
6. Select **Continue**.
7. Select **Done** to view the dashboard for the newly added vCenters.

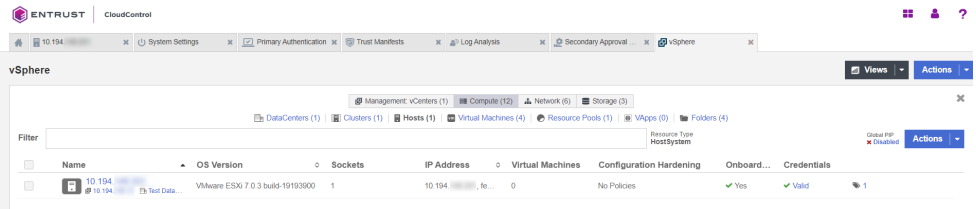


2.7. Enable Global PIP

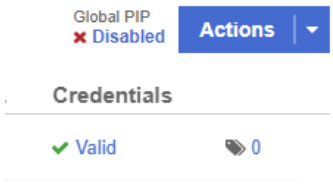
1. From the **Home** tab, select **Inventory > vSphere**.
2. On the vSphere page, select the **Compute** link.



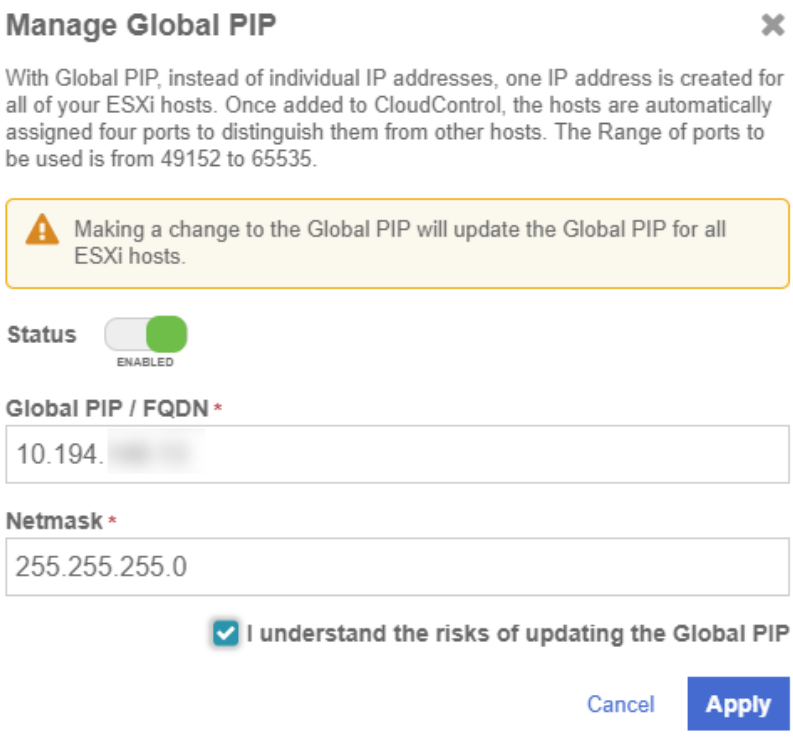
3. On the **Compute** tab, select the **Hosts** link.



4. On the **Hosts** page, next to the **Actions** button, select the **Global PIP Disabled** link.



5. Alternatively, you can select one or more hosts and select **Actions > Manage Global PIP**.
6. In the **Manage Global PIP** window, do the following:
   a. Set the **Status** to **Enabled**.
   b. For **Global PIP / FQDN**, enter the IP address or FQDN to use for the Global PIP.
   c. Enter the **Netmask**.
   d. Check the **confirmation** checkbox.
   e. Select **Apply**.



Global PIP is now enabled for all hosts that have been added to CloudControl.

Select **Download CSV** to download a CSV file that contains the details of all assigned ports.

Follow the online documentation to view the assigned ports for Global IP.

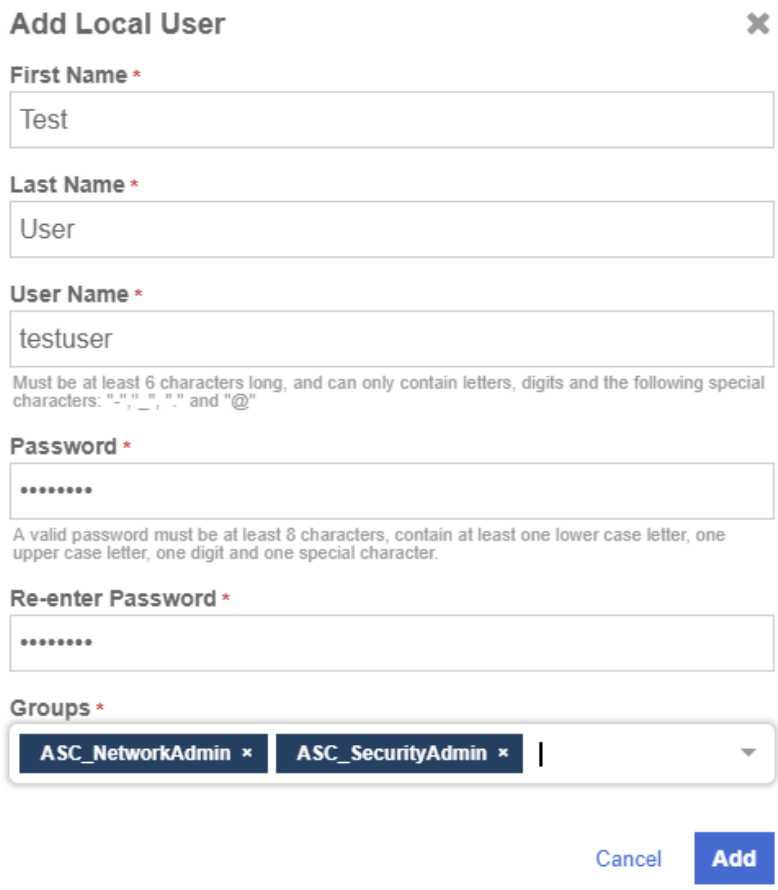
For more details, view the online documentation on Enabling Global PIP.

2.8. Add local users to the system

If you are not using AD, you can add local users to the system so they can be used to log in to vCenter and ESXi hosts using the Published IP address for the vCenter and GPIP for the ESXi hosts.

To create a local user to the following:

1. From the **Home** tab, select **System > Primary Authentication**.
2. Select the **Add** button.
3. In the **Add Local User** window, fill the information accordingly:



You can select one or more groups for the user.

For more details, view the online documentation on Adding Local Users.

2.9. Test the vCenter Published IP (PIP) and ESXi Hosts Global IP (GPIP) address and ports

2.9.1. vCenter Published IP (PIP)

Once the vCenter Published IP is set/enabled, you can test it by pointing your browser to:

```
https://PIP
```

2.9.2. ESXi Global IP (GPIP) and ports

When you know the ports that were assigned when you enabled GPIP, you can log in to any ESXi using the GPIP and the https_port:

```
https://GPIP:https_port
```

2.9.3. More information

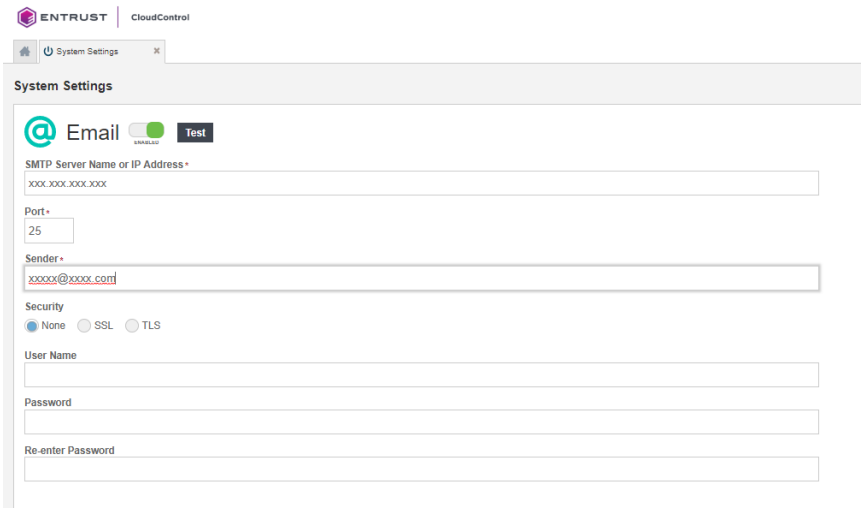
Check the online documentation for more details on connecting to the ESXi hosts using the GPIP.

If CloudControl is not in AD mode, use one of the local users in CloudControl. If local users have not been created you can use the **superadminuser** local account with the password set during CloudControl configuration. Initially users must be in the **ASC_SuperAdmin** group to be able to log in using GPIP and PIP. You can change this when you implement your own access control policy.

2.10. Configure email

It is important to setup your email settings so the system can provide notification to users when required. Your SMTP and email information settings are configured during installation. You can modify them at any time.

1. From the **Home** tab, select **System > System Settings**.
2. On the **System Settings** page, select **Settings > Email**.
3. On the **Email** page, select **ON** or **OFF** to enable SMTP.
4. Fill in the information according to your settings:



Check the online documentation for more details on how to modify your email settings.

Email notification to users is only available when Active Directory settings are enabled. This integration was performed with local users. Active Directory was not configured.

2.11. View the vSphere inventory

Now that the VMware inventory has been catalogued by CloudControl, check the online documentation on Viewing the vSphere Inventory inside CloudControl.

2.12. Logs

You can look at the logs in the system in the following places:

1. Log Analysis.
2. System Logs.

2.12.1. Log analysis

Go to the **Home** tab, select **Security > Log Analysis**.

Check the online documentation for more information on log analysis.

2.12.2. System logs

To view the system logs page, from the **Home** tab, select **System > System Logs**.

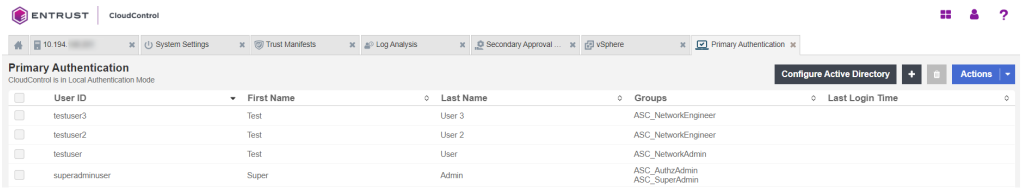
Check the online documentation for more information on system logs.

2.13. Access Control

This section will show how you can use an Access Control Policy to control access to VMware resources in the system. This example creates an access control policy that will allow anyone that belongs to the **ASC_NetworkAdmin** or **ASC_SuperAdmin** group to log in to ESXi hosts in CloudControl. Anyone that doesn't belong to these groups will be denied access. Keep in mind that you also can use tags to constrain the access control policy to only resources that have the specified tags.

2.13.1. Users

Three users were created in the system that will allow to implement and demonstrate the access control policy in action.



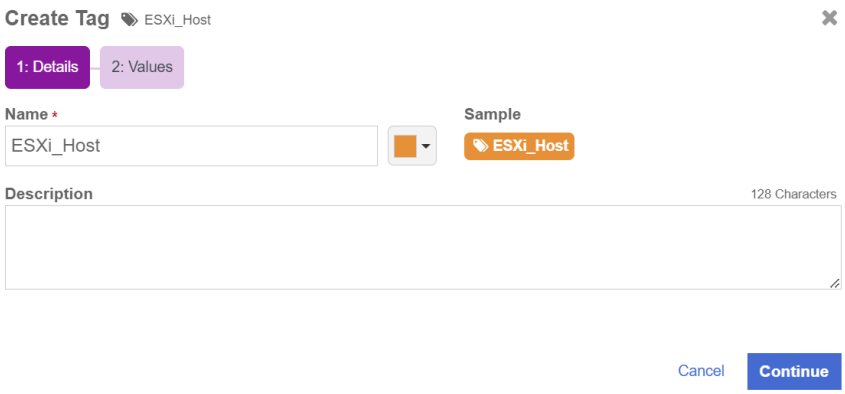
Two users belonging to the **ASC_NetworkEngineer**. One user belonging to the **ASC_NetworkAdmin** group. And lastly, the **superadminuser** (which already existed) which belongs to the **ASC_SuperAdmin** group.

2.13.2. Tags

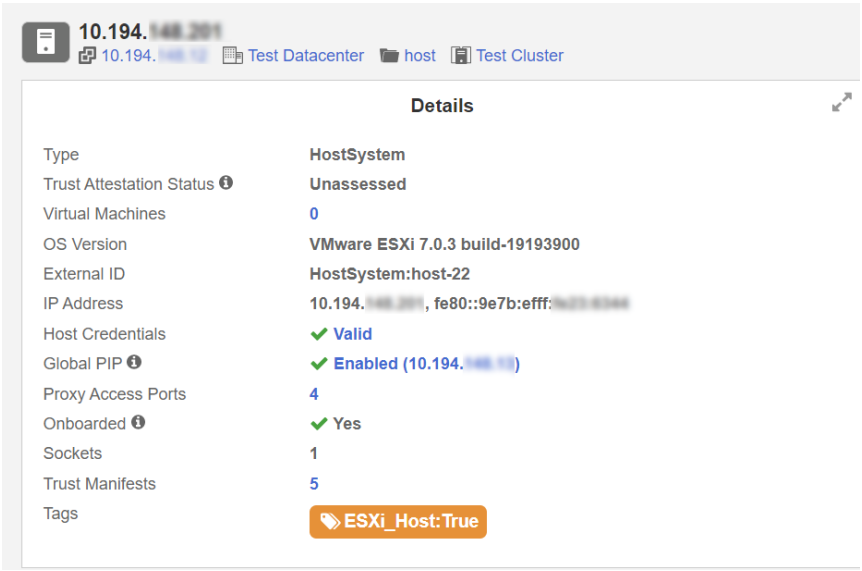
Tags will not be used in the example but here is an example of how to create a tag and assign it to a resource in the system. For instance, once assigned, you could use tags to constrain the access control policy to resources that have the tag.

Check the online documentation for more information on tags.

1. Create a tag called **ESXi_Host**. This will be used to tag the ESXi Hosts in the system.

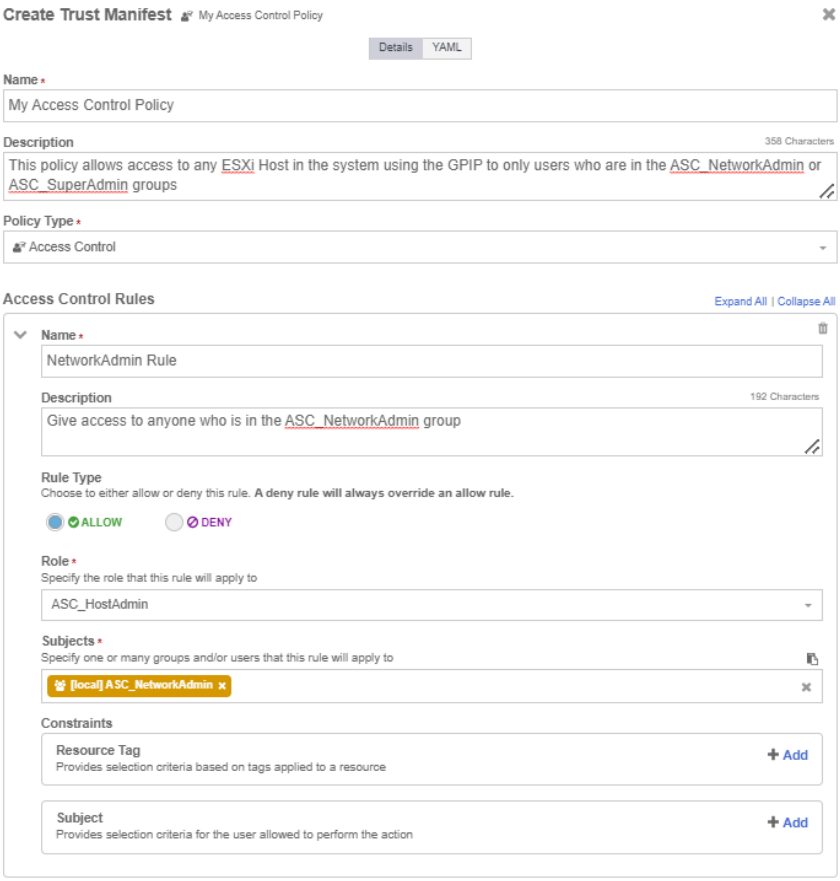


2. Tag the ESXi Hosts with the tag created.
3. Now tag the ESXi Hosts in the system with the **ESXi_Host** tag created.

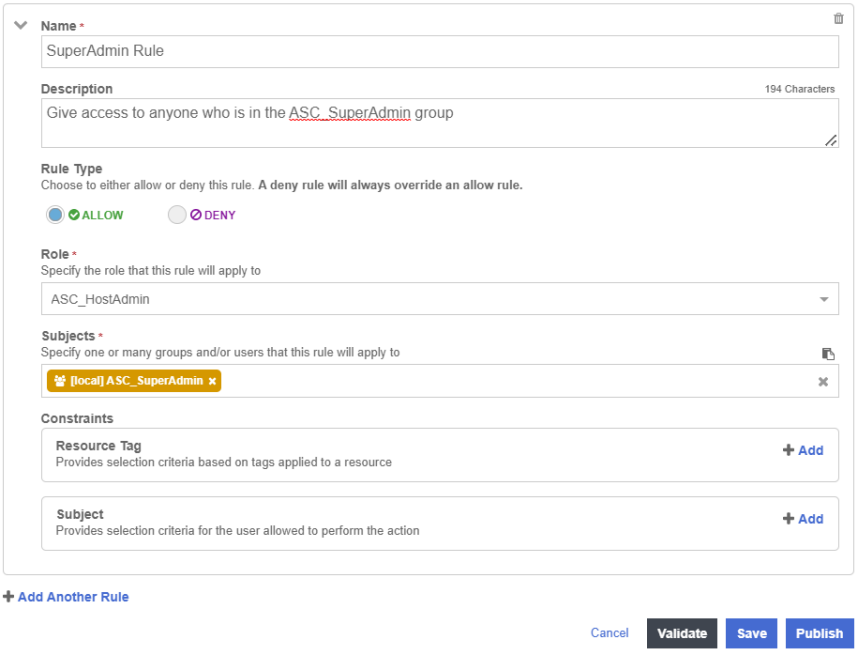


2.13.3. Create and validate the access control policy

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the **Manage Trust Manifests** page, select **Actions > Create Trust Manifest**.
3. On the **Details** tab of the **Create Trust Manifest** page, enter the name and optional description for the trust manifest.
4. For **Policy Type**, select **Access Control**.
5. In the **Access Control Policy** section, create a rule for the NetworkAdmin Group:

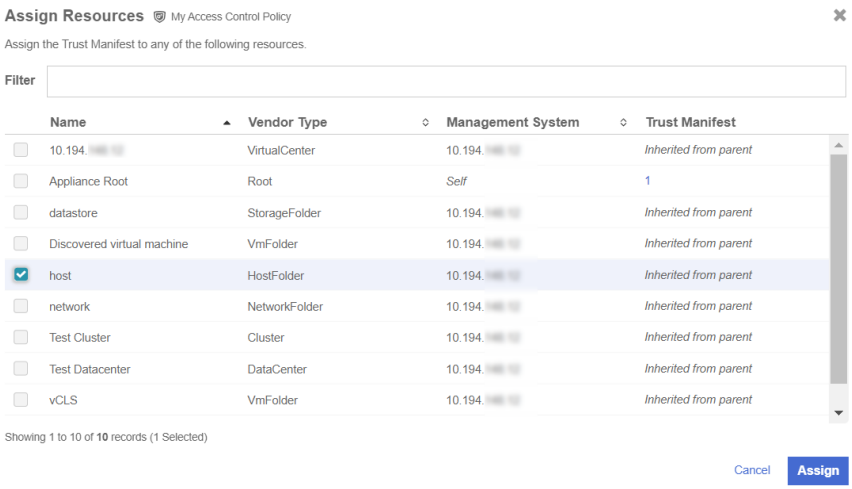


6. Select **Add Another Rule** and add the rule for the SuperAdmin group to the policy.



7. Select **Validate** to validate the policy.
8. Select **Save** to save the policy.

9. Select **Publish** to publish the policy When you publish the policy it will ask you to assign resources to the policy. Select **host** and select **Assign**.



10. Select **Close**.

Check the online documentation for more details on Creating an Access Control Trust Manifest from the CloudControl GUI.

2.13.4. Test the Access Control Policy

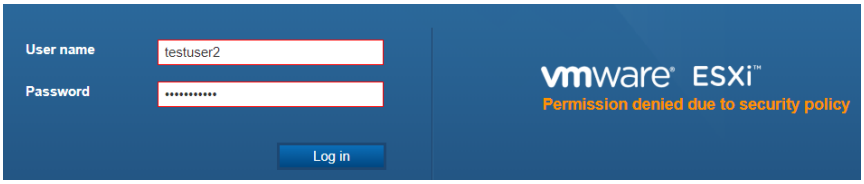
When the access control policy is in place, point your browser to the GPIP address of the ESXi host and see if you can log in.

- Success:

  Login should be successful for the **superadminuser** and **testuser**.

- Failure:

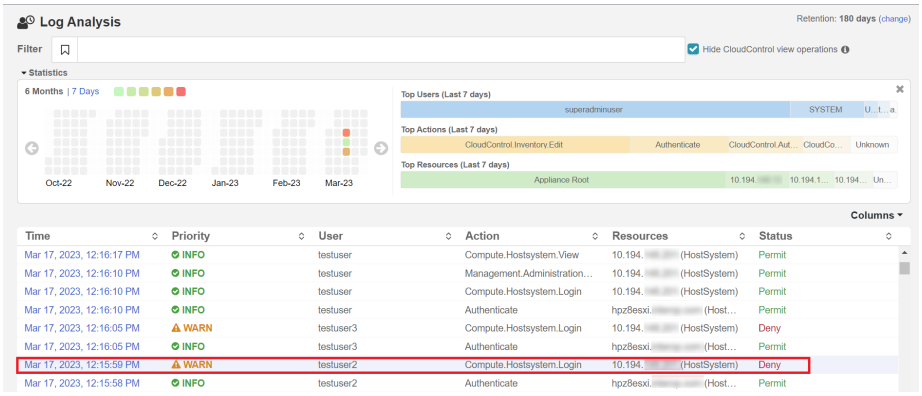
  Login should fail for the **testuser2** and **testuser3** local users.



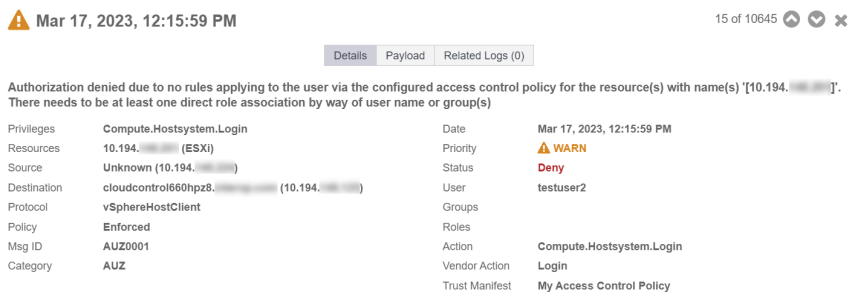
2.13.5. Logs

You can use the Logs in the system to check why access has been denied to a user. In the example, **testuser2** has been denied access. You can view the logs to see the reasons.

1. From the **Home** tab, select **Security > Log Analysis**.



2. Select the record that shows the **Deny** status to see the reason for the denial.



3. You will be able to see the **My Access Control Policy** was used to control the access.

2.14. Secondary Approval

Use Secondary Approval to configure CloudControl to require additional approval before users can perform selected disruptive operations on a resource. For example, you can require secondary approval before deleting or powering off a virtual machine or vApp, editing a firewall, or creating an Edge gateway service.

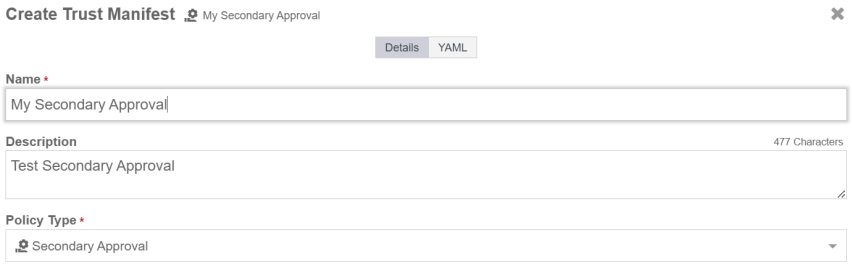
When a user attempts to perform a vSphere operation that requires secondary approval, the operation fails with a notification that secondary approval is required, and that a request was generated.

If you have SMTP configured, and the users or groups have an email address in AD, then email messages are generated.

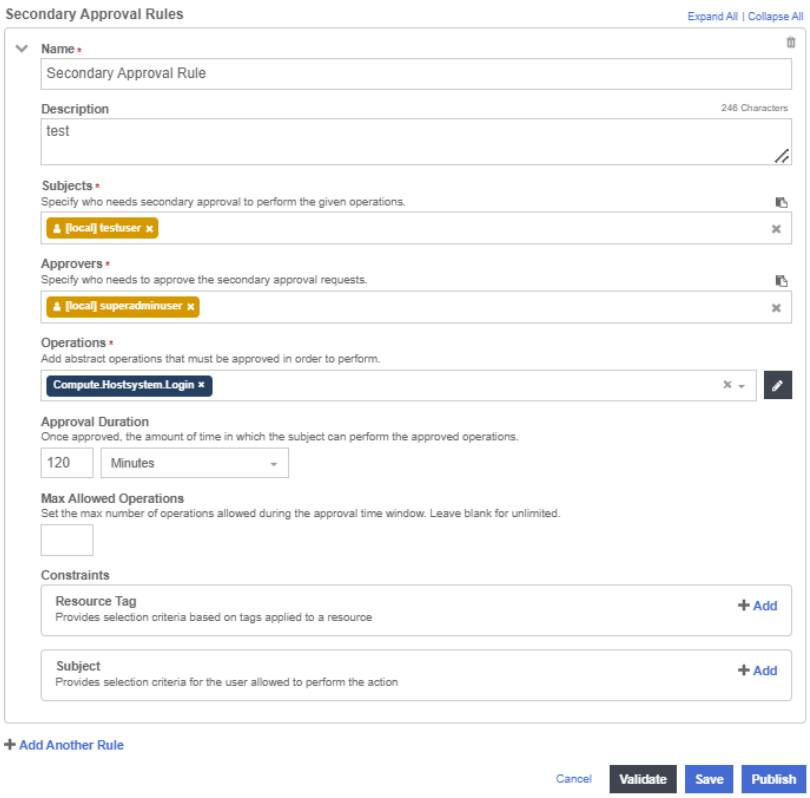
This example will require the user **testuser** a secondary approval to log in to any ESXi host.

2.14.1. Create a Secondary Approval Trust Manifest from the CloudControl GUI

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the **Manage Trust Manifests** page, select **Create Trust Manifest** (The Plus sign in the GUI).
3. On the **Details** tab of the **Create Trust Manifest** page, enter the name and optional description for the trust manifest.
4. For **Policy Type**, select **Secondary Approval**.



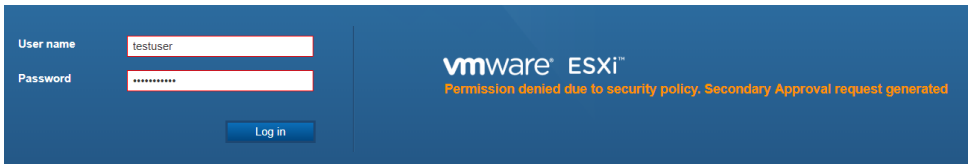
5. In the **Secondary Approval Policy** section, complete according to the image below:
   a. Select the **testuser** as the subject.
   b. Select the **superadminuser** as the approver.
   c. Select the **Compute.Hostsystem.Login** as the operation.



6. **Publish** the policy.
7. When you publish the policy you must assign resources to it. Select **host** as the resource. This will make policy applicable to any ESXi host in the system.

2.14.2. Validate Secondary Approval Policy

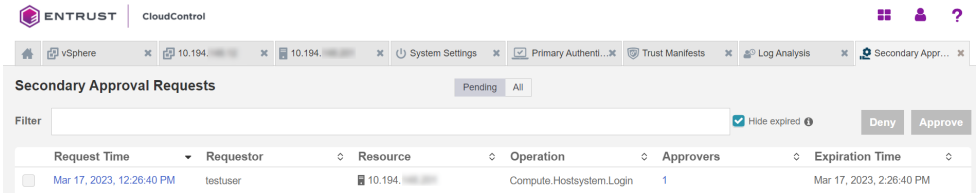
When the secondary approval policy is in place, point your browser to the GPIP address of the ESXi host and see if you can log in. Log in with the user that you used in the policy definition. The attempt should fail.



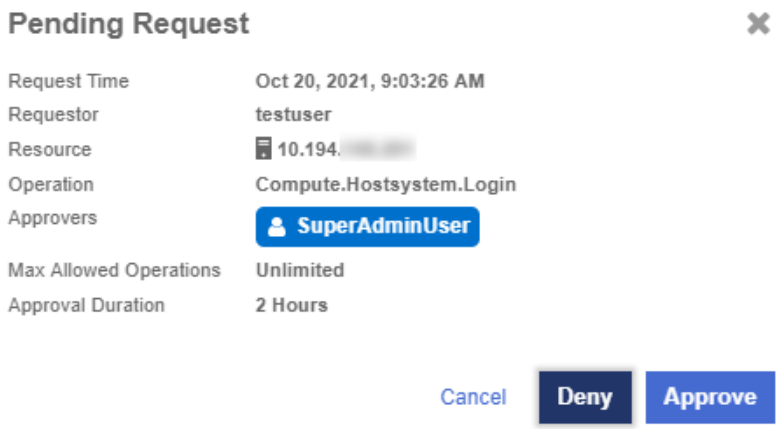
2.14.3. Approve the secondary approval request

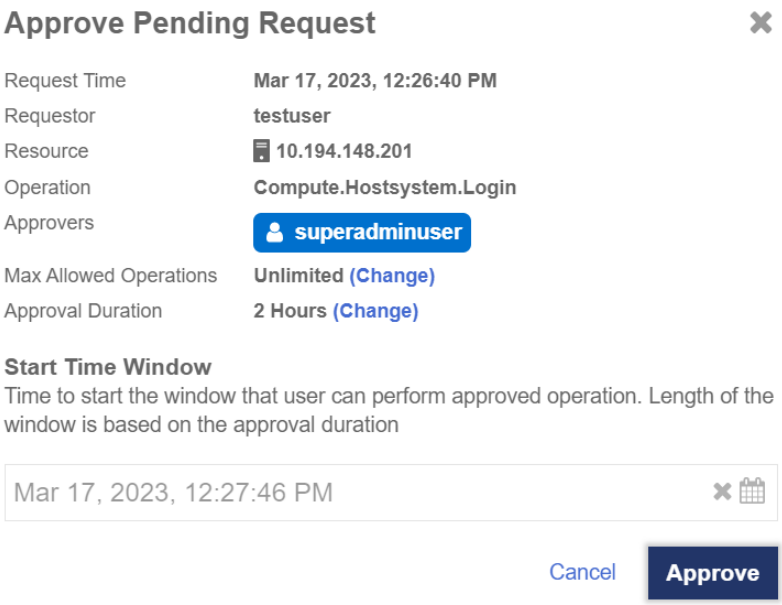
Approve the secondary approval so that the user can log in to the ESXi Host.

1. From the **Home** tab, select **Security > Secondary Approval Requests**.
2. On the **Secondary Approval Requests** page, select a tab to view **Pending** or **All** requests.



3. (Optional) Select **Approve** for a pending request to approve the request.





4. (Optional) Select **Deny** for a pending request to reject the request.

2.14.4. Attempt to log in after approval

After the secondary approval request is approved, log in:

Point your browser to the GPIP address of the ESXi host and see if you can log in. Log in with the user that you used in the policy definition. The attempt should be successful.

2.15. Configuration Hardening

Configuration hardening allows you to improve the security posture of your vSphere environment by hardening the configuration to meet either your company's specific security policy, industry best practices such as CIS or NIST, or compliance standards such as PCI or HIPAA. By automating the hardening process, you can reduce your operational burden during a compliance audit.

With CloudControl, you can:

- Create and customize templates to use in configuration hardening checks.
- Assess and remediate your environments against the configuration hardening checks defined in the templates.
- Review dashboards, reports and alerts to monitor the results of assessments and remediations.

2.15.1. About Templates

CloudControl uses templates to support all Configuration Hardening activities. CloudControl supports the following types of templates:

- **Catalog templates**—Read-only collection of hardening operations. There is a vSphere operations catalog of templates that you can use.
- **System templates**—Read-only collection of operations derived from a catalog template for a given compliance standard For example, the vSphere - HIPAA Security Standards template is derived from the vSphere operations catalog template.
- **Custom templates**—Templates created by users. In most cases, they are copied or cloned from existing system or catalog templates. Custom templates can be modified and used in configuration hardening policies.

CloudControl also includes sample custom templates that can immediately be used in a policy.

Templates can contain both assessment and remediation hardening operations. It is recommended that you review all operations in the template to ensure that any parameter values are set to those that appropriate for your infrastructure requirements.

2.15.2. About Policies

Configuration Hardening Policies are used to run custom templates. Each policy associates a template with one or more resources or tag-based resource configurations, and can be run manually or as a scheduled activity. Policies can either assess or remediate a resource, but cannot do both.

2.15.3. More information

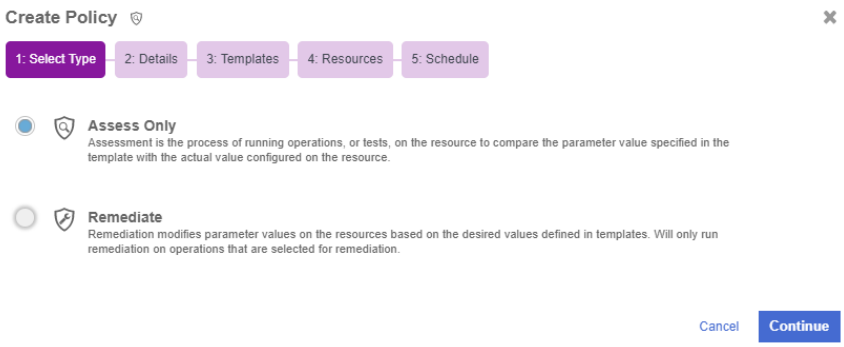
Consult the online documentation for more information on Configuration Hardening.

2.15.4. Creating a Configuration Hardening Policy Example

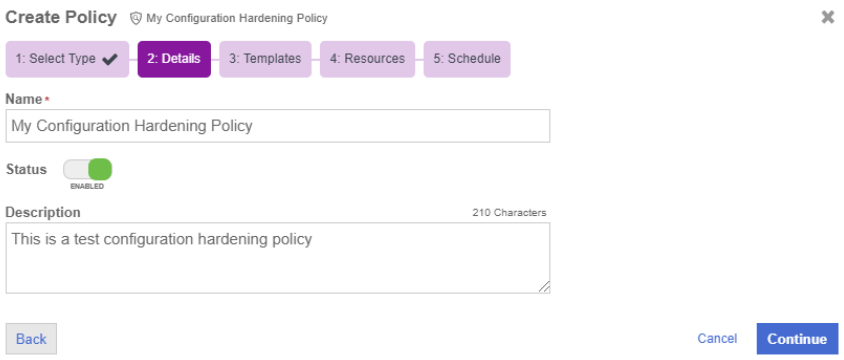
For this guide a configuration hardening policy will be created based on one of the templates available. Enforcement will be based on a rule in the template to check and make sure the ESXi vSphere version is at least version 7 and above.

1. From the **Home** tab, select **Security > Configuration Hardening**.
2. On the **Configuration Hardening Management** page, select the **Policies** tab.

3. Select the **Create (+)** button.
4. In the **Create Policy** wizard on the **Select Type** page, select the type of policy that you want to create. This can be one of the following:
    - **Assess Only** - Runs operations on the host to compare the parameter values specified in the template with the actual values on the host.
    - **Remediate Only** - Modifies the parameter values on the host in order to match the values specified in the templates.
5. Select **Assess Only**.

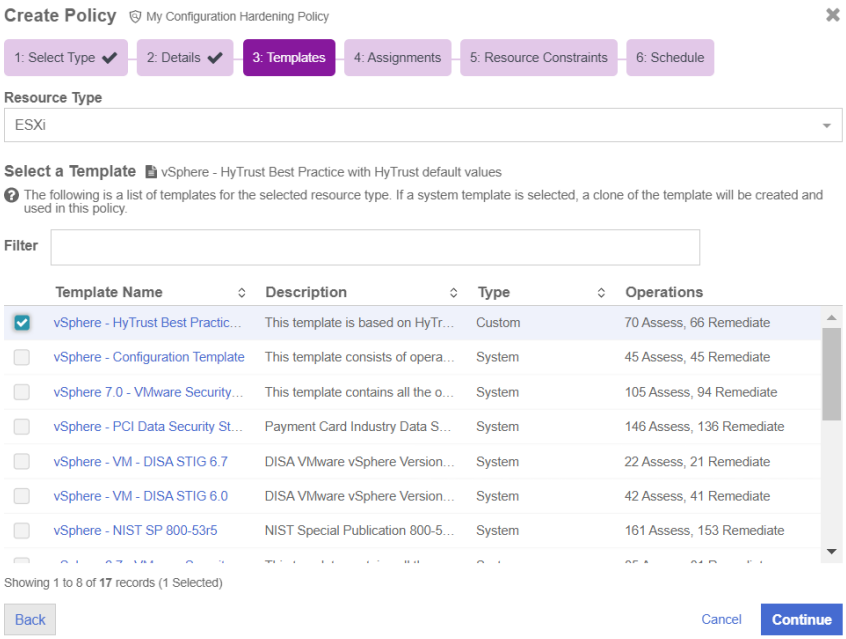


6. Select **Continue**.
7. On the **Details** page, enter the name and optional description of the policy, and specify whether the policy is enabled.



8. Select **Continue**.
9. On the **Templates** page, select the **resource type** for the policy. This can be one of the following:
    - **AWS Account** - Runs AWS-related templates against your AWS environment.
    - **ESXi** - Runs vSphere related templates against your ESXi hosts.
    - **Kubernetes** - Runs Kubernetes related templates against your Kubernetes environment.
    - **NSXDataCenter** - Runs NSX-T related templates against your NSX-T environment.

10. Select **ESXi** as the template to run against your environment.
11. The template list displays the name, description and type of operations Select a template that contains the type of operations that you selected for the policy.
12. Select **vSphere - HyTrust Best Practice** template. This template is used in the example.



See the online documentation for more information on Creating a Custom Template.

13. Select **Continue**.
14. On the **Assignments** page, select one of the following and choose what resources to which you want to apply the policy:
    - **Tags** - Select the Tags radio button and then choose a tag or tags assigned to the resource. Select the + icon if you want to assign more tags to the resource. If there are no tags assigned, you can select the Assign Tags Now link.
    - **Resources** - Select **Specific Resources** and then choose one or more resources.

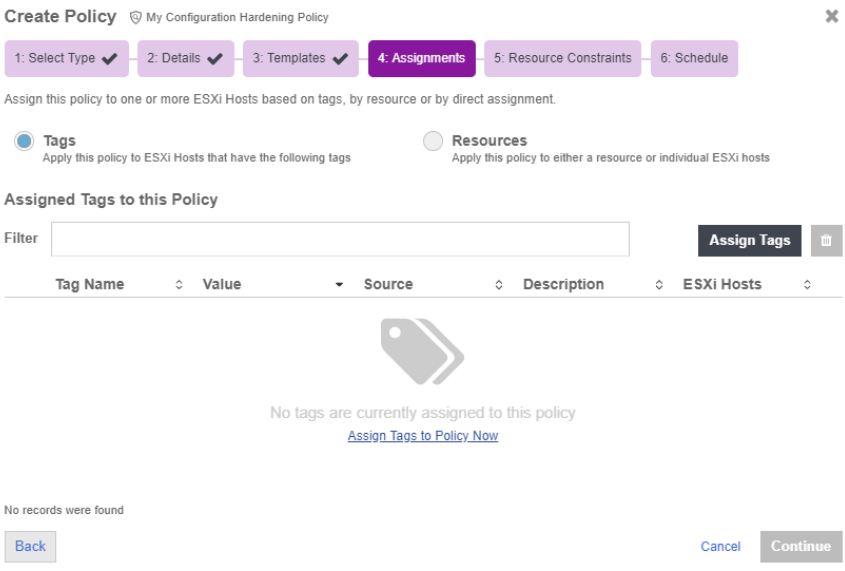
      For vSphere only, you can choose a parent for the resource type. This can be one of the following:

      - **vCenter** - Allows you to select all ESXi hosts in the selected vCenter. All onboarded ESXi hosts in the selected vCenter will be considered for hardening. You can select multiple vCenters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
      - **Appliance Root** - Allows you to select all ESXi hosts under Appliance Root. All onboarded ESXi hosts will be considered for hardening. When the

Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.

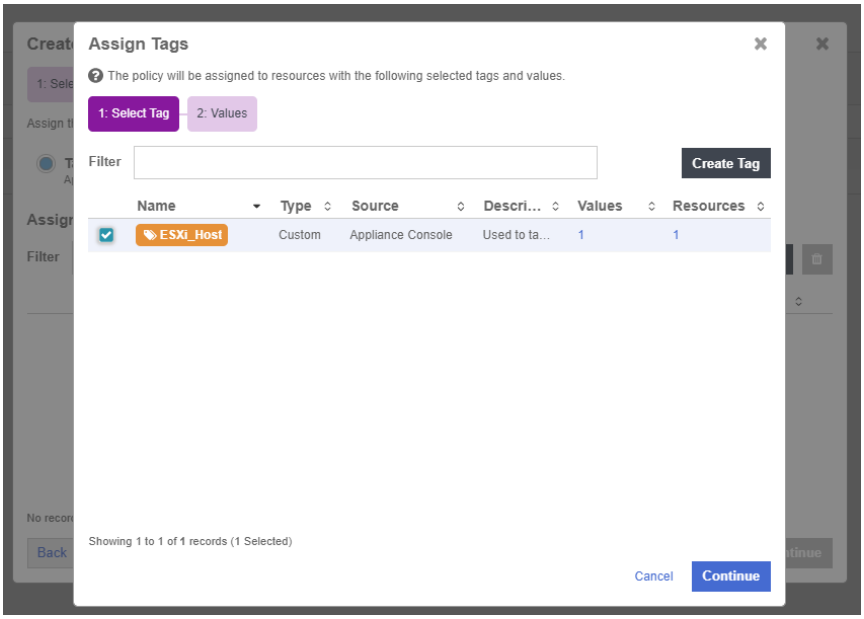
- **DataCenter** - Allows you to select all ESXi hosts in the selected DataCenter. All onboarded ESXi hosts in the selected vCenter will be considered for hardening. You can select multiple DataCenters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
- **Cluster** - Allows you to select all ESXi hosts in the selected Cluster. All onboarded ESXi hosts in the selected Cluster will be considered for hardening. You can select multiple Clusters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
- **ESXi Host** - Allows you to choose which individual ESXi hosts that you want to use as a resource. If additional ESXi hosts are onboarded, they will not be included.

15. Select **Tags** for the resources you want to apply the policy.
16. Select the **Assign Tags to Policy Now** link to select the tags.

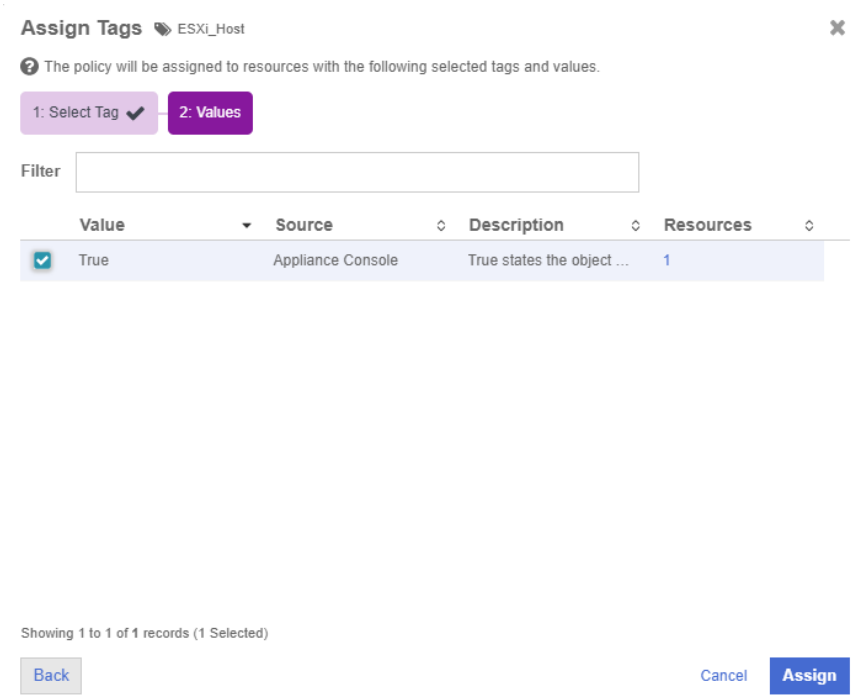


The **Assign Tags** dialog appears.

17. Select the **ESXi_Host** tag created earlier.



18. Select **Continue**.
19. Select the Tag value **True** that applies to the **ESXi_Host** tag.

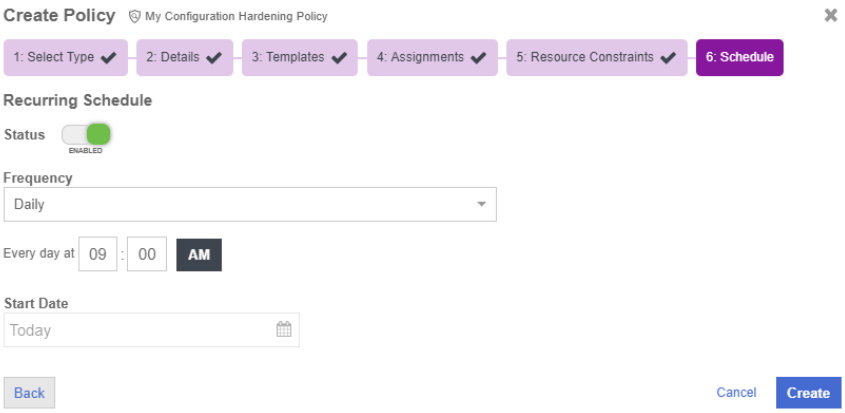


20. Select **Assign**.
21. Select **Continue**.
22. (Optional) For vSphere only. On the **Resource Constraint** page, choose which tag-based resource constraints that you want to use for your ESXi hosts. This option is not described in detail.
23. Select **Continue**.

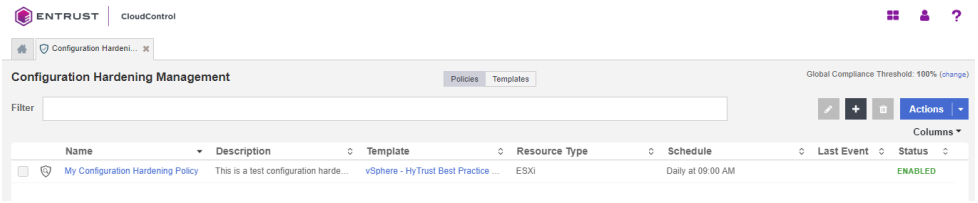
24. On the **Schedule** page, select if you want to enable a recurring schedule.

    If enabled, select the type of schedule that you want to use to run the policy, and then specify the start date. This can be one of the following:

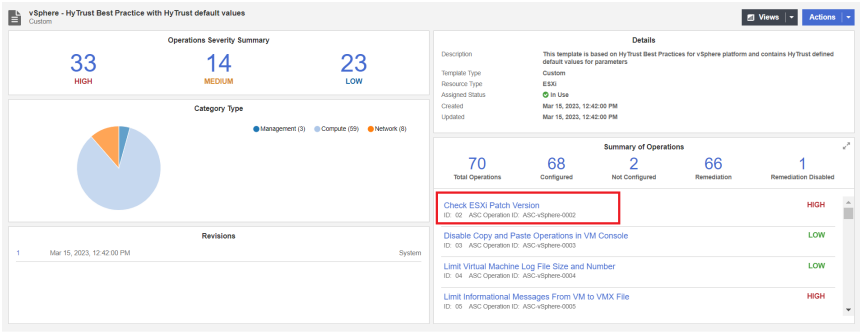
    - **Daily** - The policy will run every day at the time that you specify.
    - **Hourly** - The policy will run periodically throughout the day, based on the schedule you define.
    - **Weekly** - The policy will run on every day that you select at the time that you specify.



25. Select **Create**.
26. The newly created policy will be displayed on the **Policies** tab.

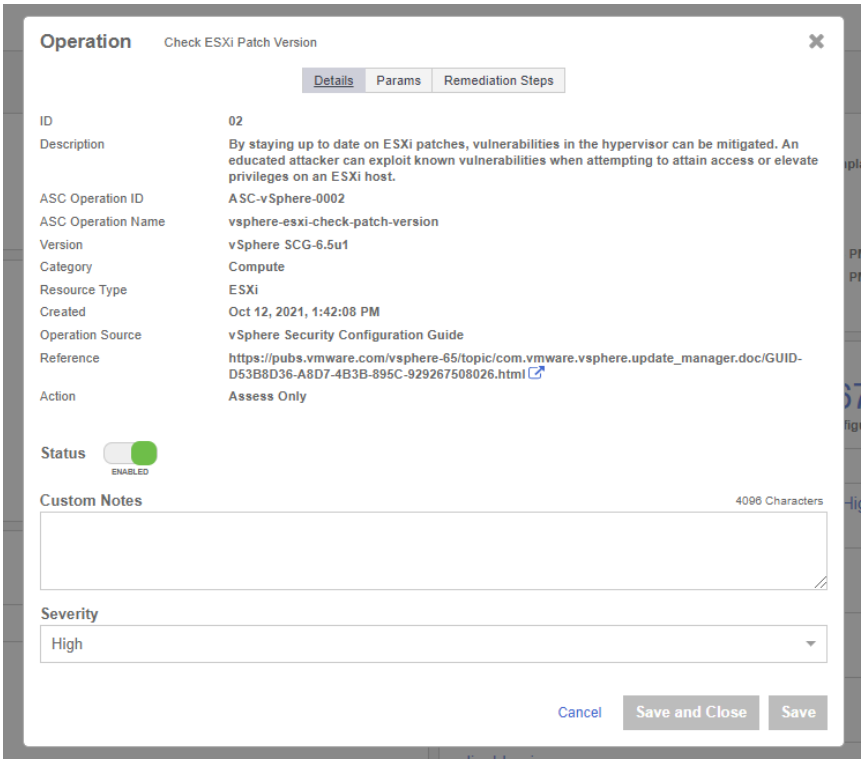


27. Edit the **Check ESXi Patch Version** Rule in the template. Select the **vSphere - HyTrust Best Practice** link in the **Template** Column. The template details appears.

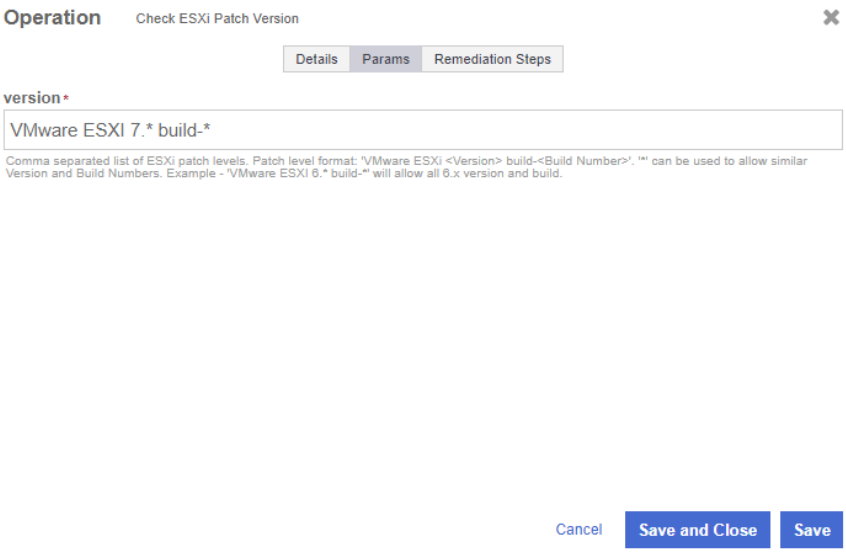


28. Under **Summary of Operations** look for **Check ESXi Patch Version**.

29. Once you find it, select the **Check ESXi Patch Version** link to edit the rule.



30. Select the **Params** tab and enter the version according to the image below.

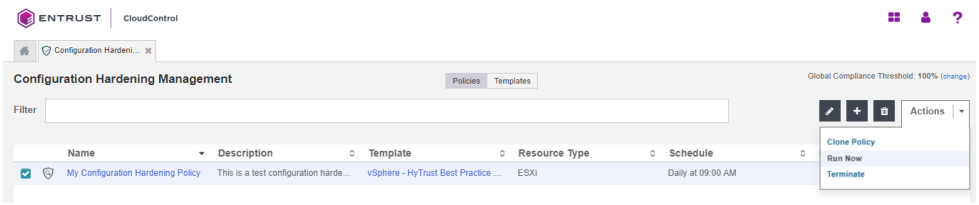


31. Select **Save and Close**.

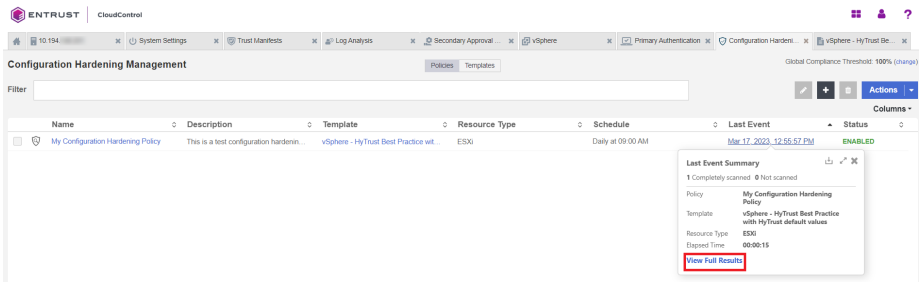
    Now when the Configuration Hardening Policy runs, this rule will check to see if the version of the ESXi Host will match what is on the version field of the rule.

When you run a remediation policy, the assessment policy will automatically run immediately following its completion. This ensures that your compliance score is updated with the new percentage.

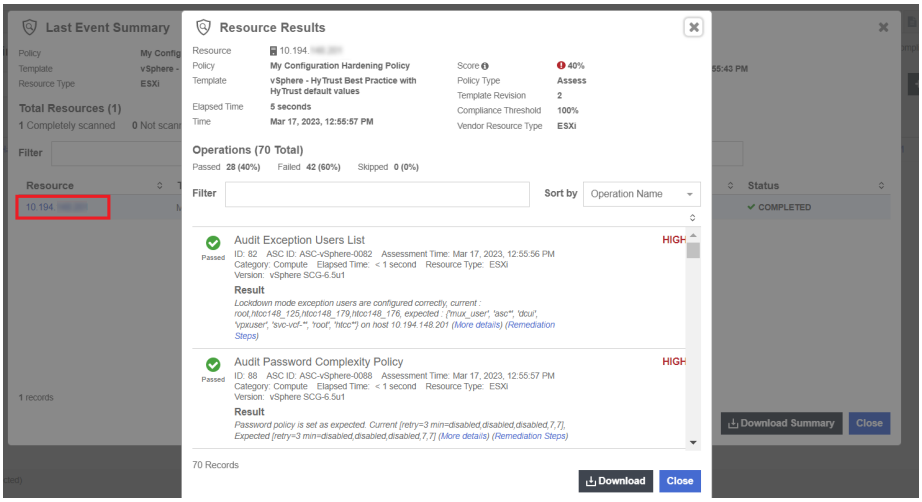
32. From the **Home** tab, select **Security > Configuration Hardening**.
33. On the **Configuration Hardening Management** page, select the **Policies** tab.
34. Select the Policy that you want to run.
35. Select **Actions > Run Now**.
36. In the confirmation window, select **Run Now**.



37. You can view the results by selecting the link in the Last Event column.
38. Select **View Full Results**.

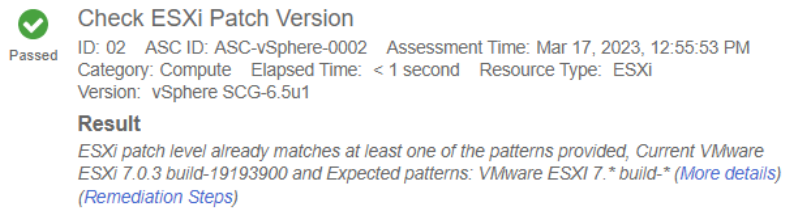


39. In the **Last Event Summary** Tab, select **Resource**.

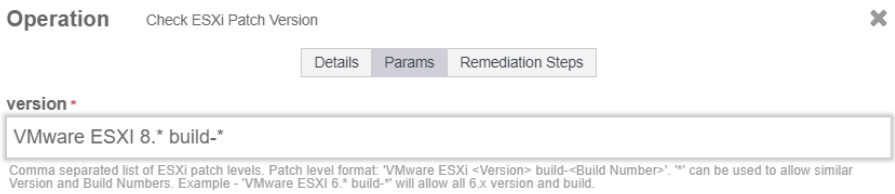


If you used resource constraints on your ESXi hosts, you can see which hosts were analyzed and which were skipped.

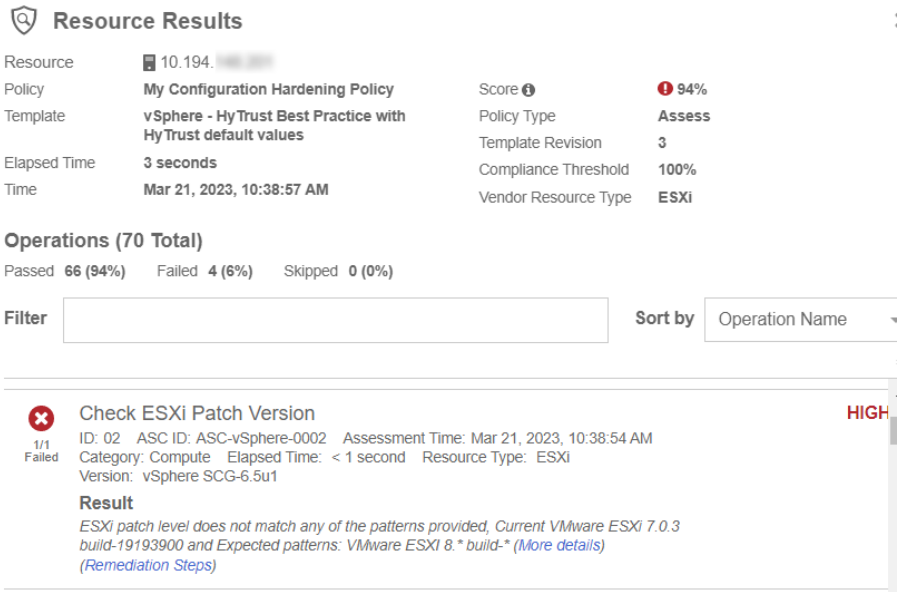
40. As you look to the results, you will be able to see that the ESXi Version test that was in the policy, **Passed**.



If you enter the incorrect version in the Check ESXi Patch Version Params, the Configuration Hardening Policy will catch the failure. For example, if you enter VMware ESXi version 8 instead of 7:



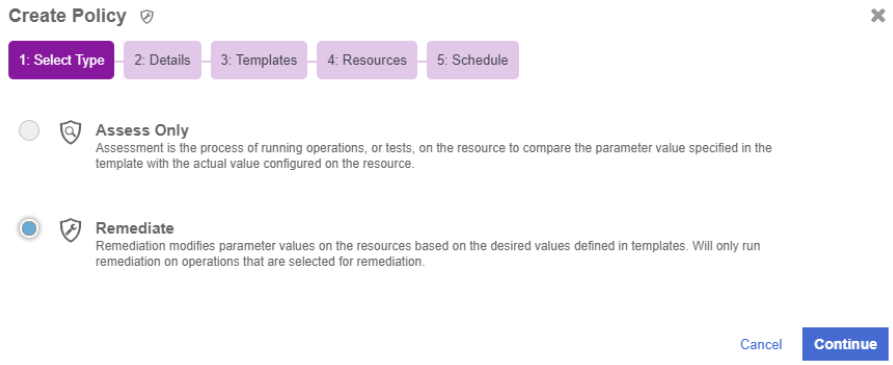
When you run the Configuration Hardening Policy, the system will catch the error and report a failed result.



2.16. Remediation Policy

Now that the Configuration Hardening Policy has been created, the same process will be used to create a Remediation Policy. The process is basically the same, with the exception that instead of selecting **Assess Only** as the type, the **Remediate** type will be selected

during the policy creation process.

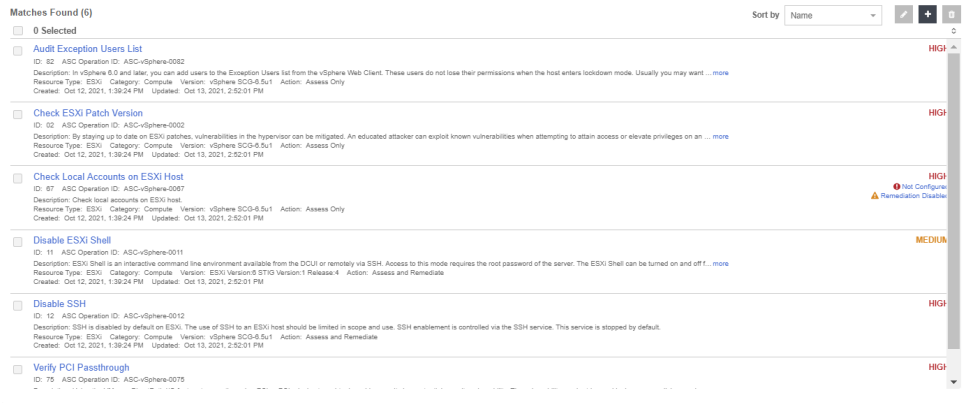


After the policy is created, edit the policy template to contain only the items you want to remediate.

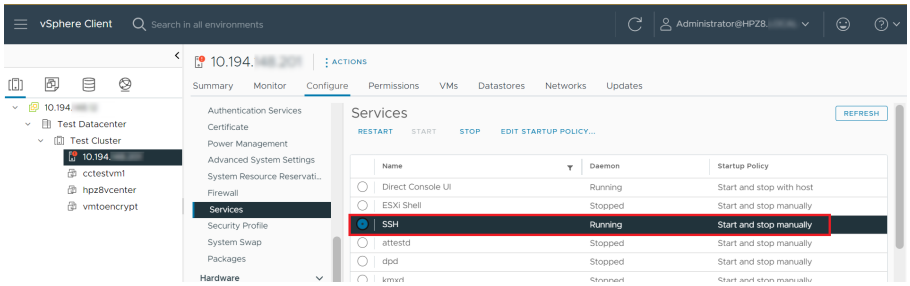
You do this in the **Configuration Hardening Management** page, by selecting the template in the **Template** column of the policy you want to edit. On the **Template** page, under the **Summary of Operations**, select **Total Operations**. The **Manage Operations** page appears. This page is used to select the rules that you want in the template. You can also **Add** and **Delete** selected rules.

Now that the template has been defined with the wanted rules, perform the remediation. This example shows how to **Disable SSH** on the ESXi host just by running the remediation policy.

The following rules are in the template. (One of them is **Disable SSH**).



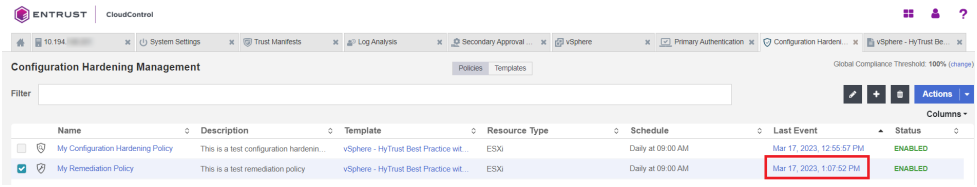
Before running the policy, go to the ESXi Host and validate that SSH service is running.



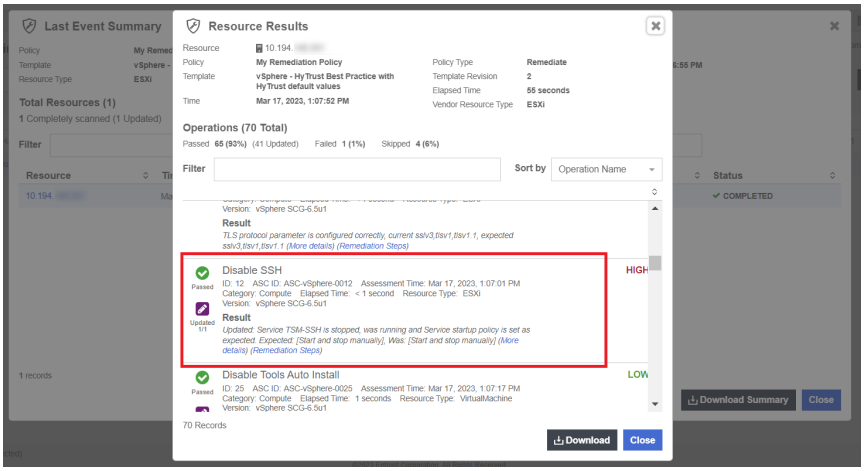
Run the remediation policy and see what happens to SSH in the ESXi Host.

In the Entrust CloudControl VM do the following:

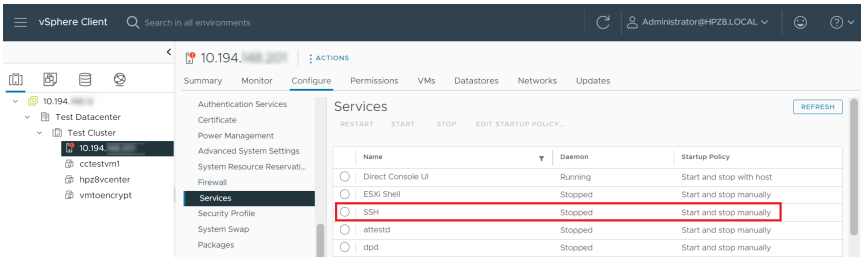
1. From the **Home** tab, select **Security > Configuration Hardening**.
2. On the **Configuration Hardening Management** page, select the **Policies** tab.
3. Select the remediation policy that you want to run.
4. Select **Actions > Run Now**.
5. In the confirmation window, select **Run Now**.
6. Once it finishes running, you can view the results by selecting the link in the Last Event column.



7. Locate the **Disable SSH** result and validate that it **Passed**.



8. Now go back to the ESXi Host and check if the SSH service is running. It should be set to **Stopped**.



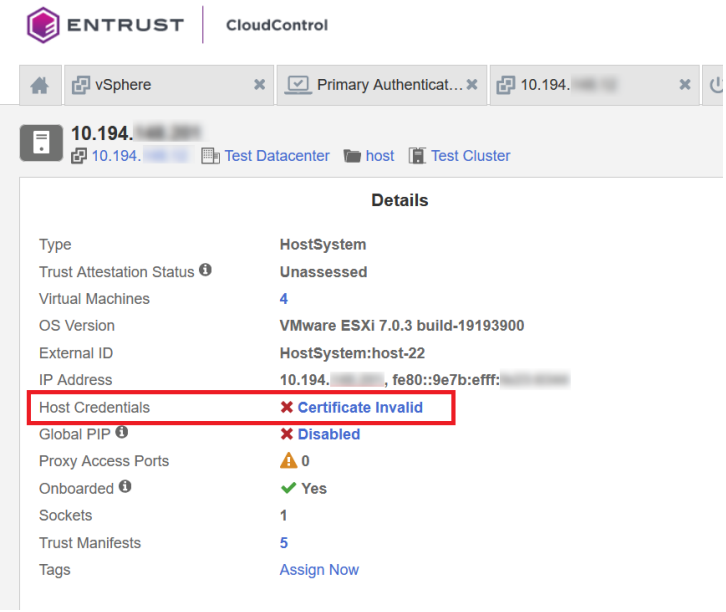
This example shows how you can use the remediation policy to automatically enforce configuration settings on your vSphere environment.

Chapter 3. Troubleshooting

The following are errors that might appear during the procedures described in this guide.

3.1. Host Credentials: Certificate Invalid

When adding the host credentials you may encounter the error **Host Credentials: Certificate Invalid**. For example:



To resolve this issue, the vCenter root CA must be imported into the CloudControl's Certificate Authorities:

1. Launch a Linux Terminal and use `openssl` to pull the root CA from vCenter. Where it shows IP, enter the vCenter IP address.

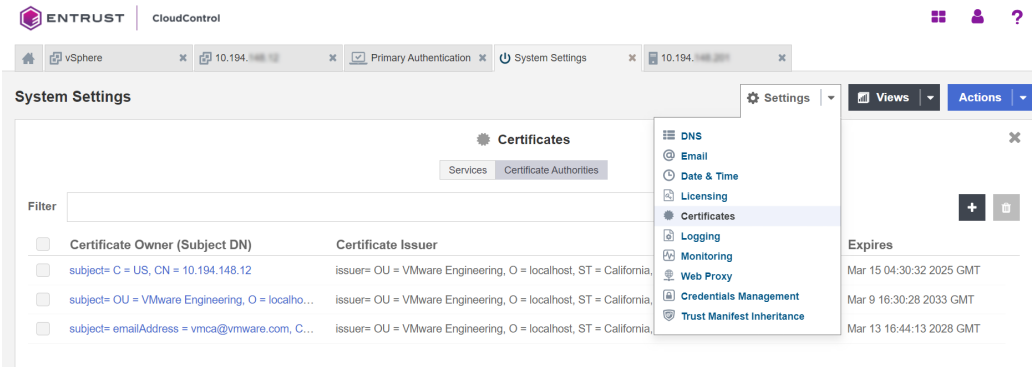
```
% echo | openssl s_client -connect <IP>:443 -showcerts
```

2. Enter the commands below to view the certificate:

```
% curl -k https://<IP>/certs/download.zip -o
% root_ca.zip
% unzip root_ca.zip
% cd certs
% cd lin
% cat 93a87255.0
```

3. Copy the certificate from the `cat 93a7255.0` command. Start from **-----BEGIN CERTIFICATE-----** and end with **-----END CERTIFICATE-----**.

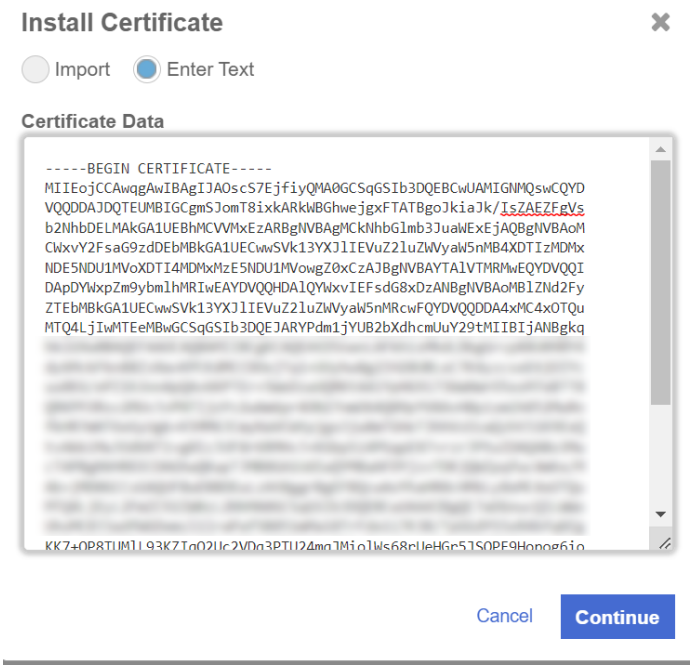
4. Login to your Cloud Control node as superadminuser.
5. From **Home**, select **System** > **System Settings** > **Settings Drop-Down Menu** > **Certificates**.



6. Select **Certificate Authorities**.
7. Select **Add** on the top right.

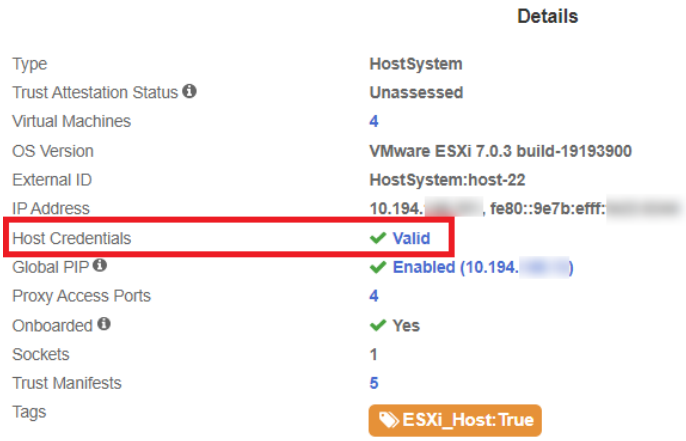
   The **Install Certificate** page appears.

8. Select **Enter Text** and paste the certificate.



9. Select **Continue**.
10. Select **Install**.
11. On the Cloud Control node, check the onboarded host **Details**.
12. Select **Certificate Invalid** and re-enter the host credentials.

    Host Credentials will update to **Valid**.


Details
Type
HostSystem
Trust Attestation Status
Unassessed
Virtual Machines
4
OS Version
VMware ESXi 7.0.3 build-19193900
External ID
HostSystem:host-22
IP Address
10.194.
, fe80::9e7b:efff:
Host Credentials
Valid
Global PIP
Enabled (10.194.
)
Proxy Access Ports
4
Onboarded
Yes
Sockets
1
Trust Manifests
5
Tags
ESXi_Host:True

Chapter 4. Additional resources and related products

4.1. CloudControl

4.2. Entrust products

4.3. nShield product documentation