Remediating Security-Policy Compliance issues using Ansible Playbooks

Create playbooks to fix security-policy issues and automate your way to RHEL infrastructure compliance
Create playbooks to fix security-policy issues and automate your way to RHEL infrastructure compliance.
Abstract

Remediate issues resulting in the noncompliance of RHEL systems with adopted security policies.
<table>
<thead>
<tr>
<th>Chapter Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAKING OPEN SOURCE MORE INCLUSIVE</td>
<td>3</td>
</tr>
<tr>
<td>PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL COMPLIANCE SERVICE REMEDIATIONS</td>
<td>5</td>
</tr>
<tr>
<td>CHAPTER 2. REMEDIATING SYSTEMS TO IMPROVE THE COMPLIANCE THRESHOLD OF A SELECTED POLICY</td>
<td>6</td>
</tr>
<tr>
<td>CHAPTER 3. REMEDIATING RULES FROM MULTIPLE POLICIES TO IMPROVE THE COMPLIANCE SCORE OF A SYSTEM</td>
<td>7</td>
</tr>
<tr>
<td>CHAPTER 4. REFERENCE MATERIALS</td>
<td>8</td>
</tr>
</tbody>
</table>
MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use Documentation.
3. Fill in the Description field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click Submit Bug.
CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL COMPLIANCE SERVICE REMEDIATIONS

The compliance service shows the compliance status of your Red Hat Enterprise Linux (RHEL) environment with adopted OpenSCAP security policies, and identifies the individual rules affecting the compliance of your systems.

For each rule + system pairing, the compliance service shows the steps to resolve the issue, and enables automated remediation with the creation of Ansible Playbooks.

The compliance service enables the following approaches to remediating issues:

- Remediate multiple systems to which a single policy is applied to bring a policy up to an acceptable threshold of compliance.
- Remediate multiple rules, whether for one or more policies, affecting the compliance status of a single system.
CHAPTER 2. REMEDIATING SYSTEMS TO IMPROVE THE COMPLIANCE THRESHOLD OF A SELECTED POLICY

Complete the following steps to remediate systems affecting the compliance threshold of a policy:

Procedure

1. Navigate to the Red Hat Enterprise Linux > Compliance > SCAP policies page and click on a policy.

2. Click the Systems tab.

3. Check the boxes for the systems you want to remediate and click Remediate.

4. Select whether to add the remediations to an existing or new playbook and take the following action:
   a. Click Add to existing playbook and select the desired playbook from the dropdown list, OR
   b. Click Create new playbook and add a playbook name.
   c. Click Next.

5. Review the information in the summary.
   a. By default, autoreboot is enabled. You can disable this option by clicking Turn off autoreboot.
   b. Click Submit.


7. Locate the playbook you just created and check the box next to it.

8. Download the playbook using the Download playbook link.
CHAPTER 3. REMEDIATING RULES FROM MULTIPLE POLICIES TO IMPROVE THE COMPLIANCE SCORE OF A SYSTEM

Complete the following steps to remediate rules affecting the compliance score of a system:

Procedure

1. Navigate to the Red Hat Enterprise Linux > Compliance > Reports page.
2. Click on a system.
3. Scroll down to see the list of rules impacting the system.
4. Use filters to refine the list to expose the most critical rules.
5. Check the boxes next to the rules to remediate and click Remediate.
6. Select whether to add to an existing or new playbook and take one of the following actions:
   a. Click Add to existing playbook and select the desired playbook from the dropdown list, OR
   b. Click Create new playbook and add a playbook name.
   c. Click Next.
7. Review the information in the summary.
   a. By default, autoreboot is enabled. You can disable this option by clicking Turn off autoreboot.
   b. Click Submit.
8. Select Remediations in the Insights for Red Hat Enterprise Linux services menu.
9. Locate the playbook you just created and check the box next to it.
10. Download the playbook using the Download playbook link.
CHAPTER 4. REFERENCE MATERIALS

To learn more about the compliance service, see the following resources:

- Assessing and Monitoring Security-Policy Compliance of RHEL Systems
- Generating Compliance Service Reports
- Insights for Red Hat Enterprise Linux Documentation
- Insights for Red Hat Enterprise Linux Product Support page