Red Hat Insights 2020-10

Remediating Security-Policy Compliance issues using Ansible Playbooks

Improve Compliance Status with Automated Remediations

Last Updated: 2020-11-02

Red Hat Insights 2020-10 Remediating Security-Policy Compliance issues using Ansible Playbooks

Improve Compliance Status with Automated Remediations

Legal Notice

Abstract

Remediate issues resulting in the noncompliance of RHEL systems with adopted security policies. Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.

Table of Contents

CHAPTER 1. COMPLIANCE SERVICE REMEDIATION OVERVIEW

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 Compliance service > 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 **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. Scroll to the bottom of the summary and toggle **Auto Reboot** if available and desired.
    b. Click **Create**.

Verification steps

1. Select **Remediations** in the Red Hat Insights services menu.
2. Locate the playbook you just created and check the box next to it.
3. 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 Compliance service > Reports page and click the **By System** tab.
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 **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. Scroll to the bottom of the summary and toggle **Auto Reboot** if available and desired.
    b. Click **Create**.

Verification steps

1. Select **Remediations** in the Red Hat Insights services menu.
2. Locate the playbook you just created and check the box next to it.
3. 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 Reports*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page