Brought to you by:

vmware®

SecOps

for dummies®
A Wiley Brand

Understand SecOps and why it matters

Explore how SecOps can help you

Learn how to apply SecOps principles

VMware Special Edition

Karl Fultz
Kendall Lovett

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.

SecOps

VMware Special Edition

by Karl Fultz and Kendall Lovett

for dummies®
A Wiley Brand

SecOps For Dummies®, VMware Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

ISBN 978-1-119-81394-1 (pbk); ISBN 978-1-119-81395-8 (ebk)

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Cynthia Tweed

Production Editor: Tamilmani Varadharaj

Special Help: Colleen Diamond

Introduction

Perhaps you've heard some talk about SecOps, and wondered what it was all about. Is SecOps a technology or a methodology? How does it change the way IT operations and security teams interact? And what impact can it have on the security of an organization?

Welcome to *SecOps For Dummies,* your guide to a new and greatly improved approach to enterprise IT security and compliance. This book teaches you the basics of SecOps and explains how it can help a business save money, become more efficient, and be more secure.

Keeping up with evolving security threats is a tall order for any IT security team. A modern IT security approach needs to be

- Integrated across security and IT operations teams
- Smarter and faster than the cybercriminals who are always looking for a way in
- Flexible enough to allow organizations to adapt it to their specific requirements and threats

SecOps can help your company realize all those goals and more.

About This Book

Don't let the small footprint fool you. This book is loaded with information that can help you understand and capitalize on the power of SecOps. In plain and simple language, we explain what SecOps is, why it's such a hot topic, how you can get started, and steps you can take to get the biggest bang for your IT buck.

Foolish Assumptions

In writing this book, we've made some assumptions about you. We assume that

- You work in IT, cloud, security, or a related role that involves some level of infrastructure management and security.
- You're familiar with IT infrastructure terminology.
- You understand the concept of virtualization.

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

REMEMBER

Take careful note of these key takeaway points.

TIP

This icon highlights tips that can save you time and effort.

WARNING

Anything marked with this icon will save you a load of trouble (or worse).

TECHNICAL STUFF

Read these optional passages if you crave a more technical explanation.

Where to Go from Here

The book is written as a reference guide, so you can read it from cover to cover or jump straight to the topics you're most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome: a better understanding of SecOps and how it can help you increase security, compliance, and IT efficiency. For more information, visit `www.vmware.com/products/vrealize-automation/saltstack-config.html`.

IN THIS CHAPTER

- **Staying ahead of security threats**
- **Confronting the IT security gap**
- **Getting how SecOps reduces security risks**

Chapter 1 Understanding SecOps

All organizations, regardless of industry or size, are becoming digital organizations. Customers *expect* digital experiences, regardless of whether they're shopping for enterprise accounting software or renewing a driver's license. Adopting new technologies can help deliver the speed, availability, and ease of use customers demand, but it also requires organizations to mitigate the security risks that naturally accompany updating operations to provide these digital experiences.

That's where SecOps comes in. SecOps, short for *security plus operations,* is a movement created to facilitate collaboration between IT security and operations teams. SecOps helps these teams integrate and automate the technologies and processes they use to keep systems and data secure.

This chapter describes the current state of IT security and shows how SecOps can help organizations reduce cybersecurity risk and improve business agility.

Keeping Up with Security Threats

If you're concerned about IT security, you're not alone. Many business leaders now list security and compliance as top concerns for their companies. Security incidents are on the rise, with cyberattacks and data breaches hitting our news feeds frequently, so the concern is justified.

Security spending is also up, with organizations spending more on information security and risk management services than ever before. Buying additional security tools and services obviously isn't enough to prevent security incidents. Defending against current and future threats requires a security-first mentality, in addition to putting systems and processes in place that reduce the attack surface, increase detection capabilities, and improve response. SecOps was created to help organizations do just that.

WARNING

Don't confuse selecting and purchasing security products with developing a security strategy. Security products are tools that can be extremely effective when applied as a component of a holistic security approach. They can also be ineffective or even detrimental to business success when applied incorrectly.

Recognizing the IT Security Gap

Security threats come in many different shapes and sizes — from malware and ransomware to network infiltration attempts or exploits of existing vulnerabilities. To better understand the types of security threats SecOps helps reduce, you need to first understand the typical roles and responsibilities of security and operations teams and where they intersect.

IT security roles and responsibilities

IT security teams ensure the security of business systems. Their specific functions include

- Defining and implementing company security policies and practices
- Finding and prioritizing vulnerabilities
- Monitoring for suspicious behavior

- Responding to active threats or infiltration attempts
- Investigating discovered breaches

IT operations roles and responsibilities

IT operations teams are responsible for maintaining and optimizing business systems and technologies. Specific functions include

- Provisioning and maintaining IT infrastructure (such as servers, containers, and networks)
- Optimizing resources
- Ensuring uptime of critical systems
- Developing custom applications or tools for the business
- Remediating any security or compliance issues discovered within the environment

Understanding the gap

IT security is responsible for defining and enforcing security policy, but they typically don't have the ability to update or make changes to the IT systems themselves. That's the job of IT operations. This is where a critical gap appears in the security practices for many organizations, and it's where a large majority of security breaches and incidents occur.

To draw an analogy, you can think of IT operations as the homeowner and IT security as the home's security company. Although a security company can install locks, alarms, and cameras, they don't own the property. The homeowner must ensure that the doors are locked, windows are shut, and any other accidental entry points are sealed to avoid a break-in.

The challenge is that the typical enterprise IT environment looks less like a single-family home and more like a gigantic palace with hundreds or even thousands of possible entry points. An enterprise IT environment is also typically under constant construction as an organization grows and evolves its IT systems to meet business goals and customer demands.

In addition, IT operations runs all the affairs of the palace — from cooking and cleaning, to construction and maintenance, to security . . . and did we mention they're nearly always understaffed?

It's under these circumstances that many IT system vulnerabilities are exploited. The security team discovers the vulnerabilities, and the organization is made aware of the vulnerabilities. Nothing has been done, however, to prevent an exploit. The resulting data breach is more akin to a hacker finding an unlocked window than executing any sort of elaborate scheme to bypass the main security system.

REMEMBER

Most exposures come from bad actors poking around an IT environment until they find an "open window" (a vulnerability) and then waltzing right in. SecOps helps security and operations reduce the attack surface and harden systems against these types of threats by integrating and automating the process of finding, prioritizing, and remediating IT vulnerabilities. In this way, SecOps works to decrease the gap between IT security and IT operations.

WARNING

Many security vendors today focus on finding and prioritizing vulnerabilities. If a vendor claims to remediate, dig deeper to understand what they truly mean. Some vendors may offer real remediation; others may take liberties with the term and provide "remediation" that's really something like a report that can be handed off to IT. Knowing you have a vulnerability is not the same as remediating it, just as identifying a window is open is not the same as actually shutting it.

Reducing Security Risks with SecOps

By following the practices in this book, you can develop a SecOps approach that enables your organization to eliminate vulnerabilities and compliance issues that could result in a data breach — accidental or malicious.

The benefits of an effective SecOps strategy include the following:

- Reduction of known vulnerabilities
- Consistent enforcement of compliance standards
- Increased IT staff efficiency

- Less opportunity for human error
- Faster, automated security remediation
- Improved cross-team communication
- Superior customer experiences
- Consistent security across cloud and on-premises environments

TIP

Following the principles outlined in this guide can help you harden your systems and greatly reduce the likelihood of an attack or breach, but no preventive security approach is foolproof. You should develop a security strategy that includes procedures for both preventive vulnerability management and active threat response.

IN THIS CHAPTER

- **Establishing SecOps objectives**
- **Tailoring your SecOps approach to your organization**
- **Earning trust to advance big changes**
- **Choosing a SecOps tool set**

Chapter 2
Putting SecOps into Practice

Much like DevOps (development plus IT operations), which preceded it, SecOps is a movement and practice that requires an organizational shift in culture, strategy, and execution. SecOps is not a tool or an individual job function. Implementing SecOps often requires purchasing new tools or using existing tools in new ways, but these actions must be underpinned by a sound strategy and organizational culture.

This isn't to say you need to redesign your entire company before you can benefit from SecOps principles. In this chapter, we outline the basics of SecOps and helpful ways to start applying them, regardless of where you are on your SecOps journey.

Getting How SecOps Works

The first key to SecOps can be found in the name: security plus IT operations. Neither operations nor security teams alone can effectively employ SecOps. As with any productive partnership, both teams must share common goals and put in the work to reach them. Often, this means understanding the core motivations and objectives of both groups. Do security teams want the company to deliver great products on time? Absolutely! Do operations teams want products and solutions that are secure and compliant? You bet!

However, although both teams share the same ultimate desires, their immediate priorities differ. Their responsibilities and the way they're measured differ. Identifying responsibilities and key performance indicators that drive team behavior is the first step to SecOps success.

TIP

To find common ground and develop shared investment in your SecOps initiative, you can work with your operations and security leaders to identify common objectives.

Your SecOps objectives could include the following:

- Shifting from manual, ad-hoc vulnerability remediation to automated processes
- Increasing visibility and reporting accuracy by integrating security and operations analytics
- Defining official IT security policies and enforcing them programmatically across business systems
- Establishing compliance requirements and continually enforcing best practices
- Improving communication by developing a mutually agreed upon cross-team engagement plan

After you identify your key objectives, you can prioritize them and build an action plan to achieve them.

Assessing Your SecOps Needs

No two organizations are the same. You may belong to a large organization with distinct security and operations teams under separate departments or executive leaders; organizations in this category can suffer from siloed decision-making and misaligned priorities and processes. Or you may belong to a small organization where security and operations roles are handled by the same team; teams in this camp may be understaffed and find themselves perpetually using a reactive, "duct tape and bailing wire" approach to security and compliance issues.

Size and structure aren’t the only variables. Organizations also vary widely in culture and mentality. You may be in an organization where security is everyone’s job and security and operations teams do their best to collaborate. Or you could be part of an organization where boundaries are clear-cut and a “not my job, not my problem” mentality is common.

TIP

Taking an honest assessment of your organization’s culture and security mindset can help you determine where to start your SecOps initiatives.

You can start by scoring your team on the following questions using a 0–4 scale, where 0 = never, 1 = rarely, 2 = sometimes, 3 = often, and 4 = always. The higher the score, the more security-focused your organization.

Criteria	**Score (0–4)**
My organization prioritizes security over speed of delivery.	
My team knows and implements our organization’s IT security policies.	
My team considers potential security impacts of new initiatives and addresses them before work begins.	
My team understands the objectives and success criteria of our SecOps counterparts (security or operations).	
My team actively collaborates with our SecOps counterparts.	
My organizational leadership encourages interaction and engagement with our SecOps counterparts.	
Total	

Use the weak areas as a starting point for your SecOps initiatives.

Developing SecOps-Focused Processes

Where people and processes are concerned, identifying and capturing a few quick wins can be helpful before diving in with significant changes. This can help build trust and interest in SecOps throughout your organization.

WARNING

A top-down approach to SecOps can certainly be effective, but implementing sweeping changes to your organization or processes has the potential to backfire and result in a lack of adoption. Ultimately, SecOps happens when people make SecOps happen. People will only do so if they catch the vision and recognize how SecOps can benefit them directly and help the organization at large.

Quick wins can be as simple as establishing a SecOps communication channel, such as a chat group or email alias, or hosting a monthly SecOps-focused lunch-and-learn, where both security and operations teams alternate presenting on topics of interest and share learnings. This can be a great way to establish common ground and begin to bridge ideological divides.

Bigger SecOps process changes may include establishing a global security policy and agreeing on a “minimum viable process” that allows IT to integrate security requirements into their existing workflows with minimal impact to performance or speed of delivery. Your organization could also choose to realign reporting structures to break down work silos or integrate seating across teams.

Organizations with sufficient resources may consider assembling a *SecOps strike team.* A SecOps strike team includes key representatives from each functional area and is empowered to find inefficiencies and breakdowns in existing IT security processes. The team works to develop solutions or provide recommendations to fix any processes they identify as requiring improvement.

Identifying a time-consuming process and creating an automation routine to simplify it can also have a big, immediate impact. For example, your security team may need to identify compliance issues in one tool and then manually submit a ticket to a separate IT tool, such as Jira or Cherwell, to notify operations of the issue. You could create a simple application programming interface (API) call that creates a ticket in Jira automatically when the security team flags the issue in their security tool. This would benefit both teams by freeing up the security team to work on other initiatives and providing a consistent, automated way for IT to receive and prioritize compliance issues alongside other operations tasks.

Choosing a SecOps Tool Set

In the upcoming chapters, we show how you can use VMware vRealize Automation to apply SecOps practices across your IT infrastructure. Although vRealize Automation has many powerful features for SecOps, no one-size-fits-all solution exists, and you should select a tool or tool set based on the unique needs of your organization.

TIP

After you define your key SecOps objectives, map out the steps you take to accomplish security tasks today, and identify major breakdowns in workflows or inefficiencies that could be improved with automation or additional tooling. Build a capabilities wish list based on your desired outcomes and the limitations of your current systems, and use this list to evaluate tools you plan to purchase or build.

Your SecOps tool capabilities wish list could include the following:

- Automated remediation
- Compliance workflow orchestration
- Out-of-the-box scanning for common compliance standards, such as Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley (SOX) Act, and Center for Internet Security (CIS) benchmarks.
- A patch management engine
- Vulnerability scanning and detection
- Integration with existing security scanners
- Artificial intelligence (AI)–driven prioritization and recommendations
- Support for a wide range of IT infrastructure types, including on-premises, public cloud, containers, network devices, workstations, and Internet of Things (IoT)
- “Security policy as code” creation and editing

IN THIS CHAPTER

- » Automating compliance and remediation
- » Accessing the SaltStack Config interface
- » Creating a compliance policy to run with SaltStack Config
- » Performing a compliance assessment and remediation

Chapter 3 Enforcing Continuous Compliance with Automation

A successful SecOps strategy requires promptly dealing with any issues related to continuous compliance. As you can imagine, managing compliance on the scale that most organizations operate can present quite a challenge.

The good news is that tools are available that help provide continuous compliance in a straightforward and simple way. This chapter shows how you can use VMware vRealize Automation SaltStack SecOps, for example, to automate the enforcement of continuous compliance.

TIP

If you haven't spent much time with SaltStack Config, we recommend checking out the VMware Cloud Management blog post, "vRealize Automation SaltStack Config – A Technical Overview" (`https://blogs.vmware.com/management/2020/11/vrealize-automation-saltstack-config-a-technical-overview.html`).

Managing Compliance with VMware vRealize Automation SaltStack SecOps

VMware vRealize Automation SaltStack SecOps offers compliance and vulnerability management for workloads running the vRealize Automation SaltStack Config minion. SaltStack SecOps is an add-on to vRA SaltStack Config, which provides both the assessment and remediation capabilities you need to maintain compliance.

Tools such as SaltStack SecOps are a great help for the IT teams charged with creating policies and assessments of operating system configurations. To streamline SecOps initiatives as much as possible, many tasks can be automated or performed manually. You also can use SaltStack SecOps to remediate targeted machine(s), restoring equipment to their proper state and addressing any discovered compliance or vulnerability issues.

The assessments use compliance benchmarks from the Center for Internet Security (CIS) and U.S. Department of Defense Systems Agency (DISA) Security Technical Implementation Guides (STIG). Vulnerability assessments use Common Vulnerabilities and Exposures (CVEs), typically directly from the source vendor.

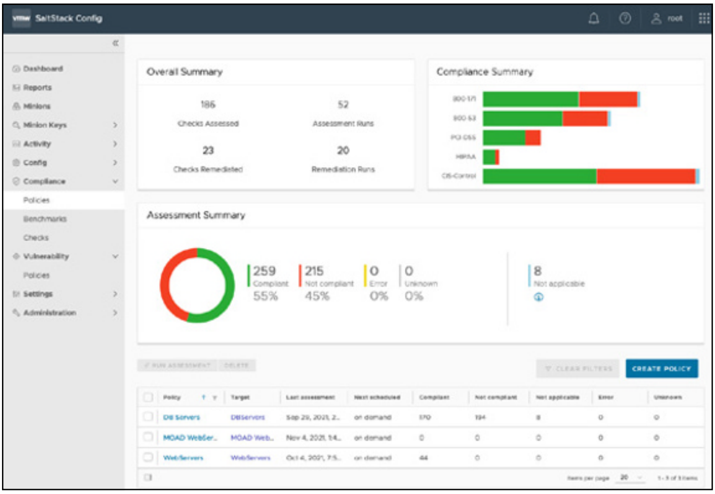
Roles-based access controls provide guardrails for people who perform particular tasks within an organization. For example, controls can be configured to allow security administrators to create policies and run assessments. After assessments are completed, operations administrators can remediate issues to bring deployments into compliance and address vulnerabilities.

REMEMBER

Working with tools like SaltStack SecOps helps IT security and operations teams reduce the notorious "gap" that exists between them, and more easily determine their organizations' compliance and security postures.

Starting SaltStack Config SecOps Compliance Management

After the SecOps user has logged into SaltStack Config, a window similar to the one shown in Figure 3-1 appears.



Overall Summary

186 Checks Assessed

52 Assessment Runs

23 Checks Remediated

20 Remediation Runs

Assessment Summary

259 Compliant 55%

215 Not compliant 45%

0 Error 0%

0 Unknown 0%

8 Not applicable

Policy	Target	Last assessment	Next scheduled	Compliant	Not compliant	Not applicable	Error	Unknown
DB Servers	DBServers	Sep 29, 2021, 2...	on demand	170	194	8	0	0
MOAD WebSer...	MOAD Web...	Nov 4, 2021, 14...	on demand	0	0	0	0	0
WebServers	WebServers	Oct 4, 2021, 7:5...	on demand	44	0	0	0	0

Items per page 20 1 - 3 of 3 items

FIGURE 3-1: Clicking Policies displays summary info on the main view.

Clicking Compliance or Vulnerability in the menu displays additional options. Click Compliance, for example, to view individual benchmarks and checks from the menu selection on the left.

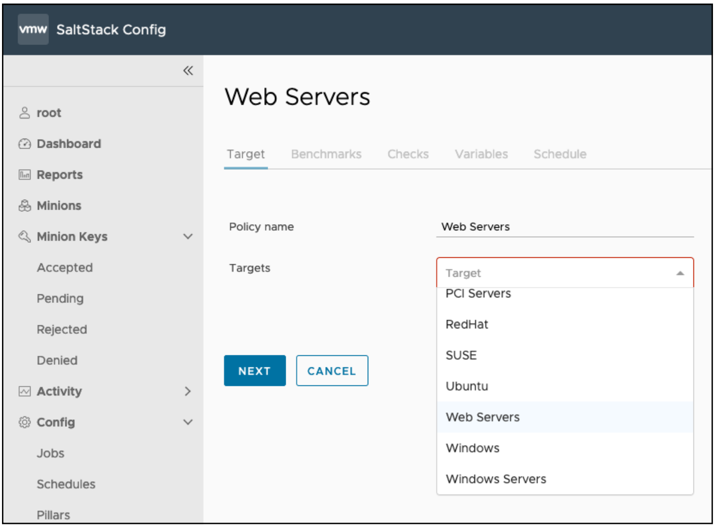
Choose Compliance ➪ Policies to view summary information on the main view (refer to Figure 3-1):

- **Compliance Summary:** Shows compliance to each regulation in a graph. In general, you want more green than red, and all green should be your goal!
- **Overall Summary:** Shows all assessments and remediation runs.
- **Assessment Summary:** The policy overview section offers summary views for each policy. From this section, you can create and manage policies by clicking the Create Policy button, which opens the Policy Configuration Wizard.

Creating a Compliance Policy

To create a compliance policy, you first must name the policy and choose a target. *Targets* are groups of minions that are created for state management needs. In this context, a target is a group of machines that will be assessed for compliance management.

In this case, we want to scan a group of web servers to check their compliance status. We name the policy Web Servers and choose the identically named Target: Web Servers from the drop-down list (see Figure 3-2).



Web Servers

Policy name: Web Servers

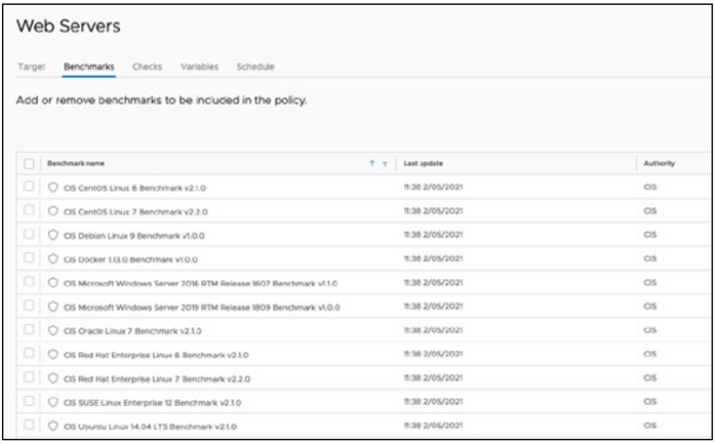
Targets

FIGURE 3-2: Checking the compliance status of Target: Web Servers.

Our web servers run CentOS 7. On the Benchmarks tab, shown in Figure 3-3, we chose CIS CentOS Linux 7 Benchmark from the list.

TIP

VMware currently supports 101 different operating system benchmarks. Each benchmark and its associated checks are taken directly from CIS, STIG, or Red Hat. You can select one or more benchmarks based on the operating system you want to assess.



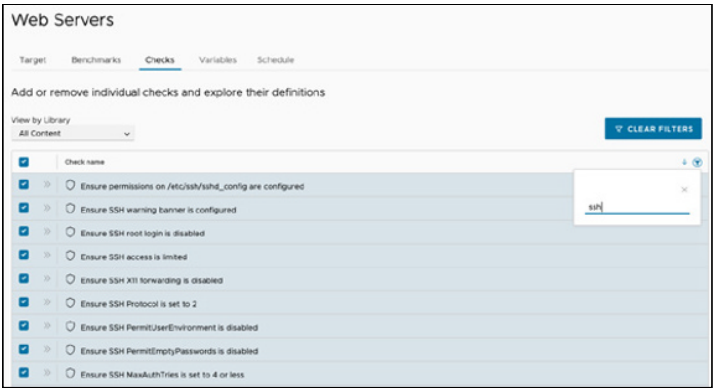
Web Servers

Add or remove benchmarks to be included in the policy.

□	Benchmark name	Last update	Authority
□	CIS CentOS Linux 6 Benchmark v2.1.0	11:38 2/05/2021	CIS
□	CIS CentOS Linux 7 Benchmark v2.2.0	11:38 2/05/2021	CIS
□	CIS Debian Linux 9 Benchmark v1.0.0	11:38 2/05/2021	CIS
□	CIS Docker 1.13.0 Benchmark v1.0.0	11:38 2/05/2021	CIS
□	CIS Microsoft Windows Server 2016 RTM Release 1607 Benchmark v1.1.0	11:38 2/05/2021	CIS
□	CIS Microsoft Windows Server 2019 RTM Release 1809 Benchmark v1.0.0	11:38 2/05/2021	CIS
□	CIS Oracle Linux 7 Benchmark v2.1.0	11:38 2/05/2021	CIS
□	CIS Red Hat Enterprise Linux 6 Benchmark v2.1.0	11:38 2/05/2021	CIS
□	CIS Red Hat Enterprise Linux 7 Benchmark v2.2.0	11:38 2/05/2021	CIS
□	CIS SUSE Linux Enterprise 12 Benchmark v2.1.0	11:38 2/05/2021	CIS
□	CIS Ubuntu Linux 14.04 LTS Benchmark v2.1.0	11:38 2/06/2021	CIS

FIGURE 3-3: The Benchmarks tab.

After choosing the benchmark(s), click Next to display the list of checks that are included. You can select all checks available for a benchmark or refine the list by using a filter. For this example, we filtered checks to a smaller number based on Secure Shell Protocol (SSH), as shown in Figure 3-4. Select the check boxes next to an item to include those checks in the policy.



Web Servers

Add or remove individual checks and explore their definitions

View by Library
All Content

ssh

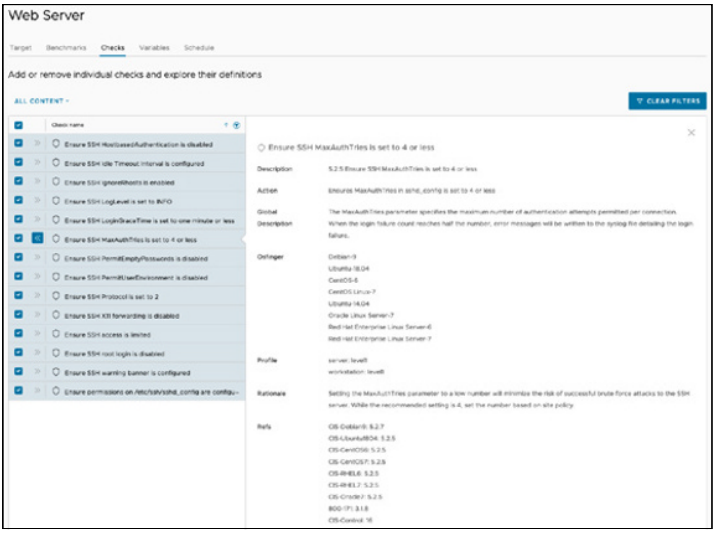
☑	Check name
☑	Ensure permissions on /etc/ssh/sshd_config are configured
☑	Ensure SSH warning banner is configured
☑	Ensure SSH root login is disabled
☑	Ensure SSH access is limited
☑	Ensure SSH X11 forwarding is disabled
☑	Ensure SSH Protocol is set to 2
☑	Ensure SSH PermitUserEnvironment is disabled
☑	Ensure SSH PermitEmptyPasswords is disabled
☑	Ensure SSH MaxAuthTries is set to 4 or less

FIGURE 3-4: Filtering the checks for a benchmark.

TIP

You can enter additional filters until all the relevant checks are selected for your needs.

If you're unsure what a check involves, click the arrows next to the check box to view a description, rationale, osfinger for grain matching, benchmark ref, and importantly, actions the check will take if remediation is required (see Figure 3-5).



Add or remove individual checks and explore their definitions

- ☑ Ensure SSH HostbasedAuthentication is disabled
- ☑ Ensure SSH Idle Timeout Interval is configured
- ☑ Ensure SSH ignoreRhosts is enabled
- ☑ Ensure SSH LogLevel is set to INFO
- ☑ Ensure SSH LoginGraceTime is set to one minute or less
- ☑ Ensure SSH MaxAuthTries is set to 4 or less
- ☑ Ensure SSH PermitEmptyPasswords is disabled
- ☑ Ensure SSH PermitUserEnvironment is disabled
- ☑ Ensure SSH Protocol is set to 2
- ☑ Ensure SSH X11 forwarding is disabled
- ☑ Ensure SSH access is limited
- ☑ Ensure SSH root login is disabled
- ☑ Ensure SSH warning banner is configured
- ☑ Ensure permissions on /etc/ssh/sshd_config are configu-

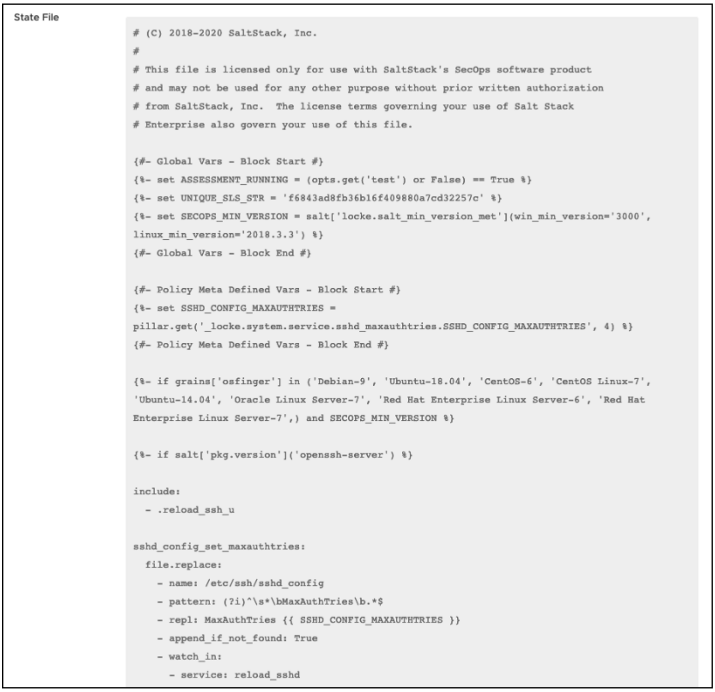
Ensure SSH MaxAuthTries is set to 4 or less

Description	5.2.5 Ensure SSH MaxAuthTries is set to 4 or less
Action	Ensures MaxAuthTries in sshd_config is set to 4 or less
Global Description	The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.
Osfinger	Debian-9 Ubuntu-18.04 CentOS-6 CentOS Linux-7 Ubuntu-14.04 Oracle Linux Server-7 Red Hat Enterprise Linux Server-6 Red Hat Enterprise Linux Server-7
Profile	server: level1 workstation: level1
Rationale	Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.
Refs	CIS-Debian9: 5.2.7 CIS-Ubuntu1804: 5.2.5 CIS-CentOS6: 5.2.5 CIS-CentOS7: 5.2.5 CIS-RHEL6: 5.2.5 CIS-RHEL7: 5.2.5 CIS-Oracle7: 5.2.5 800-171: 3.1.8 CIS-Control: 16

FIGURE 3-5: Viewing details for a check.

If you scroll down a bit on this screen (refer to Figure 3-5), you can view details on the state file (see Figure 3-6). This detail shows what Salt checks when you run an assessment, and subsequently, what happens if you choose to remediate.

The variable `test=True` tells Salt the run is a check against the state of a machine and is used for assessment purposes. *No changes will occur* to the target during the assessment phase. *Salt states*, or the state in which a system should be in, are what sets SaltStack SecOps apart from other SecOps products. Many products claim to offer remediation of an issue or configuration, but SaltStack goes well beyond simple remediation by offering full state management, configuration drift, and patching for continuous security and compliance management.



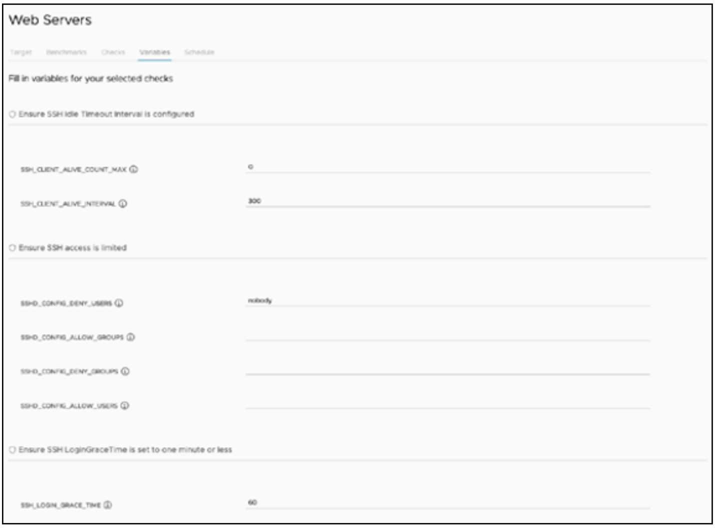
```
# (C) 2018-2020 SaltStack, Inc.
#
# This file is licensed only for use with SaltStack's SecOps software product
# and may not be used for any other purpose without prior written authorization
# from SaltStack, Inc.  The license terms governing your use of Salt Stack
# Enterprise also govern your use of this file.

{#- Global Vars - Block Start #}
{%- set ASSESSMENT_RUNNING = (opts.get('test') or False) == True %}
{%- set UNIQUE_SLS_STR = 'f6843ad8fb36b16f409880a7cd32257c' %}
{%- set SECOPS_MIN_VERSION = salt['locke.salt_min_version_met'](win_min_version='3000',
linux_min_version='2018.3.3') %}
{#- Global Vars - Block End #}

{#- Policy Meta Defined Vars - Block Start #}
{%- set SSHD_CONFIG_MAXAUTHTRIES =
pillar.get('_locke.system.service.sshd_maxauthtries.SSHD_CONFIG_MAXAUTHTRIES', 4) %}
{#- Policy Meta Defined Vars - Block End #}

{%- if grains['osfinger'] in ('Debian-9', 'Ubuntu-18.04', 'CentOS-6', 'CentOS Linux-7',
'Ubuntu-14.04', 'Oracle Linux Server-7', 'Red Hat Enterprise Linux Server-6', 'Red Hat
Enterprise Linux Server-7',) and SECOPS_MIN_VERSION %}

{%- if salt['pkg.version']('openssh-server') %}

include:
  - .reload_ssh_u

sshd_config_set_maxauthtries:
  file.replace:
    - name: /etc/ssh/sshd_config
    - pattern: (?i)^\s*\bMaxAuthTries\b.*$
    - repl: MaxAuthTries {{ SSHD_CONFIG_MAXAUTHTRIES }}
    - append_if_not_found: True
    - watch_in:
      - service: reload_sshd
```

FIGURE 3-6: The Salt state file.

VMware is certified with CIS and DISA to obtain benchmarks and adds states to the check so you don't have to. Adding a state file to the process dramatically cuts down on the amount of time it will take for your company to understand your compliance posture and, if necessary, immediately remediate states when a change is required. This process also cuts out the often lengthy process of developing your own state files, testing, and frequently iterating on those files until your operating system is properly compliant.

Many checks offer the ability to tweak a specific config in your environment. Click Variables to open the Variables tab, where you can make changes directly in the policy (see Figure 3-7). The changes you make on the Variables tab will occur during a remediation. You also can change the config state through the main SaltStack config portion of the interface or via CLI.

When you create a policy, the final step is to create a schedule for running its assessments. You do this on the Schedule tab (see Figure 3-8). For this example, we chose to run an assessment every Saturday at 2:00 a.m.



Web Servers

Fill in variables for your selected checks

○ Ensure SSH Idle Timeout Interval is configured

SSH_CLIENT_ALIVE_COUNT_MAX: 0

SSH_CLIENT_ALIVE_INTERVAL: 300

○ Ensure SSH access is limited

SSHD_CONFIG_DENY_USERS: nobody

SSHD_CONFIG_ALLOW_GROUPS:

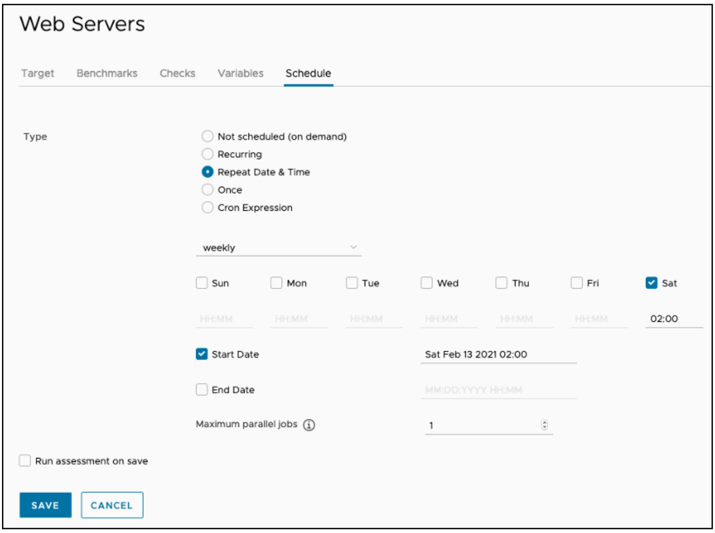
SSHD_CONFIG_DENY_GROUPS:

SSHD_CONFIG_ALLOW_USERS:

○ Ensure SSH LoginGraceTime is set to one minute or less

SSH_LOGIN_GRACE_TIME: 60

FIGURE 3-7: Modifying config states on the Variables tab.



Web Servers

Type

○ Not scheduled (on demand)
○ Recurring
● Repeat Date & Time
○ Once
○ Cron Expression

weekly

□ Sun HH:MM
□ Mon HH:MM
□ Tue HH:MM
□ Wed HH:MM
□ Thu HH:MM
□ Fri HH:MM
☑ Sat 02:00

☑ Start Date: Sat Feb 13 2021 02:00

□ End Date: MM:DD:YYYY HH:MM

Maximum parallel jobs: 1

□ Run assessment on save

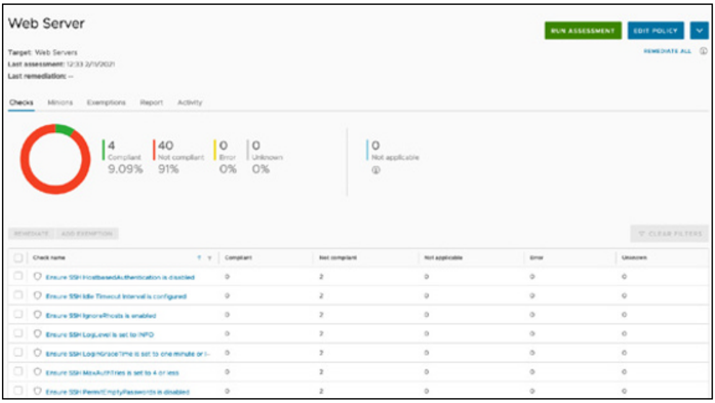
FIGURE 3-8: Scheduling assessments.

You can run an assessment once, or you can set an interval for a recurring assessment down to the hour, minute, and second. Cron expressions offer additional customization options for scheduling. You also can set a maximum number of parallel jobs to control the speed of the assessment and resource use.

Running a Compliance Assessment and Remediation

After a policy is created, you can run an assessment at any time by clicking the green Run Assessment box inside that policy. You also can make changes to a policy by editing the policy at any time to modify previously chosen settings.

For the example in this chapter, we ran the assessment using the SSH checks that were set on the filter. The assessment results indicate that the VMs are 91 percent *noncompliant* for the SSH checks we selected (see Figure 3-9).



Web Server

Target: Web Servers
Last assessment: 12:33 2/1/2021
Last remediation: --

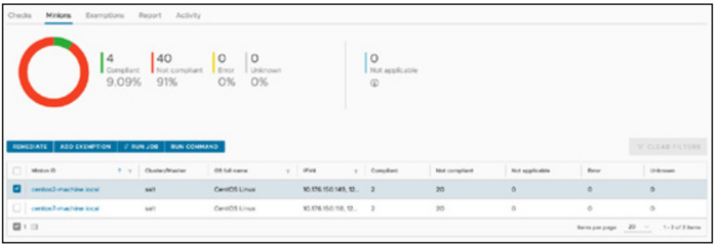
4 Compliant 9.09%	40 Not compliant 91%	0 Error 0%	0 Unknown 0%	0 Not applicable

Check name	Compliant	Not compliant	Not applicable	Error	Unknown
Ensure SSH HostbasedAuthentication is disabled	0	2	0	0	0
Ensure SSH Idle Timeout Interval is configured	0	2	0	0	0
Ensure SSH IgnoreRhosts is enabled	0	2	0	0	0
Ensure SSH LogLevel is set to INFO	0	2	0	0	0
Ensure SSH LoginGraceTime is set to one minute or l...	0	2	0	0	0
Ensure SSH MaxAuthTries is set to 4 or less	0	2	0	0	0
Ensure SSH PermitEmptyPasswords is disabled	0	2	0	0	0

FIGURE 3-9: Assessment results.

You can view each check's compliance status for the target, whether the check actually applies to the target, whether errors occurred during the assessment, and whether SecOps was able to determine the status, shown as Unknown. At this point, you can choose to remediate all checks against the Target or exempt certain checks if you decide they aren't relevant.

For a deeper view into each VM, click Minions. On the Minions tab, you get more details about the compliance status for each minion (machine) in the selected target (see Figure 3-10).



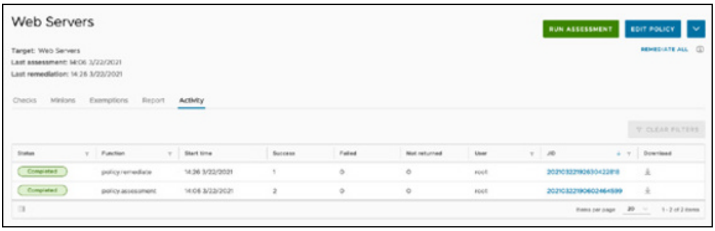
☐	Minion ID	Cluster/Master	OS full name	IPv4	Compliant	Not compliant	Not applicable	Error	Unknown
☑	centos2-machine.local	salt	CentOS Linux	10.176.150.149, 12...	2	20	0	0	0
☐	centos7-machine.local	salt	CentOS Linux	10.176.150.118, 12...	2	20	0	0	0

Items per page 20 1 - 2 of 2 items

FIGURE 3-10: The Minions tab.

At this level, you can choose individual VMs for remediation or exemption, or all VMs. You also can run SaltStack Config jobs and commands directly against the VMs. A set of predefined and custom jobs and commands can be used at this level that offer much greater state management flexibility beyond what is provided in each Check.

In Figure 3-10, we selected one of the CentOS VMs and clicked Remediate. When the remediation completes, click Activity to view job status and other job details (see Figure 3-11).



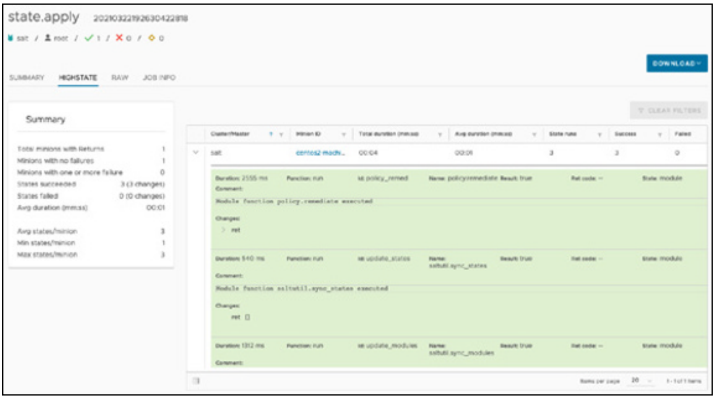
Target: Web Servers
Last assessment: 14:06 3/22/2021
Last remediation: 14:26 3/22/2021

Status	Function	Start time	Success	Failed	Not returned	User	JID	Download
Completed	policy.remediate	14:26 3/22/2021	1	0	0	root	20210322192630422818	
Completed	policy.assessment	14:06 3/22/2021	2	0	0	root	20210322190602464599	

Items per page 20 1 - 2 of 2 items

FIGURE 3-11: Viewing job status on the Activity tab.

You can view job details in several ways to get a different level and type of information on what was assessed, or in this example, what was remediated. For this example, we chose Highstate, which includes summary and deeper job details about the remediation (see Figure 3-12). These views can provide an audit trail of changes to the state of a VM and can provide attestation of compliance. You also have this detail for root isolation/cause should an error occur in the assessment or remediation process.



state.apply 20210322192630422818

salt / root / ✓ 1 / ✗ 0 / ◇ 0

Summary

Total minions with Returns	1
Minions with no failures	1
Minions with one or more failure	0
States succeeded	3 (3 changes)
States failed	0 (0 changes)
Avg duration (mm:ss)	00:01
Avg states/minion	3
Min states/minion	1
Max states/minion	3

Cluster/Master	Minion ID	Total duration (mm:ss)	Avg duration (mm:ss)	State runs	Success	Failed
salt	centos2-machi...	00:04	00:01	3	3	0

Duration: 2555 ms Function: run id: policy_remed Name: policy.remediate Result: true Ret code: -- State: module

Comment:

```
Module function policy.remediate executed
```

Changes:

› ret

Duration: 540 ms Function: run id: update_states Name: saltutil.sync_states Result: true Ret code: -- State: module

Comment:

```
Module function saltutil.sync_states executed
```

Changes:

ret []

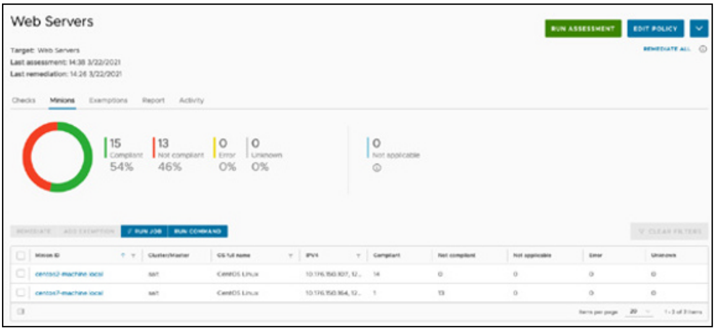
Duration: 1312 ms Function: run id: update_modules Name: saltutil.sync_modules Result: true Ret code: -- State: module

Comment:

Items per page 20 1 - 1 of 1 items

FIGURE 3-12: Viewing job details.

After remediation is complete, running the assessment again updates the assessment results (see Figure 3-13). The selected CentOS VM is now compliant with the checks we chose. When we clicked remediate, SaltStack Config made the configuration changes detailed in the state files for those checks.



Web Servers

Target: Web Servers
Last assessment: 14:38 3/22/2021
Last remediation: 14:26 3/22/2021

15 Compliant 54%
13 Not compliant 46%
0 Error 0%
0 Unknown 0%
0 Not applicable

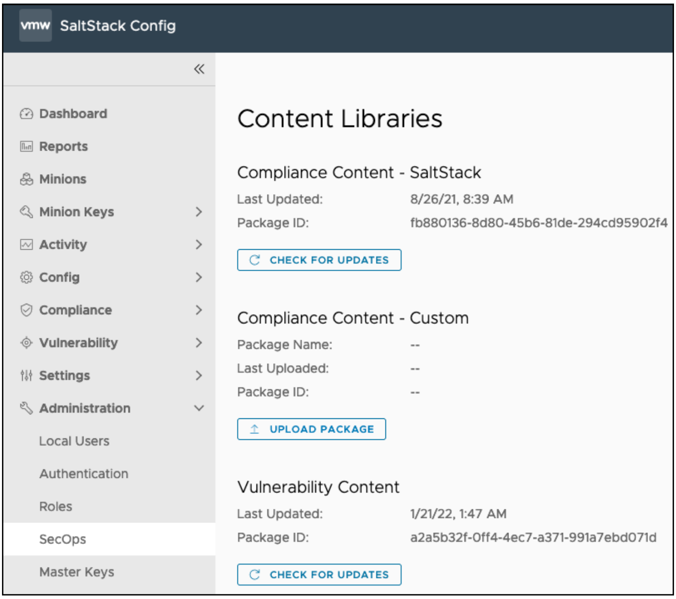
Minion ID	Cluster/Master	OS full name	IPV4	Compliant	Not compliant	Not applicable	Error	Unknown
centos2-machine.local	salt	CentOS Linux	10.176.150.107, 12...	14	0	0	0	0
centos7-machine.local	salt	CentOS Linux	10.176.150.164, 12...	1	13	0	0	0

Items per page 20 1 - 2 of 2 items

FIGURE 3-13: Updated assessment results.

Now that the VM is compliant, clicking Report shows further information about the policy status. You can now download a report to use for your organization's audit process.

SaltStack SecOps automatically downloads compliance (and vulnerability) content. However, you can also manually check for content or upload your own organization's content. Often customers will create their own content, which allows for assessment and remediation of corporate-specific configurations, such as application or operating system settings not covered by vendor-provided content. An interface is provided as part of the administration menus within SaltStack Config (see Figure 3-14).



Content Libraries

Compliance Content - SaltStack

Last Updated: 8/26/21, 8:39 AM

Package ID: fb880136-8d80-45b6-81de-294cd95902f4

Compliance Content - Custom

Package Name: --

Last Uploaded: --

Package ID: --

Vulnerability Content

Last Updated: 1/21/22, 1:47 AM

Package ID: a2a5b32f-0ff4-4ec7-a371-991a7ebd071d

FIGURE 3-14: The SecOps Content Library interface.

IN THIS CHAPTER

- **Summarizing your vulnerability posture**
- **Creating vulnerability policies that fit your needs**
- **Remediating operating system vulnerabilities**
- **Integrating external vulnerability assessments**

Chapter 4 Finding and Fixing Critical Vulnerabilities

SaltStack SecOps handles vulnerability management for operating systems much in the same way that it handles compliance management (see Chapter 3). To determine overall vulnerability, SaltStack uses common vulnerabilities and exposures (CVEs), which are obtained directly from vendors and automatically updated on a regular basis within SaltStack SecOps. As with compliance management, SaltStack uses a state file for assessment and remediation.

This chapter explains how to use SaltStack SecOps to create and manage vulnerability policies. You also see how to use SaltStack SecOps to address system vulnerabilities and how to incorporate external vulnerability assessments into the vulnerability management process. First, though, you must understand your security posture.

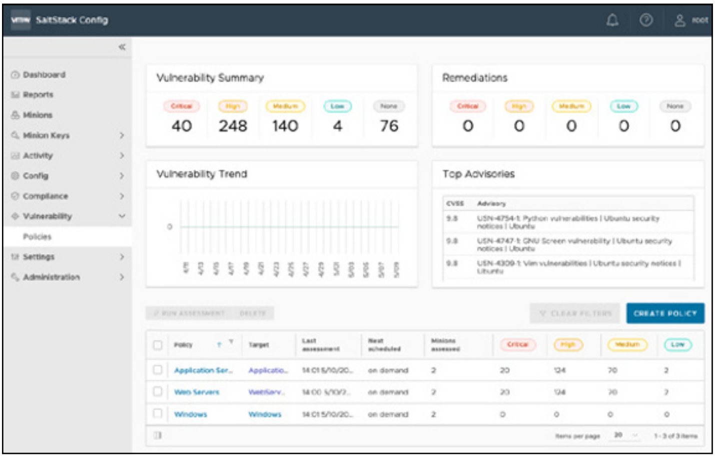
Checking Your Security Posture

For the example we use in this chapter, we begin by connecting to a Salt Master in the Vulnerability section of SaltStack SecOps. As with the Compliance section of the product, a summary view provides a snapshot of your vulnerability posture, trends, top advisories, and remediations.

You create a policy in the Vulnerability section of the product in much the same way as you do in the Compliance section (see Chapter 3). The Vulnerability section, however, has fewer options to choose from. Unlike Compliance policies, where benchmarks, checks, and variables are included as part of the policy configuration wizard, all vulnerabilities are checked against the selected minions.

The vulnerability policy creation process only requires you to name the policy, choose the targets, and set an assessment schedule or manually trigger a Run Now operation to determine your overall vulnerability posture.

When the assessment is complete, SaltStack SecOps displays a view similar to the one shown in Figure 4-1.



Vulnerability Summary

Critical	High	Medium	Low	None
40	248	140	4	76

Remediations

Critical	High	Medium	Low	None
0	0	0	0	0

Top Advisories

CVSS	Advisory
9.8	USN-4754-1: Python vulnerabilities | Ubuntu security notices | Ubuntu
9.8	USN-4747-1: GNU Screen vulnerability | Ubuntu security notices | Ubuntu
9.8	USN-4309-1: Vim vulnerabilities | Ubuntu security notices | Ubuntu

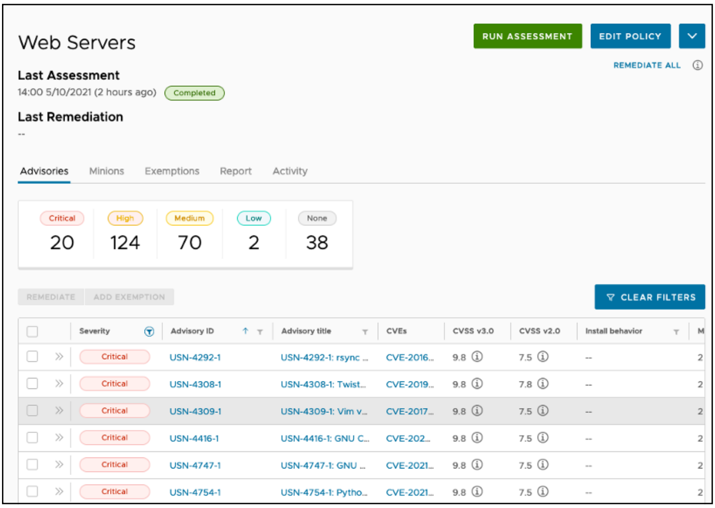
□	Policy	Target	Last assessment	Next scheduled	Minions assessed	Critical	High	Medium	Low
□	Application Ser...	Applicatio...	14:01 5/10/20...	on demand	2	20	124	70	2
□	Web Servers	WebServ...	14:00 5/10/2...	on demand	2	20	124	70	2
□	Windows	Windows	14:01 5/10/20...	on demand	2	0	0	0	0

Items per page 20 1 - 3 of 3 items

FIGURE 4-1: The vulnerability assessment is complete.

Creating and Managing Vulnerability Policies

If you open the Web Servers policy, you see we used the same Target as the example in Chapter 3. You can view the vulnerabilities that were discovered in the Advisories view (see Figure 4-2). From this Advisories view, you can filter advisories by severity and open advisories for more detail on the vulnerabilities SaltStack found in your environment. You also can remediate or exempt selected advisories across all minions in the selected Target.



Web Servers

Last Assessment
14:00 5/10/2021 (2 hours ago) Completed

Last Remediation
--

Critical	High	Medium	Low	None
20	124	70	2	38

□		Severity	Advisory ID	Advisory title	CVEs	CVSS v3.0	CVSS v2.0	Install behavior	M
□	»	Critical	USN-4292-1	USN-4292-1: rsync ...	CVE-2016...	9.8 ⓘ	7.5 ⓘ	--	2
□	»	Critical	USN-4308-1	USN-4308-1: Twist...	CVE-2019...	9.8 ⓘ	7.8 ⓘ	--	2
□	»	Critical	USN-4309-1	USN-4309-1: Vim v...	CVE-2017...	9.8 ⓘ	7.5 ⓘ	--	2
□	»	Critical	USN-4416-1	USN-4416-1: GNU C...	CVE-202...	9.8 ⓘ	7.5 ⓘ	--	2
□	»	Critical	USN-4747-1	USN-4747-1: GNU ...	CVE-2021...	9.8 ⓘ	7.5 ⓘ	--	2
□	»	Critical	USN-4754-1	USN-4754-1: Pytho...	CVE-2021...	9.8 ⓘ	7.5 ⓘ	--	2

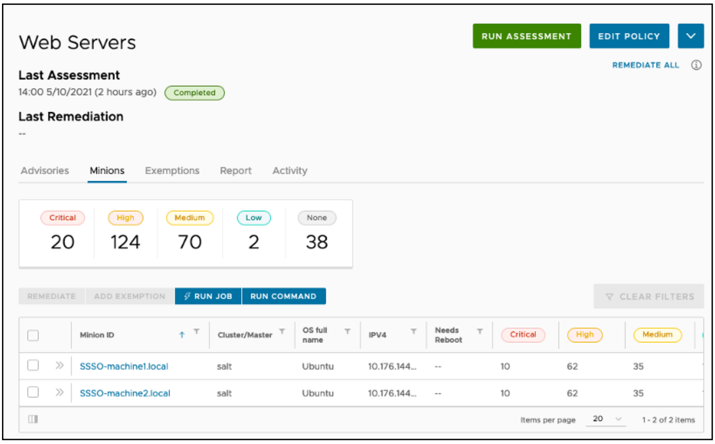
FIGURE 4-2: Vulnerabilities discovered in Target: Web Servers.

TIP

To measure vulnerabilities, SaltStack SecOps uses the Common Vulnerability Scoring System (CVSS) score, which is based on v2.0 and v3.0. Many users find that the additional severity ratings of v3.0 and expanded metrics allows for better differentiation among types of vulnerabilities and a more accurate picture of vulnerabilities encountered in the environment.

Addressing Operating System Vulnerabilities

From the Minions view, you can review Operating System vulnerability information for individual minions (see Figure 4-3). You can use the options in this view to instruct SaltStack Config SecOps to remediate or exempt only those minions you select. You also can run jobs or commands directly from the interface, just as with the Compliance section of the product.



Web Servers

Last Assessment
14:00 5/10/2021 (2 hours ago) Completed

Last Remediation
--

Critical	High	Medium	Low	None
20	124	70	2	38

□	Minion ID	Cluster/Master	OS full name	IPV4	Needs Reboot	Critical	High	Medium
□	SSSO-machine1.local	salt	Ubuntu	10.176.144...	--	10	62	35
□	SSSO-machine2.local	salt	Ubuntu	10.176.144...	--	10	62	35

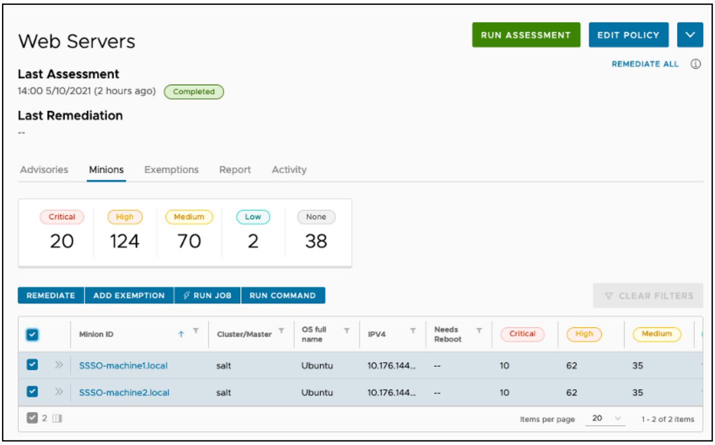
Items per page 20 1 - 2 of 2 items

FIGURE 4-3: The Minions view.

Clicking Remediate initiates a remediation job against the selected minions and updates the state of each minion to address known vulnerabilities (see Figure 4-4).

Navigating to the Activity tab allows you to monitor the job status, examine previous jobs, and view jobs details to determine what was assessed or remediated (see Figure 4-5). You view job details on the vulnerability side the same way you view job details on the compliance side (covered in Chapter 3).

Clicking the Report tab shows further details about the vulnerability status for minions within the policy, including vulnerability summary, vulnerability trends over time, remediations, and top advisories (see Figure 4-6). You can also click Download to generate a JSON version of the report for external needs.


Web Servers

RUN ASSESSMENT | EDIT POLICY

REMEDIATE ALL

Last Assessment
14:00 5/10/2021 (2 hours ago) Completed

Last Remediation
--

Advisories | **Minions** | Exemptions | Report | Activity

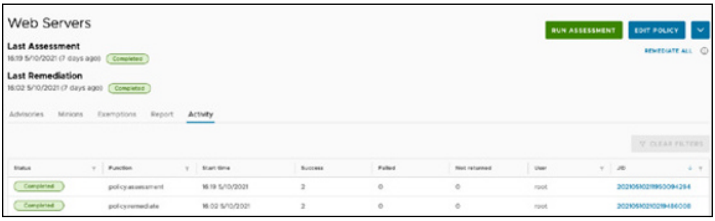
Critical	High	Medium	Low	None
20	124	70	2	38

REMEDIATE | ADD EXEMPTION | RUN JOB | RUN COMMAND | CLEAR FILTERS

☑	Minion ID	Cluster/Master	OS full name	IPV4	Needs Reboot	Critical	High	Medium
☑	SSSO-machine1.local	salt	Ubuntu	10.176.144...	--	10	62	35
☑	SSSO-machine2.local	salt	Ubuntu	10.176.144...	--	10	62	35

☑ 2 Items per page 20 1 - 2 of 2 items

FIGURE 4-4: Initiating a remediation job against selected minions.


Web Servers

RUN ASSESSMENT | EDIT POLICY

REMEDIATE ALL

Last Assessment
16:19 5/10/2021 (7 days ago) Completed

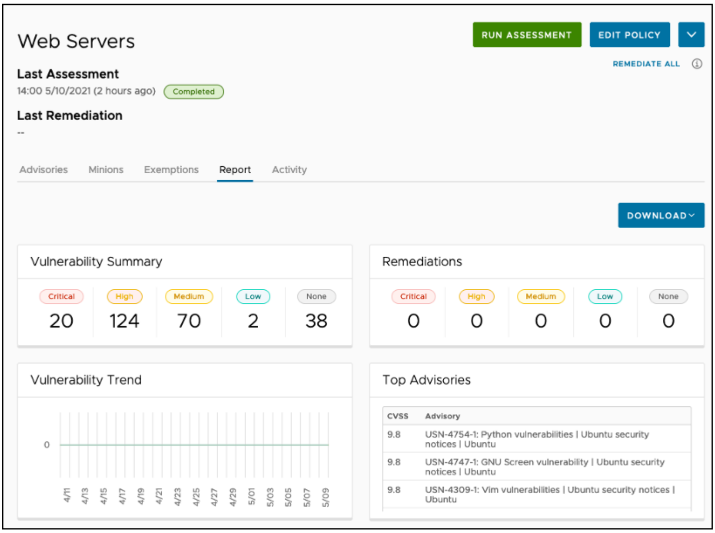
Last Remediation
16:02 5/10/2021 (7 days ago) Completed

Advisories | Minions | Exemptions | Report | **Activity**

CLEAR FILTERS

Status	Function	Start time	Success	Failed	Not returned	User	JID
Completed	policy.assessment	16:19 5/10/2021	2	0	0	root	20210510211953094294
Completed	policy.remediate	16:02 5/10/2021	2	0	0	root	20210510210219486008

FIGURE 4-5: Monitoring job status from the Activity view.


Web Servers

RUN ASSESSMENT | EDIT POLICY

REMEDIATE ALL

Last Assessment
14:00 5/10/2021 (2 hours ago) Completed

Last Remediation
--

Advisories | Minions | Exemptions | **Report** | Activity

DOWNLOAD

Vulnerability Summary

Critical	High	Medium	Low	None
20	124	70	2	38

Remediations

Critical	High	Medium	Low	None
0	0	0	0	0

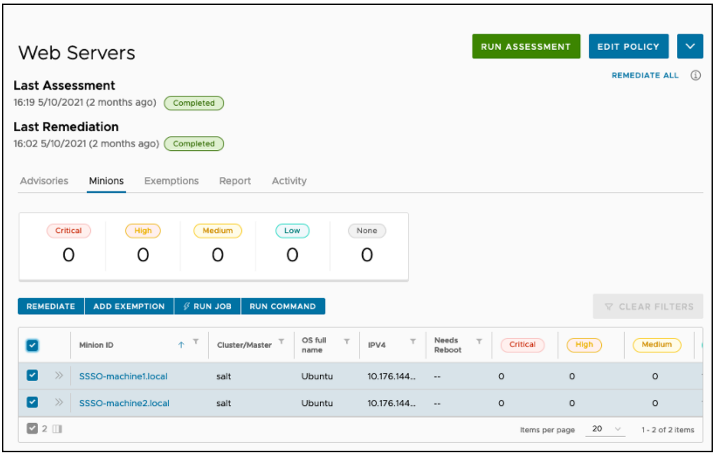
Vulnerability Trend

Top Advisories

CVSS	Advisory
9.8	USN-4754-1: Python vulnerabilities | Ubuntu security notices | Ubuntu
9.8	USN-4747-1: GNU Screen vulnerability | Ubuntu security notices | Ubuntu
9.8	USN-4309-1: Vim vulnerabilities | Ubuntu security notices | Ubuntu

FIGURE 4-6: The Report view shows further details about vulnerability status.

When a remediation and post-assessment are complete, the policy details will update to show the minions are no longer vulnerable based on the CVEs used during the assessment (see Figure 4-7).



Web Servers

Last Assessment
16:19 5/10/2021 (2 months ago) Completed

Last Remediation
16:02 5/10/2021 (2 months ago) Completed

Critical	High	Medium	Low	None
0	0	0	0	0

☑	Minion ID	Cluster/Master	OS full name	IPV4	Needs Reboot	Critical	High	Medium
☑	SSSO-machine1.local	salt	Ubuntu	10.176.144...	--	0	0	0
☑	SSSO-machine2.local	salt	Ubuntu	10.176.144...	--	0	0	0

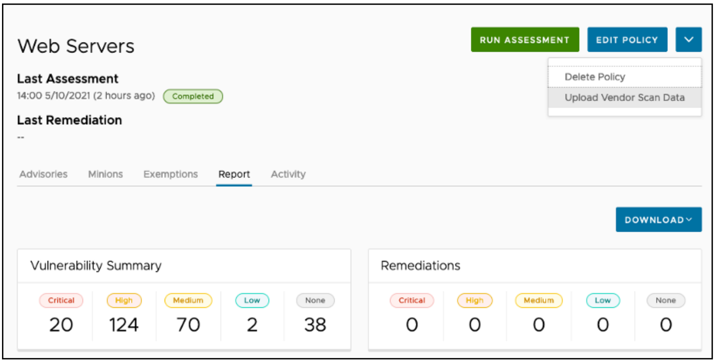
☑ 2 Items per page 20 1 - 2 of 2 items

FIGURE 4-7: Policy details after remediation and post-assessment.

Using External Vulnerability Assessments

SaltStack SecOps includes integrations with VMware Carbon Black and third-party vulnerability vendors. Choosing the down arrow in the upper-right corner of the Policies screen opens a drop-down menu with the option to Upload Vendor Scan Data (see Figure 4-8).

SaltStack SecOps supports the ability to upload or integrate vendor scan data from VMware Carbon Black, Tenable, Rapid7, Qualys, and Kenna Security (see Figure 4-9). The vulnerability assessment details will update to show your assessed posture in the policy if you choose to use an external vulnerability scanner.



Last Assessment
14:00 5/10/2021 (2 hours ago) Completed

Last Remediation
--

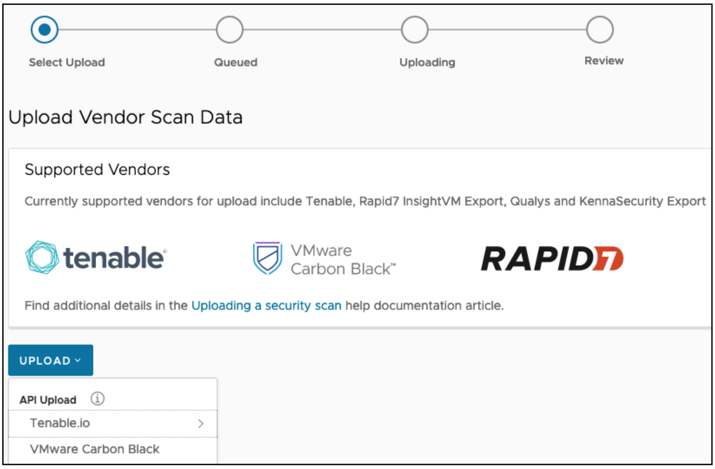
Vulnerability Summary

Critical	High	Medium	Low	None
20	124	70	2	38

Remediations

Critical	High	Medium	Low	None
0	0	0	0	0

FIGURE 4-8: Accessing the Upload Vendor Scan Data option.



Upload Vendor Scan Data

Supported Vendors

Currently supported vendors for upload include Tenable, Rapid7 InsightVM Export, Qualys and KennaSecurity Export

tenable VMware Carbon Black RAPID7

Find additional details in the Uploading a security scan help documentation article.

FIGURE 4-9: Uploading vendor scan data.

IN THIS CHAPTER

- **» Creating role-based access controls for a SecOps workflows**
- **» Working with SaltStack Config SecOps Enterprise APIs**
- **» Putting Enterprise APIs to work**

Chapter 5 Customizing SecOps Tool Chains for Your Organization

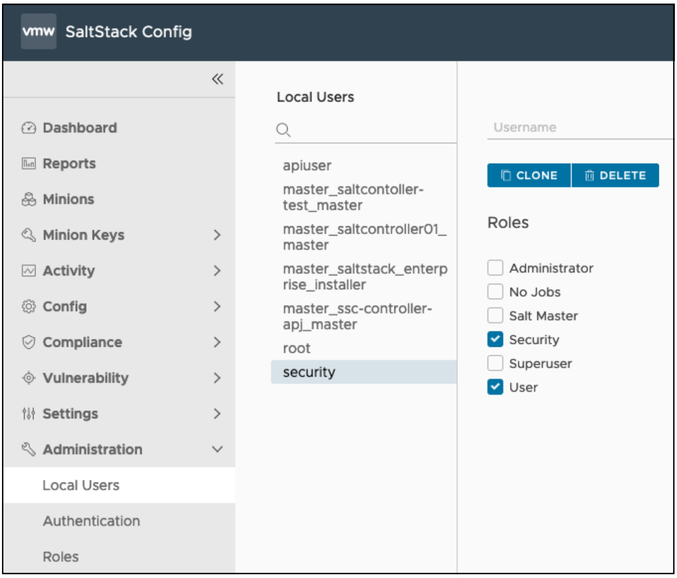
This chapter shows you how to create role-based access controls (RBAC) for SecOps workflows. It also introduces the SaltStack Config Enterprise APIs (eAPIs), a powerful way to incorporate compliance and vulnerability management into your DevSecOps methodologies and as part of your continuous integration/continuous deployment (CI/CD) infrastructure pipelines. Finally, this chapter provides examples of APIs in action.

Ensuring continuous compliance and vulnerability management before you release templates in the final stages of your pipelines is critical to operations as your business continues on a digital transformation journey to modern applications and services.

Using Role-Based Access Controls

RBAC in SaltStack SecOps allows organizations to control access to objects and define the permissions users will have over those objects. As an example, many organizations designate personnel with the roles required to manage the state of the operating systems used throughout their environment. Usually, security teams are charged with creating security and compliance policies, managing those policies, and running assessments of the operating systems under management. Then, after the security team completes running assessments, an operations team typically handles remediation of the operating system. SaltStack SecOps' RBAC controls enable organizations to define roles and permissions, which helps create and maintain separation of duties between the teams serving these roles. In many cases, a separation of duties is required by organizations.

When you log into SaltStack Config SecOps as an administrator, clicking Administration opens the user and role management parts of the product (see Figure 5-1).



Local Users

apiuser
master_saltcontoller-test_master
master_saltcontroller01_master
master_saltstack_enterprise_installer
master_ssc-controller-apj_master
root
security

Roles

☐ Administrator
☐ No Jobs
☐ Salt Master
☑ Security
☐ Superuser
☑ User

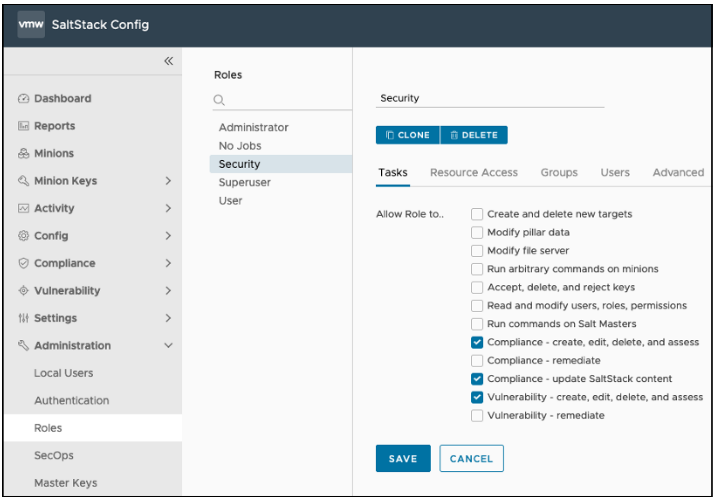
FIGURE 5-1: Assigning roles to define user permissions.

Selecting Local Users opens a screen where you can assign *roles* (responsibilities) to local users. You also can synchronize users and groups from an external directory, such as Microsoft Active Directory.

In either case, you define permissions for users by assigning roles to them. After you define a user, you can add that user to a role, which determines what they can do within the interface.

In the example shown in Figure 5-1, we created a security user and assigned that user the roles User and Security. User is a default role, whereas the Security role was created with specific permissions for a security persona.

If you select the Security role and click the Tasks tab, a series of tasks appears (see Figure 5-2). Notice that the Security role only has the permissions required to create compliance and vulnerability polices, run assessments, and update the content used for assessments. Importantly, the security user does not have permissions to remediate compliance or vulnerability issues; only the operations admin has permissions necessary to complete these tasks.



Security

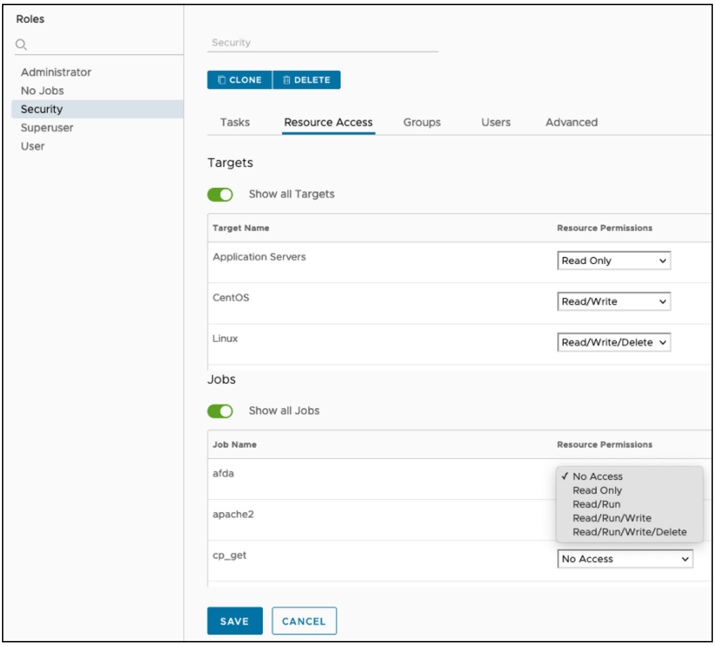
Allow Role to..

- □ Create and delete new targets
- □ Modify pillar data
- □ Modify file server
- □ Run arbitrary commands on minions
- □ Accept, delete, and reject keys
- □ Read and modify users, roles, permissions
- □ Run commands on Salt Masters
- ☑ Compliance - create, edit, delete, and assess
- □ Compliance - remediate
- ☑ Compliance - update SaltStack content
- ☑ Vulnerability - create, edit, delete, and assess
- □ Vulnerability - remediate

FIGURE 5-2: Viewing the permissions assigned to a role.

SaltStack Config includes numerous predefined jobs you can use to determine and change the state of a minion. Predefined jobs are useful for patching or updating a VM as part of a remediation or any other state changes related to compliance and vulnerability management.

The RBACs in SaltStack Config allow admins to limit the targets and jobs a role can access (see Figure 5-3). By default, no access is granted to targets and jobs already defined in the system. Any new job needs to have access explicitly granted. Many options are available for permissions, including read only, read/write, read/write/delete, and run; the options available depend on the target or job you select. (To see more about how targets and minions work in SaltStack Config, see Chapter 3.)



Target Name	Resource Permissions
Application Servers	Read Only
CentOS	Read/Write
Linux	Read/Write/Delete

Job Name	Resource Permissions
afda	✓ No Access
apache2	
cp_get	No Access

FIGURE 5-3: RBAC in the Resource Access view.

REMEMBER

After the user and roles are defined, as expected, the objects a user can access and the actions that user can perform on those objects are determined by their role.

SaltStack Config Enterprise API

SaltStack Config has a full enterprise application programming interface (eAPI) that allows users to accomplish tasks without using the user interface (UI). Clients (including the UI and all configured Salt masters) can use the eAPI to connect to SaltStack Enterprise (SSE). An API request endpoint is used to authenticate, send requests, and return data from the SSE server.

Communication via eAPI can happen in two ways:

- **A remote procedure call (RPC) client that works over a WebSocket connection:** RPC calls are accessed via Python code using the APIClient, which is installed as part of the SSC master plugin.
- **Calls made using an HTTP/S bridge:** Tools such as Postman can be used with the HTTP/S bridge as well.

TECHNICAL STUFF

Full details of the eAPI are beyond the scope of this book. For more information, you can access the eAPI Documentation from the SaltStack Config help documentation after logon by clicking the question mark link in the upper-right corner of the UI.

Getting Started Using eAPI

This section provides examples to get you started using the eAPI. These examples leverage Python to make an RPC call and can be run directly on the master or remotely. APIClient, imported in the Python code, is the purpose-built client that is installed as part of the SSC master plugin. The plugin is available on `https://customerconnect.vmware.com` (formerly My VMware) in the vRealize Automation downloads section.

The eAPI examples used in this section are from the auth, sec, and vman interface sections of the documentation. The auth interface allows management of the administration functions, including user, group, and roles management, among other options. The sec and vman interfaces focus on compliance and vulnerability aspects of the product respectively, including policy creation and management, running assessments, and remediations.

TIP

For many more options beyond the examples provided in this section, see the product documentation in the SaltStack Config help menu.

Note: The universally unique identifier (UUID) and login credentials are examples only. Be sure to replace the values in the Python code with details from your environment.

Creating users and assigning user roles

The first example uses eAPI to create a user and assign a role to that user. The example is essentially the same process that was used to create a user and assign a role earlier in this chapter.

```
from sseapiclient import APIClient
client = APIClient('https://localhost', 'root',
  'salt')
response = client.api.auth.save_
  user(username='security',
  config_name='internal', password='VMware1!',
  roles=['Security'])
```

Requesting lists of existing targets

Before creating a policy, you need to determine the UUID for existing targets. ***Remember:*** A target is used during policy creation and represents the group of minions the policy covers. This example returns a list of configured targets using the response and print options:

```
from sseapiclient import APIClient

client = APIClient('https://localhost', 'root',
  'salt')

response = client.api.tgt.get_target_group()

print(response)
```

Creating policies

In most cases, you'll use existing policies that are configured within the user interface. You can create a policy and assign specific targets, benchmarks, checks, variables, and exemptions using the eAPI, as well.

```
from sseapiclient import APIClient
client = APIClient('https://localhost or remote
  FQDN', 'root', 'salt')
client.api.sec.save_policy(
    name="Ubuntu",
    tgt_uuid="61edbf8c-8b5c-483c-845b-ff12280aa171",
    benchmark_uuids=["b4109610-1ca0-4e21-b03f-
35159c25089b"],
    check_uuids=[
       "55c17549-095a-4dba-9817-0db845385eeb",
       "985b5057-42c8-4c86-8c8e-06d8b3f51472",
       "a2f200b6-6040-46bb-9005-9725e9b65490",
       "c0df2e2d-13df-457a-bbca-cb0cbf495525"
       ],
    variables=[{
        "check_uuid": "985b5057-42c8-4c86-8c8e-
06d8b3f51472",
        "name": "_locke.system.service.sshd_
maxauthtries.SSHD_CONFIG_MAXAUTHTRIES",
        "value": "3"
    }]
)
```

Listing all policies

In this example, we find a list of policies using eAPI and then run a policy assessment for the policy with one of our associated UUIDs. `client.api.sec.get_policies` is used to request compliance policies, and `client.api.vman.get_policies` is used for vulnerability policies.

```
import APIClient
from sseapiclient
client = APIClient('http://localhost', 'root',
  'salt')
client.api.sec or vman.get_policies()
```

Listing specific policies

You can also call the policy by using the UUID in the response. A summary of the policy, including name, target, assessment, and remediation information appear in the response.

```
import APIClient
from sseapiclient
client = APIClient('http://localhost', 'root',
  'salt') client.api.sec.get_policies(
    policy_uuids=[
        "f768e864-b5c2-494f-a116-8c335edcb7bd",
        "292372eb-ce12-4c6f-bbfc-bf916ba02649"
    ],
    include_stats=True
)
```

Running assessments against existing policies

This example triggers an on-demand assessment by using the configurations set in a given policy.

```
from sseapiclient import APIClient
client = APIClient('https://localhost', 'root',
  'VMware1!')
response = client.api.sec.
  assess_policy(policy_uuid="b1061eb1-8869-451f-
  8f93-9a07931c81bd")
print(response)
```

Running remediations against existing policies

This example triggers an on-demand remediation using the configurations set in a given policy.

```
from sseapiclient import APIClientclient =
  APIClient('https://localhost', 'root', 'salt')

response = client.api.sec.remediate_policy(

policy_uuid="f01f9da5-478d-4882-8cd2-3874c2429c76"
)

print(response)
```

IN THIS CHAPTER

- **Assessing your current security posture**
- **Fixing any gaps identified in your security audit**
- **Evangelizing your SecOps successes**
- **Automating your SecOps process**

Chapter 6 Ten Important Milestones on Your SecOps Journey

With so many ways available to begin implementing SecOps, getting started can feel a little daunting. This chapter is here to help! Incorporate the following ten milestones into your organization's SecOps journey, and you'll be on your way to SecOps success. The SecOps principles you apply will deliver fast value and help make your organization more secure.

Here are those milestones:

- **Identify and review your organization's corporate security policies, and work with your security team to update them, if needed.** Most organizations have established security plans. If you're unfamiliar with your organization's security plan, start a conversation with the security team to understand the expectations and compare them to reality. If security plans are inaccurate or outdated, consider updates and review them with the appropriate IT and security owners.

- **Use the "SecOps scorecard" found in Chapter 2 to understand the current state of IT security in your organization.** Identifying the unique security strengths and weaknesses of your organization can help you determine and prioritize ways to improve.
- **Audit and document your organization's existing processes for executing compliance and security tasks.** Too often these tasks occur in silos, making it difficult to visualize and understand processes from start to finish.
- **Perform a gap analysis based on your audit, and identify problem areas or opportunities for improvement.** After you identify and document current processes, look for areas where key steps are missing or ineffective or creating bottlenecks. As part of this analysis, you may even identify complete breakdowns in procedures.
- **Meet with key stakeholders to discuss and prioritize identified issues and opportunities.** Present your findings to key security and IT stakeholders, and start a discussion on how to begin improving processes.
- **Designate a "SecOps champion" and form a cross-functional team that can focus on solving key issues.** This individual or group of individuals should have a good understanding of both IT and security systems, and act as an objective consultant, collecting feedback and coming up with ideas to address risks.
- **Find or build tools to help bridge the gaps and streamline IT security processes.** After you establish priorities and identify a champion to begin addressing them, look for tools that can be used to help solve key challenges.
- **Promote SecOps in your organization.** Hold educational meetings, include SecOps information in your organization's security newsletters, and evangelize your SecOps wins. Doing so is a great way to get a conversation started and begin cultivating a healthy SecOps culture.
- **Automate key compliance and security processes.** Doing so enables you to shift precious human resources away from repetitive tasks and focus them on critical challenges.
- **Build an integrated, "closed-loop" solution for identifying, prioritizing, remediating, and reporting back on vulnerabilities.** This can involve connecting existing tools and processes, and communication between security and IT teams. The end result should be increased speed and efficiency in addressing discovered vulnerabilities and compliance issues.

Discover all you need to know about SecOps

Digital organizations are moving fast to meet the needs of their customers. IT security must evolve to meet the needs of today's organizations. Existing security processes are often too slow, inefficient, and siloed. If your organization is looking for a way to provide security and agility, *SecOps For Dummies* is for you. This handy guide explains everything you need to know about SecOps, including what SecOps is, why it's important, and how you can use it to secure and optimize your critical business systems. This practical guide also explains in plain English the ins and outs of SecOps and how your organization can quickly benefit from it.

Inside...

- Understand what SecOps is
- Get a clear picture of IT security challenges
- Assess your SecOps needs
- Develop SecOps-focused solutions
- Learn to enforce compliance with automation
- Discover how to find and fix vulnerabilities
- Customize SecOps Tools to meet your needs

vmware®

Kendall Lovett is a Senior Product Line Marketing Manager on VMware's Modern Apps and Management Unit. **Karl Fultz** is a Staff Technical Marketing Architect on VMware's Modern Apps and Management Unit.

ISBN: 978-1-119-81394-1
Not For Resale

9 781119 813941

for dummies®
A Wiley Brand