Progress® Chef®

Chef InSpec Best Practices

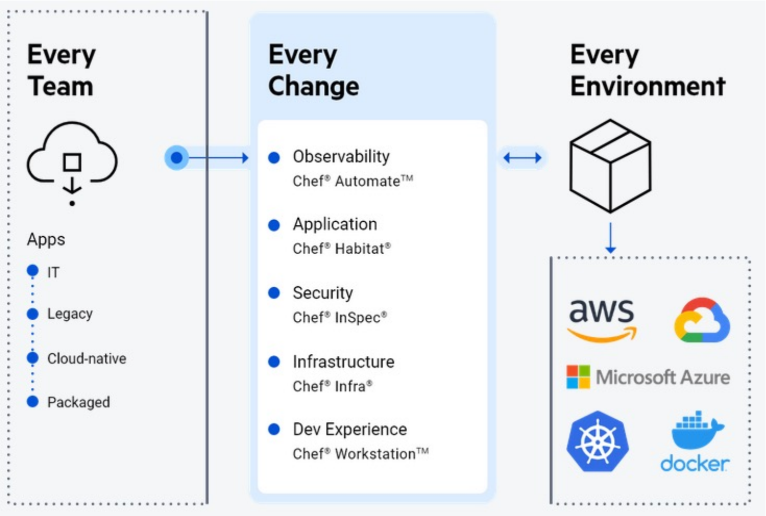
Optimize Your Chef Compliance Automation Investment

EBOOK

The Secure Infrastructure Automation Journey

Provisioning and deploying infrastructure across an organization at scale is a process that taxes resources and manpower. It is susceptible to human failures and configuration errors if not handled efficiently.

Securing and maintaining the compliance state of IT resources only adds to existing IT complexities.



With Chef's Policy as Code, compliance processes become automated and easy to maintain. Chef Compliance breaks down complex routines into repeatable functionalities with the ability to run on any system.

Transform into a secure and compliant coded enterprise with Chef.

- **Integrate compliance into infrastructure and application delivery** – Get the power of Chef InSpec and certified Premium Content to ensure compliance at scale.
- **Automation made easy with Chef EAS** – Utilize the complete range of Chef products to enable consistency, velocity, and security in application delivery on any infrastructure.
- **Enhance continuous delivery with an emphasis on test-driven-development** – Easily automate the delivery of heterogenous environments with increased system coverage and cloud support.

5 Chef InSpec Facts

1. An open-source framework based on RSpec, used for testing and auditing your applications and infrastructure.

2. Compares the actual state of your system with the desired state that you express in the easy-to-read and easy-to-write code.

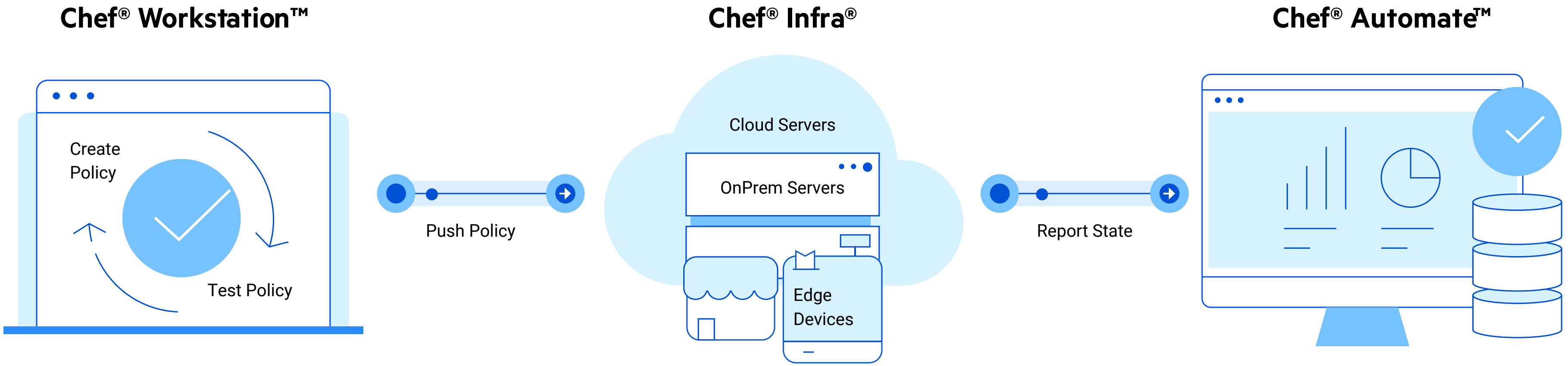
3. Detects violations and displays findings in the form of a report but puts you in control of the remediation.

4. Chef InSpec provides a **consistent** DSL that is **platform agnostic** to check the status of any component.

5. InSpec does not require an agent, or even ruby, to be on a target node in order to scan a system.

Chef Policy-Based Secure Infrastructure Automation Architecture

Using Chef Infra to automate configuration management allows DevOps teams to define repeatable, consistent and reusable policies. The result is increased business agility and security because all systems and resources are continuously and automatically evaluated, corrected and modified.



Chef Workstation

Reduce risks by iterating on policy changes before pushing them to production. Workstation includes:

- **Chef Tools:** Chef Infra Client, Chef InSpec, Chef Habitat, Chef Cookstyle and knife
- **Chef Language:** Pre-built resources for managing systems and helpers that make authoring and distributing cookbooks easy

Chef Infra Client and Server

Enforce policy by converging systems to the state declared by Chef resources. Chef Infra Client key capabilities include:

- Planned, unstructured and policy-based updates
- Dynamic behavior support
- Ephemeral resource management
- Data collection

Chef Automate

View and validate intended and actual state across all systems. Chef Automate key capabilities include:

- Real-time interactive dashboards
- Role-based access controls
- Third-party integrations
- Data APIs
- Chef Infra Server management

Shift-Left Security Testing

Testing for security and compliance is a significant challenge for dev teams, and it has a direct impact on application delivery. If development and testing processes are not optimized, it introduces vulnerabilities in the system that impact security, stability and performance.

Incorporating security testing in every phase of the software development cycle is the only way to achieve stable and reliable release cycles. Test driven development (TDD) results in shorter design cycles that help deliver resilient software consistently.

With Chef InSpec, implementing TDD is easier as TDD uses policy as code to secure infrastructure irrespective of scale. As a result, you can continually evaluate business requirements by shifting security testing left, developing the right tests, and driving good software design.

Benefits

- Reduces risks in the deployment phase; errors are caught and fixed before they reach production.
- Incorporates security testing into every phase of software delivery, minimizing security breaches and vulnerabilities.
- Improves code quality with repeated testing.
- Enables automation and continuous delivery at scale.
- Reduces time taken to debug code, and overall script maintenance is more manageable.

Resources

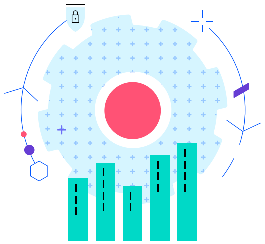
Webinar: Test Driven Development with Chef Workstation

InSpec Linting in Chef Cookstyle

inspec check is a top-level linting command that checks InSpec profiles for errors, missing metadata, and other common style issues.

Key benefits of Cookstyle integration with InSpec linting:

- Enforcing style conventions and best practices.
- Helping every member of a team author code that is structured the same.
- Maintaining uniformity in the source code.
- Detecting deprecated code that creates errors after upgrading to a newer release.
- Detecting common Chef InSpec mistakes that cause code to fail or behave incorrectly



Build Business Aligned Policies Using InSpec Controls

An InSpec control is a descriptive wrapper for your tests. Controls allow you to group tests that are logically related. It also allows you to put some logic around how and when your tests run. Controls are also inheritable between InSpec profiles that are dependent upon each other.

InSpec Profiles are made up of controls, which bundle one or more InSpec resources into blocks that define one or more expectations for your target systems. It also allows you to add logic about how, when, and where your tests run.

Where a control might be a simple logical grouping of describe blocks, it also allows the user to add metadata that will show up in reporting when the controls are used in compliance scanning. For example, a control metadata like “title” and “desc” helps understand what the tests in the control are for.

Benefits

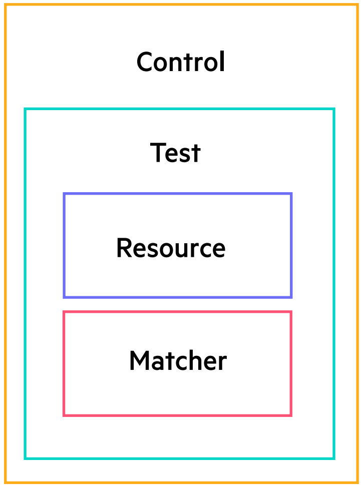
- The metadata determines the importance of control. For example, how does it impact the system should a system fail to pass the tests within the control.
- Controls can also create the scenario where only one describe block needs to have passing tests in order for the control to succeed.

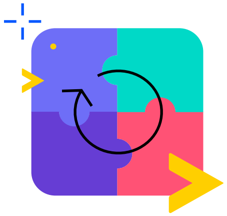
Resources

- **Video:** Chef InSpec Profile Basics
- **Webinar:** Chef InSpec Security Profile Basics

Add Metadata to Meet the Needs of Your Entire Business

There’s even more metadata that can be included in a control, such as tags, references and longer descriptions.





Test More than Cookbooks with Chef InSpec

A cookbook is the fundamental unit of configuration and policy distribution in Chef Infra. It is a collection of Chef Infra recipes that define everything required to support a specific environment and all the actions needed to configure a system. Chef InSpec is a security testing solution that defines policies as code and provides continuous visibility into compliance status across all systems and teams. Easy-to-read controls describes system state expectations in ways that can be mapped directly to policies defined by Chef Infra, providing tools and insights into how to remediate any misconfigurations uncovered in audits. Integrating Chef cookbooks with Chef InSpec profiles has been simplified. This enables InSpec user in creating cookbooks through Chef Workstation and Test Kitchen

Chef InSpec Rules	Integration tests	Compliance scan
Types of Rules	Governed by the developmental processes (cookbook) requirements	Generic rules defined by industry security requirements (not governed by the application requirements)
Location of Rules	Shipped with a cookbook	Stored centrally (Compliance server, GitHub)
Invocation	Use Test Kitchen to provision a sandbox environment to perform functional tests of the cookbook	Use Chef InSpec DSL or Chef Automate to perform compliance tests during development, or in production

Chef Compliance Automation for Secure Infrastructure

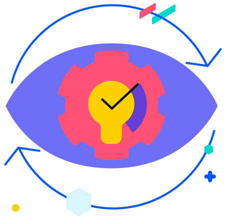
- Defines policies and system configurations as code to integrate with automated pipelines.
- Detect and correct configuration drift to ensure the entire infra is in the desired state.
- Manage diverse systems irrespective of OS.
- Maintain security and compliance with minimum effort.
- Allows security and compliance to shift-left, increasing release velocity:

Benefits

- Assets within organizations are ensured that these are always secure and conform to regulatory and industry standards. Chef can scale large heterogenous IT fleet of million assets.
- Cookbooks with security tests defining firewall rules, ports, SSL, and other baselines, and compliance tests defining regulatory, or industry requirements can be tested in Test Kitchen and validated seamlessly through easy-to-read and easy-to-write code.

Resources

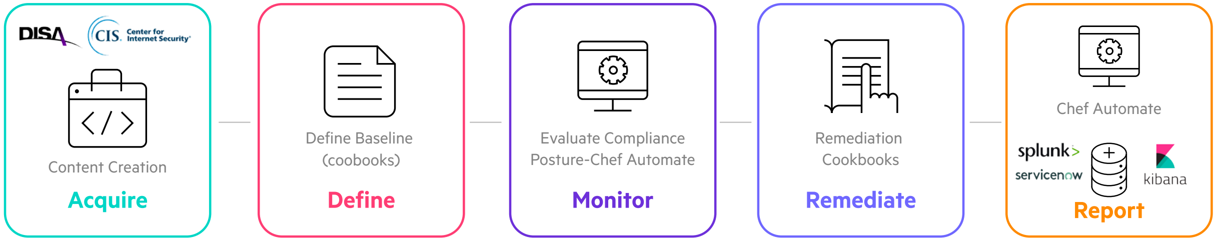
- **Webinar:** Scaling Infrastructure Testing with Chef InSpec
- **Blog:** Chef InSpec Best Practices: #1 Scaling Infrastructure Testing



System Hardening with Chef InSpec

System hardening is a method of preventing cyberattacks, enabled by reducing security drifts in servers, applications, firmware and other areas. System hardening is achieved with the help of infrastructure and security management tools that help audit all systems, detect potential attack vectors and minimize the attack surface.

With Chef Compliance, enterprises can maintain security across hybrid and multi-cloud environments while also improving processes' overall efficiency and speed. Chef enables IT teams to perform system hardening with the help of continuous security audits and remediation that detects and fixes any security drifts in diverse IT fleets.



Benefits

- **Improved security postures:** Continuous audits and remediation based on CIS and STIG standard profiles. This means all misconfigurations are detected and addressed, ensuring reduced risk of data breaches, malware and unauthorized access.
- **Better auditability:** Easy-to-read code that works across all platforms and Operating systems. Chef's curated profiles make complex security audits easier, fast and more transparent.
- **Improved system functionality:** With error-free automation, speed of processes, consistency of configurations, and fully secure infrastructure, Chef improves the overall efficiency of all systems in the fleet and the productivity of the workforce.

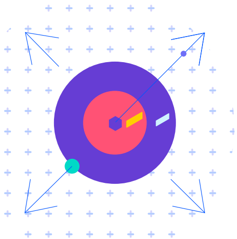
Fact check: System Hardening

Policyfiles are particularly useful if you encounter one of the scenarios:

- According to a 2020 research study conducted by global intelligence firm IDC, "Security misconfiguration/lack of system hardening" was one of the top security concerns indicated by 67% in the survey of 300 CISO's.
- To further illustrate the challenge, Gartner Group predicts that over the next five years, "At least 99% of cloud security failures will be the customer's fault." Many of these are errors resulting from misconfigurations or lack of system hardening.

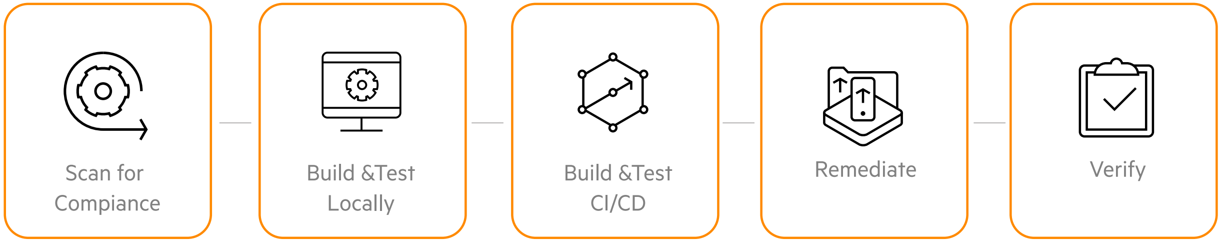
Resources

- **Blog:** What is System Hardening? Standards and Best Practices
- **Whitepaper:** Harden Your Systems Using CIS and DISA STIGs Benchmarks

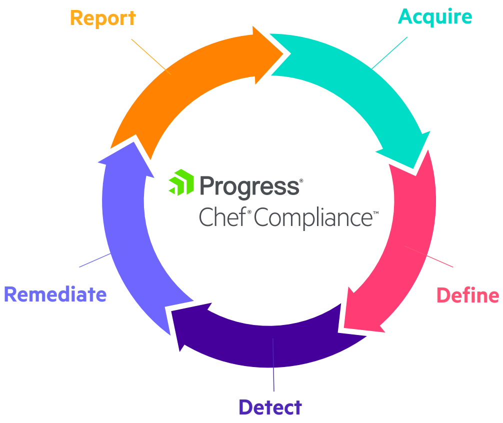


Audit and Remediate with a Single Solution

Chef InSpec enables continuous compliance by streamlining and automating all the manual processes involved during audits. Incorporating compliance at every stage of development will resolve most of the potential complexities that arise during the software delivery phase. With Chef, you have a single solution to handle on-demand auditing and remediation and gives customers a consolidated view of their organization’s security and compliance status in real-time.



Chef Continuous Compliance



Benefits

- **Audit for Security:** Implement continuous security assessments and easily tune/customize audits to quickly identify new Common Vulnerabilities and Exposures (CVEs).
- **Audit for Compliance**: Pair compliance checks with CIS or DISA-STIGs benchmarks to maintain continuous compliance.
- **Test Configuration:** Verify configuration management results to enhance the effectiveness of existing infra management and testing tools.

Resources

- **Documents:** Compliance Automation
- **Blog:** Audit and Remediate with a Single Solution - Chef InSpec
- **Webinar:** Compliance Automation to the Rescue

Streamline Security Testing with Chef Infra Compliance Phase

Chef Infra Client Compliance Phase replaces the existing audit cookbook, enabling compliance and auditing reporting. It uses the Chef InSpec engine as part of any Chef Infra Client run without the need for the audit cookbook. The compliance phase is fully backwards compatible with the audit cookbook.

The Compliance Phase also features a compliance reporter: `cli`. This report mimics the Chef InSpec command line output giving you a visual indication of your system's compliance status.

Existing audit cookbook users can migrate to the new Compliance Phase by removing the audit cookbook from their run_list and setting the `node['audit']['compliance_phase'] = true`

Benefits

- **Zero Dependencies:** Compliance out of the box without the need for solving or managing cookbook dependencies.
- **Simplified Upgrade:** Compliance code upgrades with your Chef Infra Client releases so you always have a working solution.
- **Reduced Server Dependency:** No cookbook code to fetch from the server. Perfect for high latency or air-gapped environments.

Resources

- **Documents:** Chef Infra Compliance Phase
- **Blog:** Serve-up Continuous Compliance with Chef Infra Compliance Phase
- **Webinar:** Configure Chef Infra & Compliance Using Built-In Functionality

Chef InSpec and Chef Infra Better Together

Chef Infra Compliance Phase simplifies the workflow needed to run Chef InSpec compliance audits, view results and do analysis. It extends our policy-based approach to configuration enabling a single agent than can handle the end-to-end workflow from state enforcement to, data aggregation to validation.

Take Advantage of Reporting, Alerts and Analytics

Chef Automate platform offers comprehensive reporting and alerting enabling developers, operations engineers and security engineers to collaborate on application and infrastructure changes while remaining secure and compliant.

Enable compliance automation through Chef Automate. Use one of Chef Automate's 90+ baseline profiles to quickly get started with compliance rules. Get access to SCAP and Microsoft SCCM XML converters to import external content into InSpec format.

Benefits

- Single dashboard for all compliance and infra data.
- Debug and determine root cause of Chef run failures.
- Gain operational visibility across the entire fleet.
- Get alerted immediately through chat or webhook for critical events of interest.

Resources

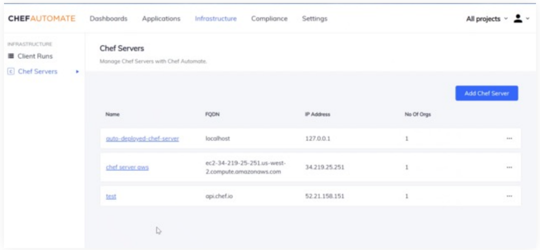
Documents: [Chef Automate Datasheet]

Documents: [Continuous Delivery Whitepaper]

Blog: [Getting started with Chef Automate in public clouds or on-prem]

Video: [Using Chef Automate for Infrastructure Managemen]

Chef Automate Compliance Management Dashboard



Chef Servers

Manage Chef Servers with Chef Automate.

Name	FQDN	IP Address	No Of Orgs	
auto-deployed-chef-server	localhost	127.0.0.1	1	···
chef server aws	ec2-34-219-25-251.us-west-2.compute.amazonaws.com	34.219.25.251	1	···
test	api.chef.io	52.21.158.151	1	···

The Chef Automate Enterprise dashboard and analytics tool allows you to:

- Get real-time data across the IT estate.
- Collaborate effortlessly across teams.
- Use powerful auditing capabilities.
- Implement intelligent access controls.
- Use built-in compliance assets.
- Identify actionable insights for compliance.

Jump Start Audits with CIS Aligned Benchmark Profiles

CIS Benchmarks and The Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGs) are a set of best practices and standards for configuring a secure system.

With Chef Compliance, you can create and test secure Chef configuration Cookbooks and InSpec Compliance Profiles, based on the CIS and DISA STIG Benchmarks. This allows you to protect against malware, insufficient authorization and remote intrusion.

Any organization operating in an industry governed by regulations, such as PCI DSS or NIST, can quickly audit and remediate systems using CIS-aligned audit profiles available with Chef Compliance.

Benefits

- Leverage ready-to-use, certified, curated audit and remediation content to quickly configure and maintain compliant systems.
- Automate auditing to ensure vulnerabilities are identified faster and eliminate risk of human error.
- Chef Compliance offers extensibility and flexibility, customize pre-packaged remediation content to suit specific requirements.

Resources

- **Guide:** Chef Automate Guide to PCI DSS Compliance
- **Video:** Chef Compliance An Update Story
- **Blog:** Chef Premium Content

Chef Premium Content

Chef Premium Content offers traditional target scanning and remediation content that allows users to easily scan an extensive set of target systems through CIS Certified and DISA STIG's referenced content. Chef Compliance offers:

- Chef Premium Content for Operating Systems.
- Chef Premium Content for Cloud Environments.
- Chef Premium Content for Chef Desktop.

Streamline Audits with Waivers

A Chef InSpec Waiver is a mechanism used to mark controls as “waived” for various reasons, and to control the running and/or reporting of those controls. It uses a YAML input file that identifies:

- Which controls are waived
- Why a description is waived
- (Optionally) whether they should be skipped from running
- (Optionally) an expiration date for the waiver

For example, you’re releasing a security fix next week, but you have tests that validate the fix rolling out as a part of this week’s release. You may want to waive the tests related to the issue until the fix is rolled out to prevent failing tests.

Benefits

- **Streamline Audits:** Chef InSpec can take waivers as input to an audit run. The result of that audit can then be piped into Chef Automate to provide complete operational visibility into the customer’s compliance posture, which now includes waivers that are applied throughout the fleet.
- **Self-Documenting:** Waivers enable you to provide a detailed explanation or reason why controls are not being run.
- **Automated Expiration:** Configuring expiration dates in your waivers automates the expiration process. Once the expiration date has passed, previously waived controls will run as expected.

Resources

- **Documents:** Chef InSpec Waivers
- **Livestream:** Getting Started with Waivers
- **Blog:** An introduction to Chef InSpec Waivers

Chef InSpec Waivers

You can use Chef InSpec’s Waiver Feature to mark individual failing controls as being administratively accepted, either on a temporary or permanent basis.

Ensure OS Patches are Properly Applied

Converting the patching process into simple, repeatable functions will make it possible to automate and scale the whole patching workflow. The patch events can be fully automated and managed easily from end-to-end using a comprehensive patch management tool like Chef.

Chef automates patch management by incorporating system patching into CI/CD pipelines. Using Chef, the I&O teams can prioritize patches, test every patch event, install on any environment and even validate the deployed patches.

Benefits

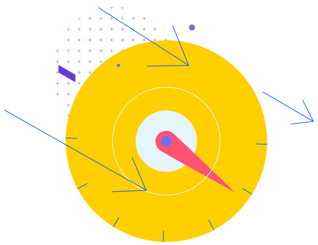
- **Efficiency:** I&O teams can focus on patch deployment without worrying about application dependencies or packaging.
- **Agility:** Automated patch management eliminates downtime as patch events are handled through tested CI/CD pipelines.
- **Reliability:** Every patch event is validated, and compliance teams can view the status of the patched systems in real-time.

Resources

- **Whitepaper**: Effective Patch Management
- **Video:** A Windows View into DevSecOps Success at Bluestem Brands
- **Blog:** Manage Your IT Resource Fleet at Scale Through Automation

TESCO

> ***"The redesigned patch management process leveraging Chef has significantly reduced the time and effort needed from engineering and application teams to patch systems, enabling them to spend more time innovating vs. remediating."***
>
> Nathan Luxford, Head of Cloud Platforms, Tesco



Simplify User Management with Identity and Access Management (IAM)

Operating complex services and environments is a collaborative effort requiring a consistent view of intended and actual system states across teams.

Chef Automate administrators can create customizations providing resource-specific authorization for users or teams, either created locally or imported from existing LDAP or Active Directory. Project data within Automate is then restricted to authorized users and teams.

Benefits

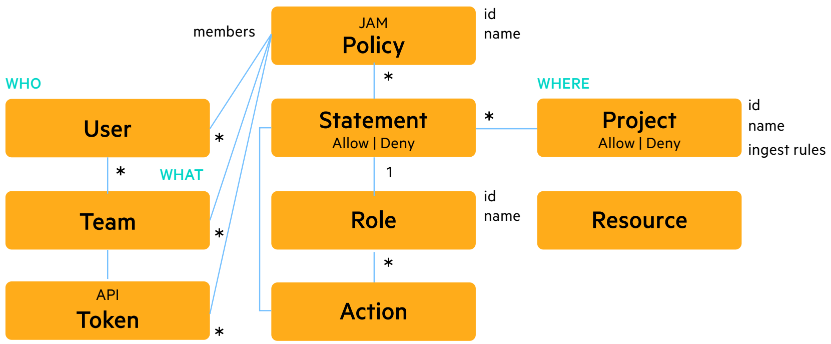
- **Secured Access:** Enhanced multi-statement policies and role-based access control with a set of built-in roles to simplify typical security configurations.
- **Project Level Control:** Project-scoped access control for up to 30 projects that limit permissions to resources defined in the project.
- **Enterprise Manageability:** Easily onboard and manage hundreds of users.

Resources

Documents: [Chef Automate LDAP Authentication via Existing Identity Management Systems]

Documents: [Chef Automate Identity and Access Management (IAM) Overview]

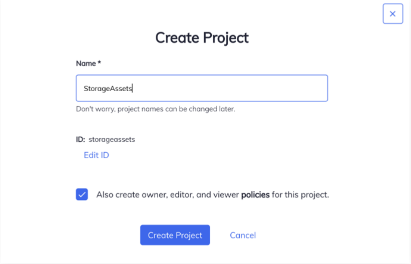
Blog: [Chef Automate Product Announcement: Identity and Access Management Release]



Chef Automate Policy Structure

Enterprise Control and Coordination

Data within Chef Automate can be restricted to the projects a user or team has access to. Notifications can be displayed on a per-node, per-failure basis, or configured for alerts to chat, webhook endpoints or ServiceNow.



Create Project

Name *

StorageAssets

Don't worry, project names can be changed later.

ID: storageassets

☑ Also create owner, editor, and viewer **policies** for this project.

Take Advantage of Chef Community Content

Chef's community is one of its key strengths, and we value the relationships and interactions we have with our members. Progress sees the contributor model Chef built as an ideal model for any open-source project. We are committed to the long-term support of the entire community. Our community's value impacts the complete DevOps and DevSecOps ecosystem, and Progress is proud to participate.

Benefits

- **Constant Support:** Help from people using Chef products at scale.
- **Access to Content:** Access to community-provided and supported resources.
- **Ongoing Collaboration:** Weekly updates from internal development teams.

Resources

- **community.chef.io - your one-stop shop for all the ways to connect to the rest of the chef community**
- **youtube.com/c/getchefdotcom - access all of the talks from the past two ChefConfs, largely from our community members!**

Get Involved with the Chef Community

Chef Community Discourse
https://discourse.chef.io

Chef Community Slack
https://community.chef.io/slack

Weekly Community Meetings
Thursdays at 9:00AM PT |
#community-meetings in Slack

Chef User Groups and Meet-Ups
https://events.chef.io/

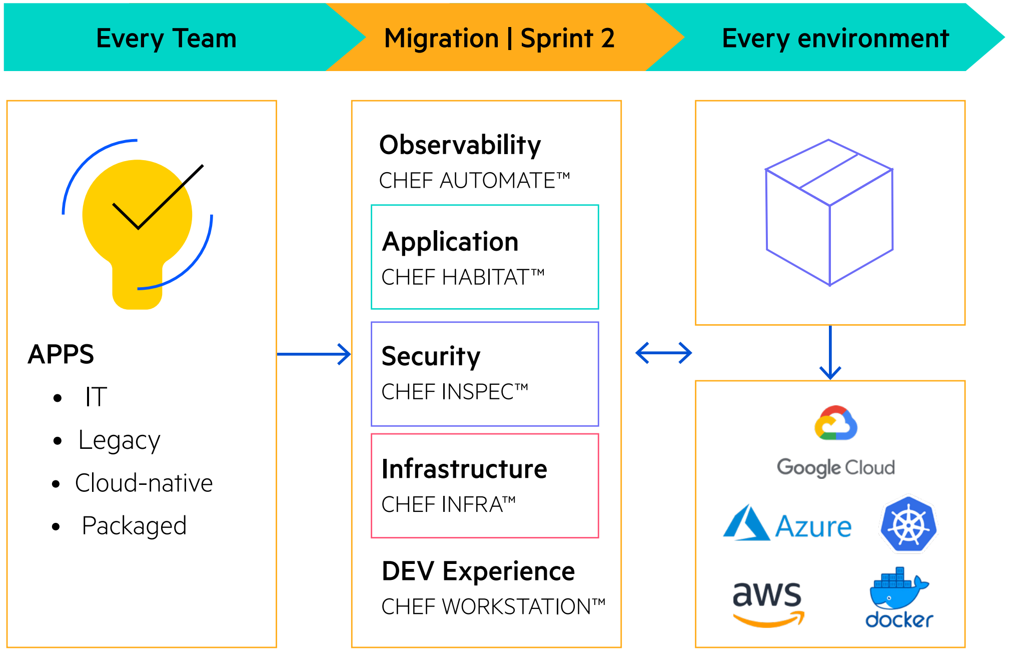
Go Beyond Infrastructure Management Automation

Chef Enterprise Automation Stack (EAS) provides teams implementing DevSecOps with a common approach for automating application delivery, infrastructure configuration and compliance auditing.

Chef InSpec provides an additional level of system state enforcement. It provides a language describing system state expectations which can directly map to policies defined for Chef Infra. The same toolkit offers insight into how to remediate any misconfigurations uncovered in audits.

Chef Habitat is the evolution of Chef's software configuration capabilities and redefines the way applications are delivered. While traditional code-based configuration solutions are acceptable for managing infrastructure as code, they are not well suited for managing service architected applications. Many dependencies require frequent updates and swift actions like stop/start/restart.

A use case Chef EAS is remarkably well suited for is managing complex applications on Windows. OS-level configuration concerns such as domains, firewalls and others can be managed with Chef Infra, while Chef Habitat handles the build and deployment of your applications itself. With Chef InSpec, you can guarantee your application is delivered safely and securely while enforcing the defined policies.



Every Team

Migration | Sprint 2

Every environment

APPS

- IT
- Legacy
- Cloud-native
- Packaged

Observability
CHEF AUTOMATE™

Application
CHEF HABITAT™

Security
CHEF INSPEC™

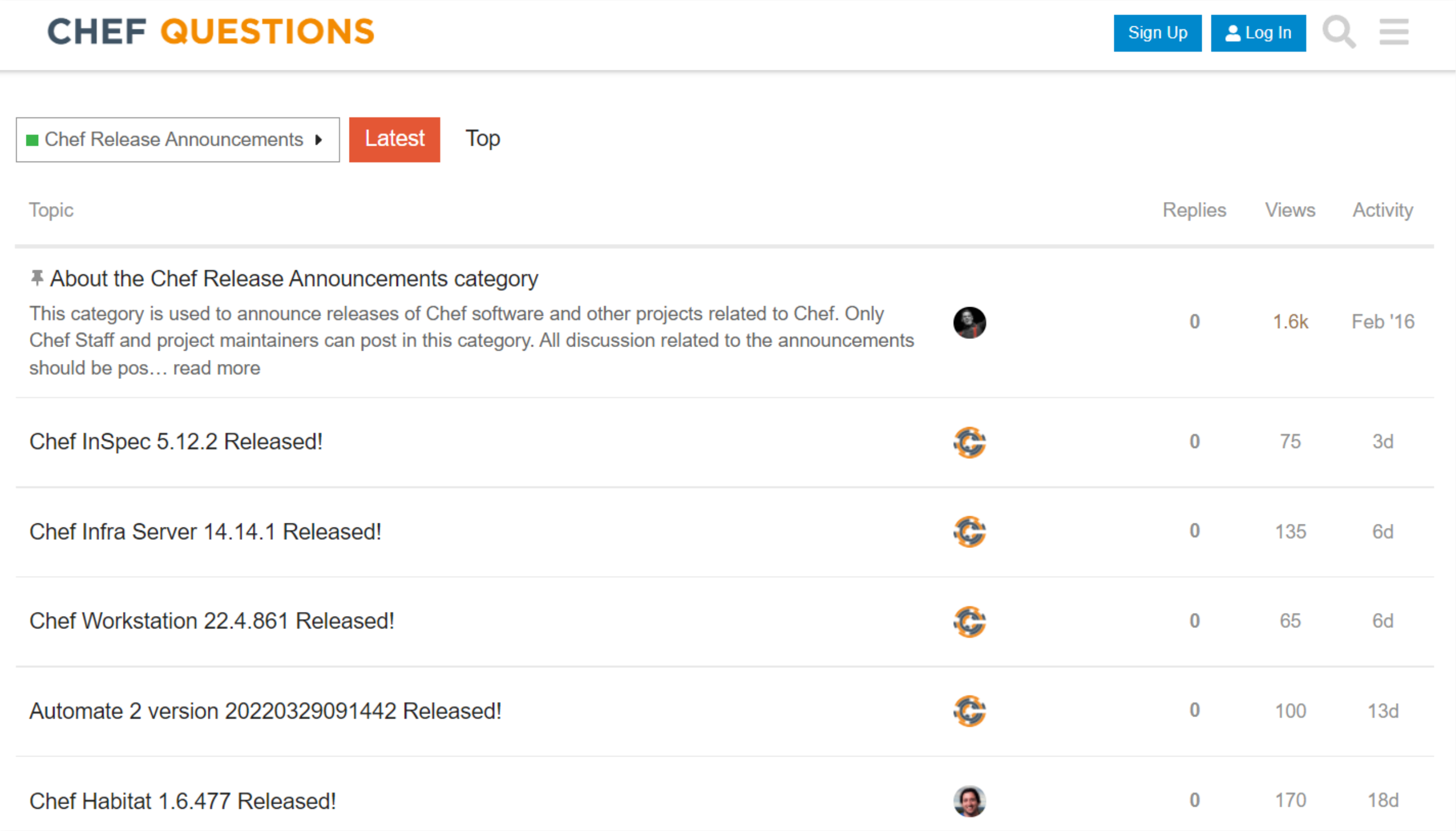
Infrastructure
CHEF INFRA™

DEV Experience
CHEF WORKSTATION™

"We not only wanted to accelerate our adoption of agile delivery practices but create an organization of developers that we taught to do operations and collaborate via code. Chef's code based approach to automation enabled us to do this and now sits as the foundation that everything else is built upon including our core applications, services, containers, etc"

Corey Johnston, Manager of Cloud Engineering, Edgenuity

Stay on Top of the Latest and Greatest from Chef



Topic	Replies	Views	Activity
About the Chef Release Announcements category This category is used to announce releases of Chef software and other projects related to Chef. Only Chef Staff and project maintainers can post in this category. All discussion related to the announcements should be pos… read more	0	1.6k	Feb '16
Chef InSpec 5.12.2 Released!	0	75	3d
Chef Infra Server 14.14.1 Released!	0	135	6d
Chef Workstation 22.4.861 Released!	0	65	6d
Automate 2 version 20220329091442 Released!	0	100	13d
Chef Habitat 1.6.477 Released!	0	170	18d

Subscribe to the **Chef Releases** Discourse Channel: https://discourse.chef.io/c/chef-release/9

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to develop the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com.

Progress®

facebook.com/getchefdotcom
twitter.com/chef
youtube.com/getchef
linkedin.com/company/chef-software
learn.chef.io
github.com/chef
twitch.tv/chefsoftware