

SonarQube Training


Admin Session

A journey in the land of code quality and security



Agenda

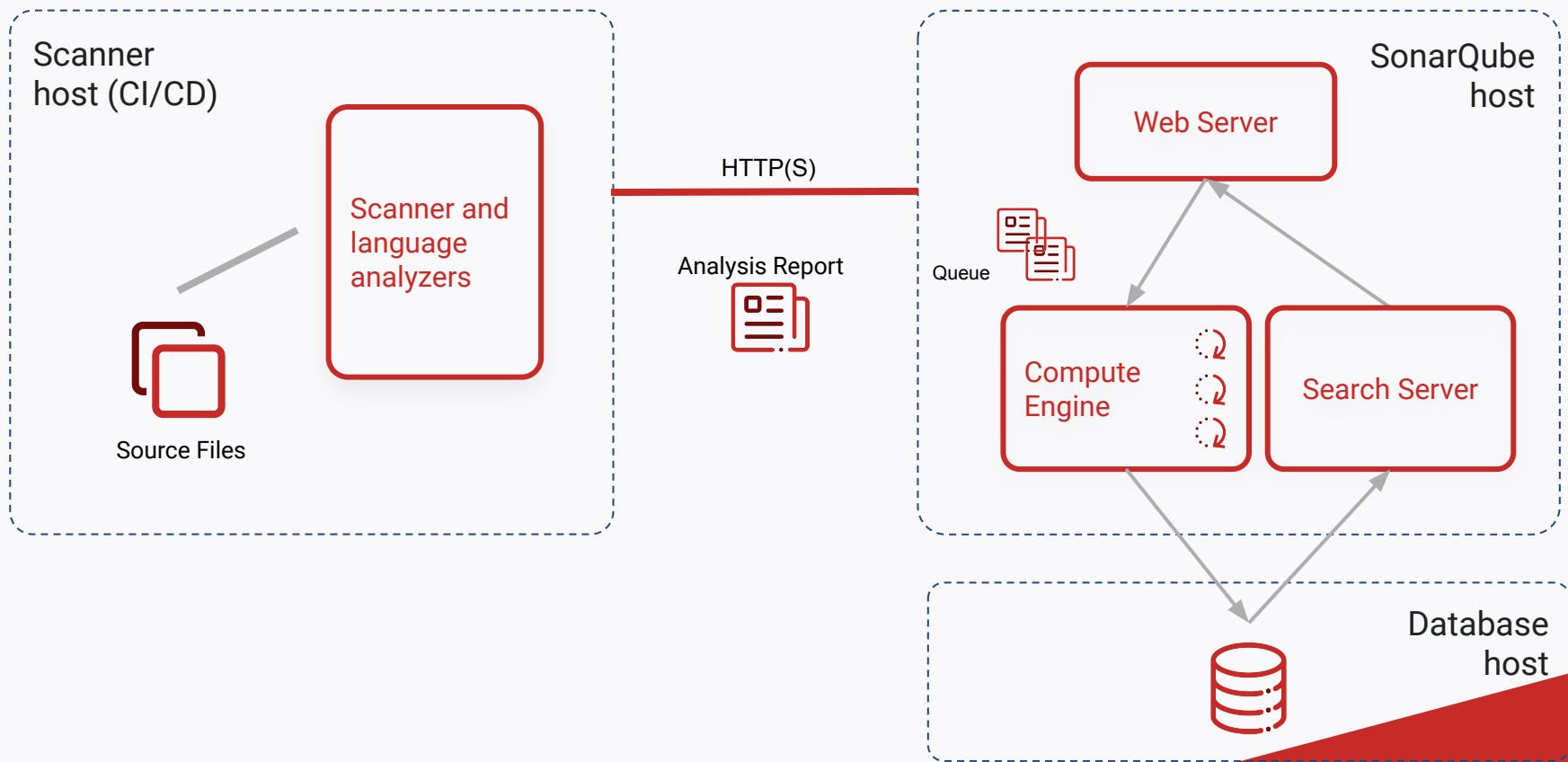
Admin Session

- SonarQube Architecture Overview
 - Platform performance tuning, scaling
 - Setting up Portfolios & Applications
 - Securing your platform & other administration topics
 - Roadmap
 - Working (well) with our Support team
 - Product news and updates
- 
- A large red triangle is located in the bottom right corner of the slide, pointing towards the top right.

SonarQube Architecture

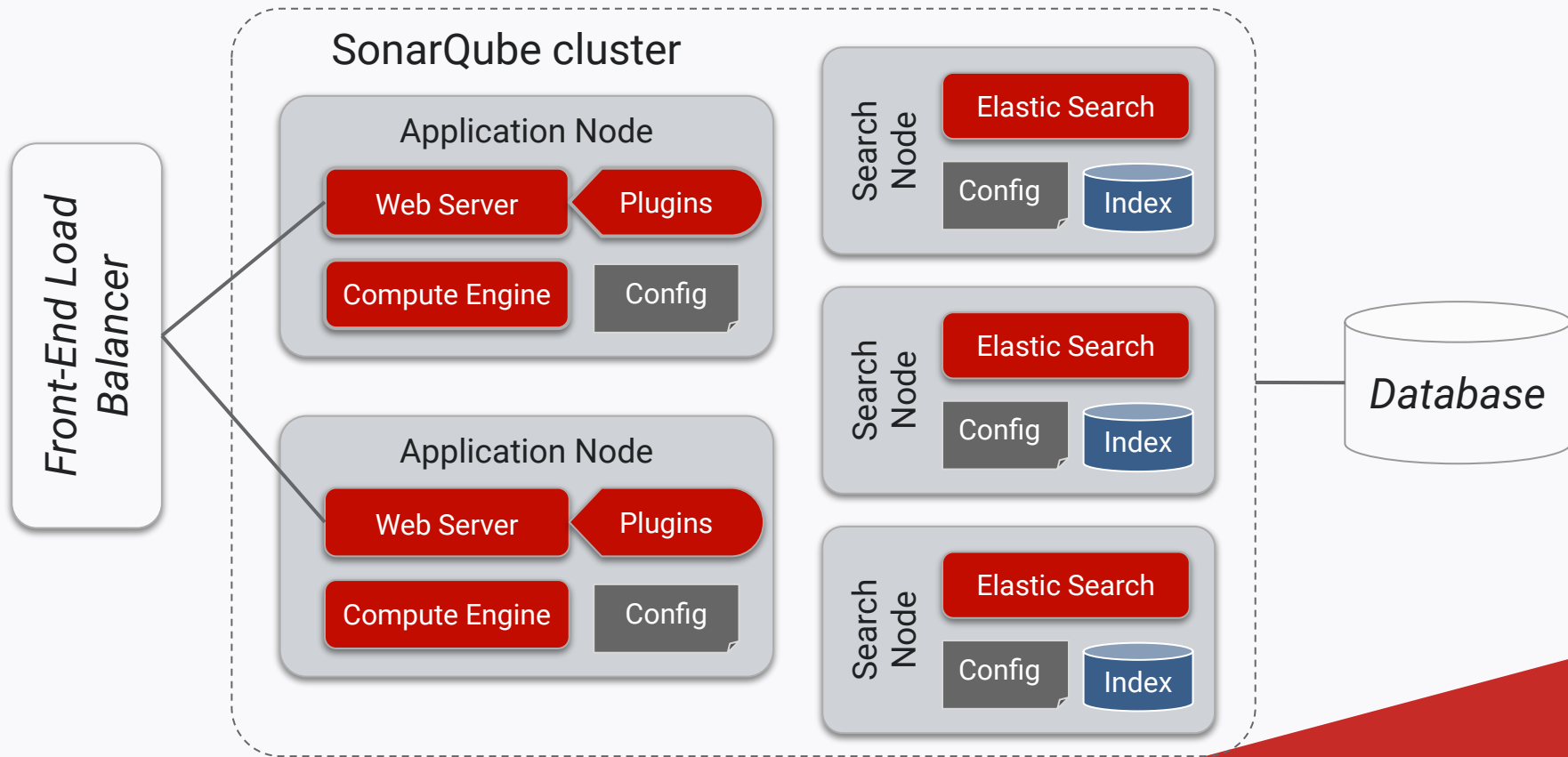
Overview

Architecture - Enterprise Edition

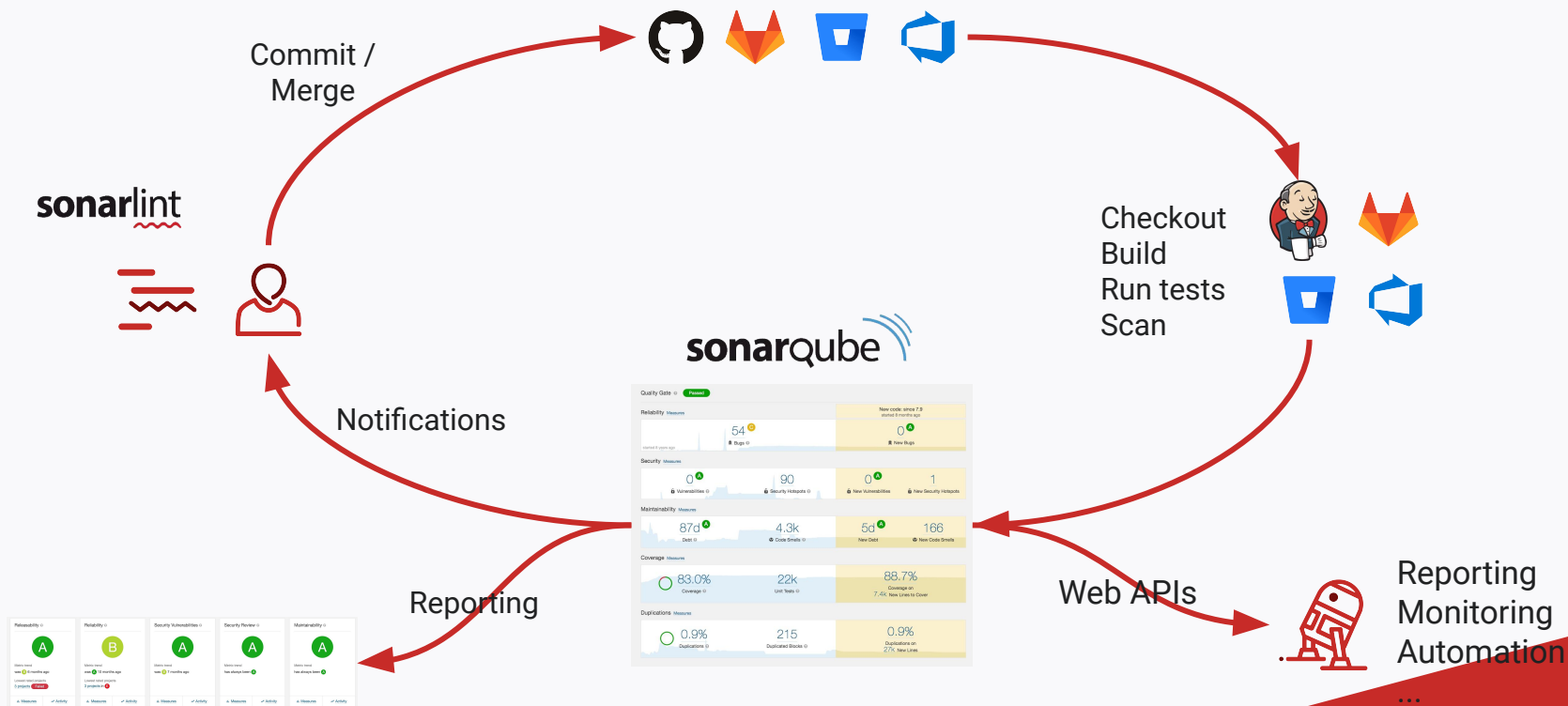




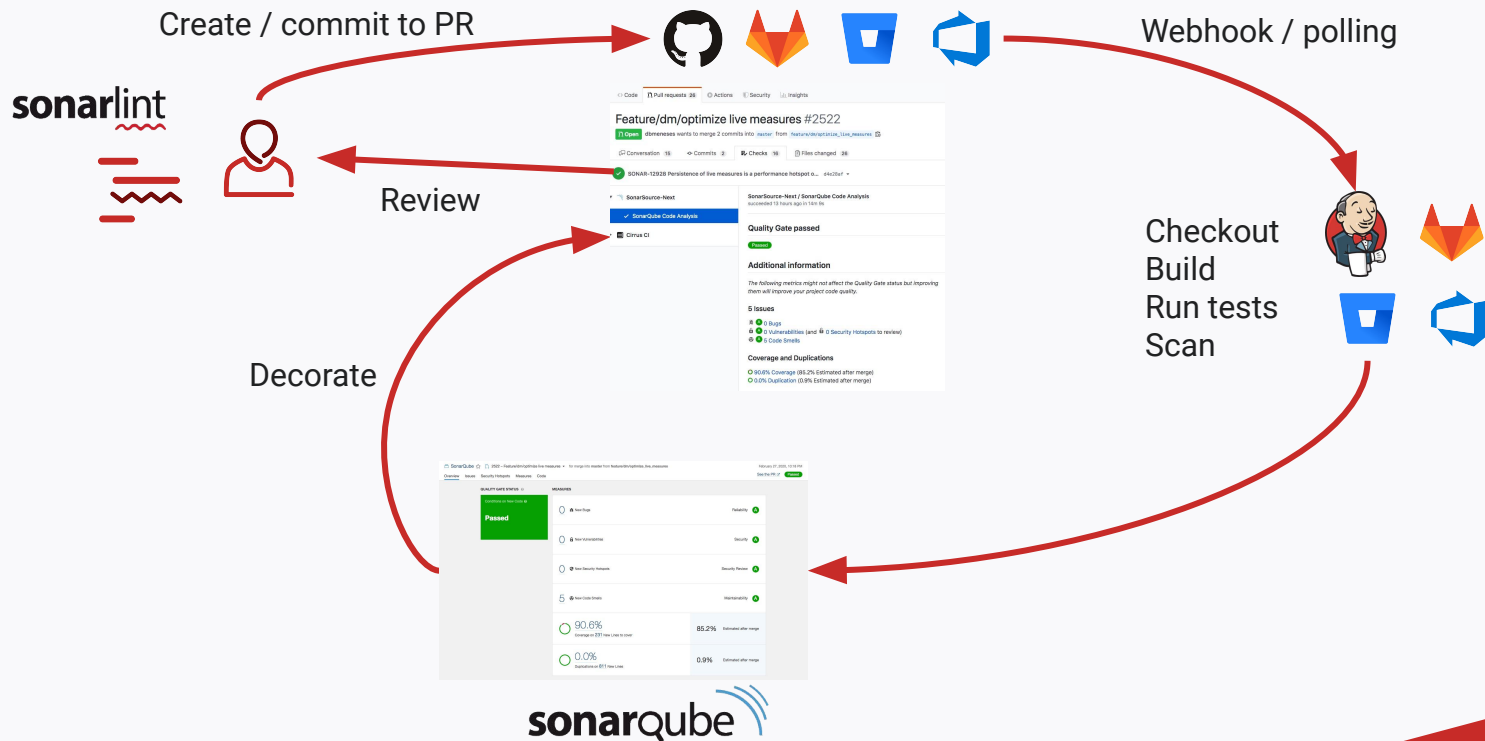
Architecture



Integration - main branch analysis



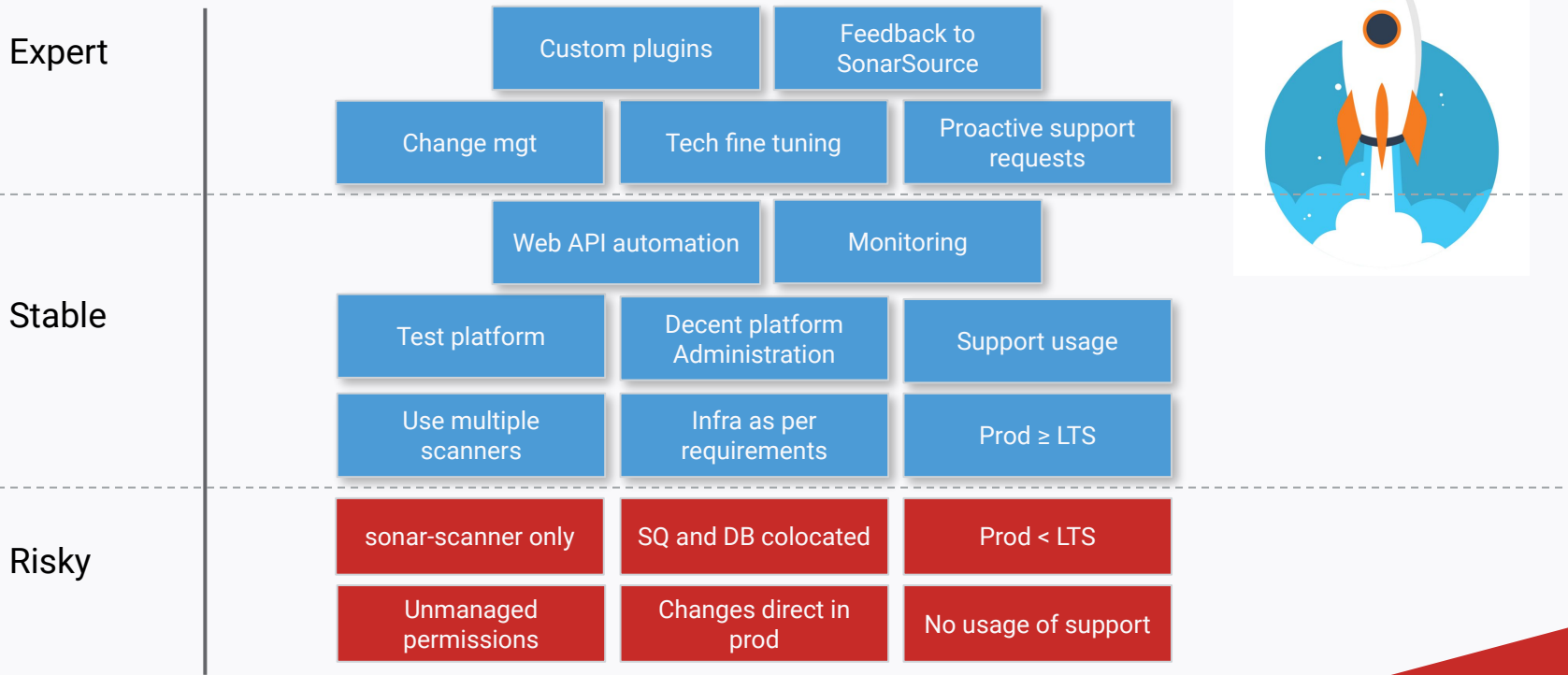
Integration - PR analysis





Operational maturity

Keep SonarQube flying at scale



Performance tuning & scaling


Options for Enterprise and DataCenter Editions

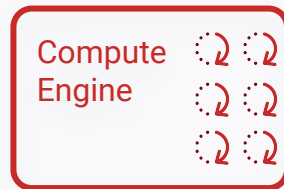
A solid red triangle is located in the bottom right corner of the slide, pointing upwards and to the left.



Scaling Enterprise Edition

Vertical Scalability

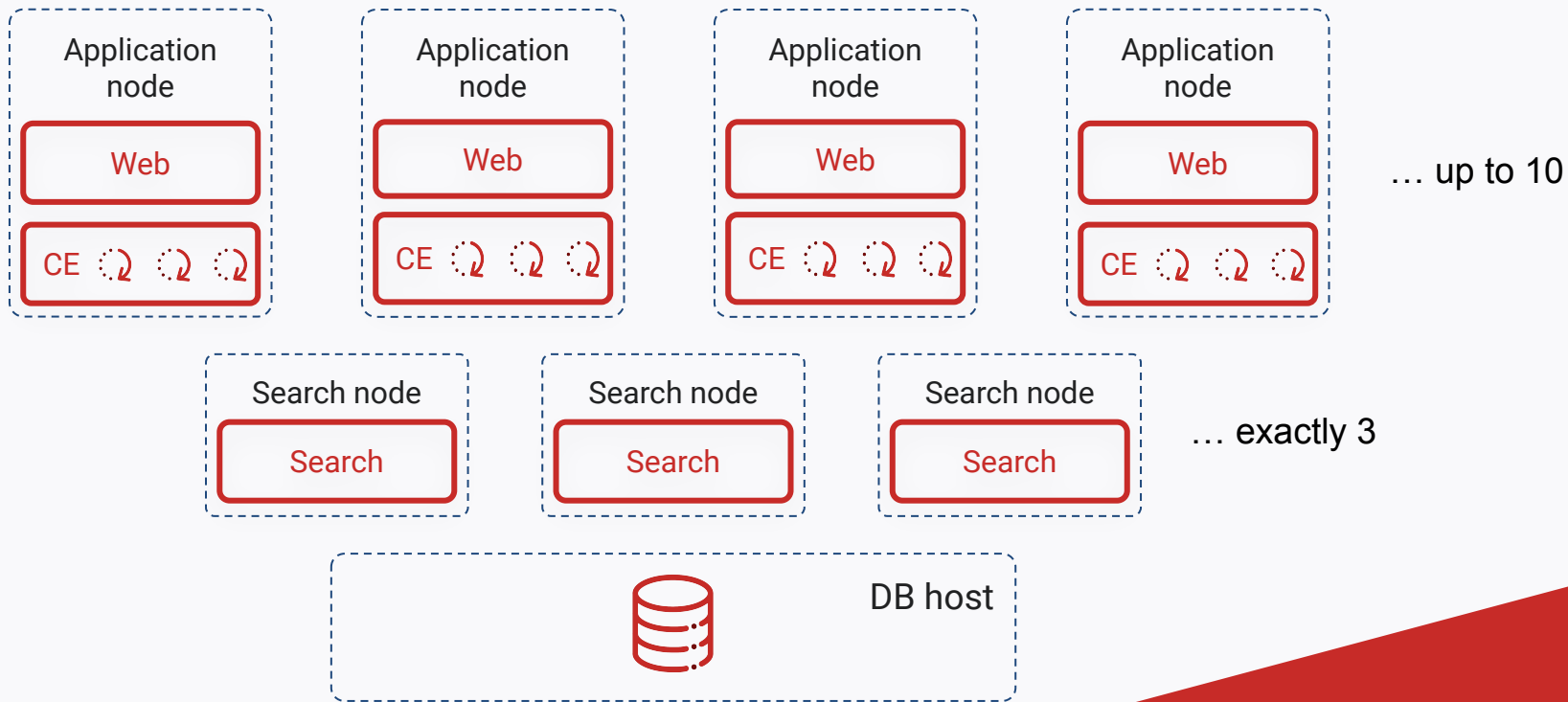
- Compute Engine multiple workers for parallel analysis
- Up to 10 workers supported
-  Requires sufficient resources
 - CPU
 - Heap memory
 - Database processing capacity
- Important: [Memory tuning guidelines](#)






Scaling Data Center Edition

Horizontal scalability



Setting up portfolios & apps

Use cases & best practices

A solid red shape in the bottom right corner of the slide, consisting of a triangle with its hypotenuse facing towards the top-left.

Securing the platform

Best practices

A solid red triangle is located in the bottom right corner of the slide, pointing towards the top right.

Securing the platform

Best practices 1/2

- Force authentication
- Set project default visibility to **Private**
- Use reverse proxy for HTTPS connectivity
- Use tokens for all non interactive sessions

Security

Force user authentication

Forcing user authentication prevents anonymous users from accessing the SonarQube UI, or project data via the Web API. Some specific read-only Web APIs, including those required to prompt authentication, are still available anonymously.

[Reset](#)

Default: False

Key: sonar.forceAuthentication

Default visibility of new projects: **Private** [Create Project](#)

Generate Tokens

[Generate](#)

New token "Token for scripts" has been created. Make sure you copy it now, you won't be able to see it again!

[Copy](#)

b5018eab7 693aa4a

Securing the platform

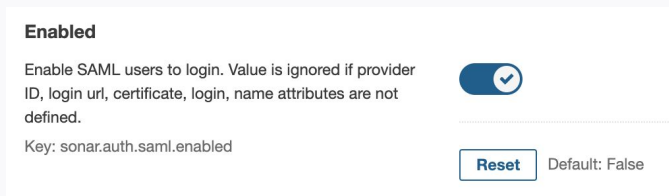
Best practices 2/2

- Encrypt sensitive settings:

`sonar.jdbc.url={aes}a1pLYQrr+QU+b953iQr1X4wPchVx1nsoqqCyfR8bXW/iD08pZMfr/gDCMEGrgFMr`

- Configure external authentication






LDAP, SAML, OAuth...



- Define a meaningful project permissions scheme
- Disable permission management for project administrators
- Integrate Audit Logs (9.1+)

Global Permissions

Typical permissions (other variations OK)

	Administer System ?	Administer ?	Execute Analysis ?	Create ?	
 CI Tools Service accounts for CI platforms	<input type="checkbox"/>	<input type="checkbox"/> Quality Gates <input type="checkbox"/> Quality Profiles	<input checked="" type="checkbox"/>	<input type="checkbox"/> Projects <input type="checkbox"/> Applications <input type="checkbox"/> Portfolios	
 Language Experts Group of language experts that can decide on rules to include in quality profiles	<input type="checkbox"/>	<input type="checkbox"/> Quality Gates <input checked="" type="checkbox"/> Quality Profiles	<input type="checkbox"/>	<input type="checkbox"/> Projects <input type="checkbox"/> Applications <input type="checkbox"/> Portfolios	QP admin for admins and language expert committee
 SonarQube Admins System administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Quality Gates <input checked="" type="checkbox"/> Quality Profiles	<input type="checkbox"/>	<input checked="" type="checkbox"/> Projects <input checked="" type="checkbox"/> Applications <input checked="" type="checkbox"/> Portfolios	Create Projects for admin only (and optionally CI) Create Apps & Portfolios for everyone
 sonar-users Any new users created will automatically join this group	<input type="checkbox"/>	<input type="checkbox"/> Quality Gates <input type="checkbox"/> Quality Profiles	<input type="checkbox"/>	<input type="checkbox"/> Projects <input checked="" type="checkbox"/> Applications <input checked="" type="checkbox"/> Portfolios	
 Anyone	<input type="checkbox"/>	<input type="checkbox"/> Quality Gates <input type="checkbox"/> Quality Profiles	<input type="checkbox"/>	<input type="checkbox"/> Projects <input type="checkbox"/> Applications <input type="checkbox"/> Portfolios	No permissions for Anyone

Execute Analysis for CI only

Projects creation for CI can also optionally be granted

Global admin for admins only

QG admin for restricted list of users (Admins)

Project Permissions

Typical permissions (other variations OK)

SonarQube core ☆ master

Last analysis had 1 warning August 18, 2020, 5:10 PM Version 1.0

Overview Issues Security Hotspots Security Reports Measures Code Activity Project Settings Project Information

Permissions

Grant and revoke project-level permissions. Permissions can be granted to groups or individual users. This project is private. Only authorized users can browse and see the source code.

☐ Public ☒ Private [Apply Permission Template](#)

	Browse	See Source Code	Administer Issues	Administer Security Hotspots	Administer	Execute Analysis
SonarQube Project Managers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SonarQube Tech Leads	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Team SonarQube Development Team for SonarQube	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
sonar-users Any new users created will automatically join this group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Auditors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Project Managers group with Project Admin permission

Tech Leads group with Issue and Hotspot Admin

Overall Dev Team group with Browse and See Source Code (optionally Issue Admin & Hotspot Admin)

All users can only *Browse*

Optional Auditor groups with Issue and Hotspot Admin (Not strongly recommended)



Other administration topics

- New Code period
- Analysis Scope
- Background tasks
- Branch and Pull Request scanning

SonarQube 9.x Roadmap

Even more Enterprise-grade features
Improvements across code quality and security domains





9.x main colors

Security ++



Enterprise grade ++



Operability ++





Security in 8.9 LTS

Languages coverage and evolution

Web and Common Apps

- Injections (taint) vulnerabilities
- Non injection vulnerabilities
- Security Hotspots



System & Embedded

- Buffer overflow Vulnerabilities
- Other non-injection Vulnerabilities
- Security Hotspots





Security in 9.x

Boosting mobile and cloud-native security

Mobile Apps

- Android
- iOS



Cloud native Apps

- Security of **cloud functions**
- Security of **Infrastructure as Code**





Other language features

- C# 9 and 10
- Java 16 and 17 ✓
- C++ 20
- New rules to support safety-critical C++
- Free-format RPG ✓
- Contextual/Educational Security content



Working at Enterprise scale

- Project-level PDF reporting ✓
- Security audit trails ✓
- Regulatory reports
- OWASP Top 10 2021 and OWASP ASVS
- Speed of analysis is a feature
- User and token housekeeping



Improved integration

- GitHub Actions ✓
- BitBucket Pipes ✓
- SonarQube as a GitHub Security scan



Improved operability

- Robust Kubernetes support for all editions
- Specific K8S cloud provider support
- DCE Helm chart (beta in 9.2, GA in 9.3)





SonarLint

- Secret detection: stop secrets leaking into your repos ✓
- Quick Fix support for on-the-fly fixes ✓
- Simpler project/module binding ✓
- JetBrains Rider support for C# ✓
- CLion support for C, C++ ✓
- Better/faster project synchronization
- Branch awareness

...and more to come!

<https://portal.productboard.com/sonarsource/3-sonarqube/tabs/11-planned-for-9-x-lts>

<https://portal.productboard.com/sonarsource/4-sonarlint/tabs/9-coming-soon>



Working with support

Best practices

A solid red triangle is located in the bottom right corner of the slide, pointing upwards and to the left.



Choosing a Version

Highest stability vs latest & greatest features

- LTS version
 - 8.9.x → 18/24 months (until ~ Spring 2023)
 - 7.9.x LTS transition period from May to October 2021
 - Occasional patch releases
- LATEST version (9.x)
 - New release expected ~every 2 months
 - Expectation that you upgrade on a timely basis at each release



Support

- What: <https://www.sonarsource.com/support>
- How: <https://support.sonarsource.com>
- Report more than only issues
 - False Positives / False Negatives
 - Advice on best practices
 - Rule suggestions



Support best practices

For the best experience (for everyone!)

- 1 issue = 1 ticket
- [Support Info file](#) + full logs (server or scanner)
- Portable file formats please
- Please don't cross-post to the Community forum
- Add your name to the ticket :)

Product news and updates

Staying in touch

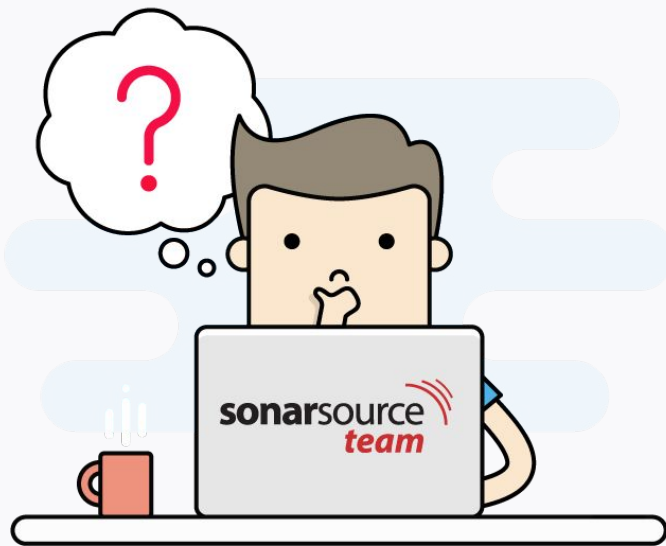
A solid red shape in the bottom right corner of the slide, consisting of a triangle with its hypotenuse facing the top-left.



Staying in touch

Get updates on what SonarSource is cooking

Public Jira instance	https://jira.sonarsource.com
Product roadmaps	SonarCloud Product Roadmap SonarLint Product Roadmap Planned for 9.x LTS - SonarQube Product Roadmap
Rules	https://rules.sonarsource.com
Community	https://community.sonarsource.com
Twitter	@SonarSource @SonarQube @SonarLint
Blog	https://blog.sonarsource.com



Feedback is a gift ! Thank you



<http://tiny.cc/h21xlz>

