Security **C**ontent **A**utomation **P**rotocol

Peter Vrabec <pvrabec@redhat.com>

redhat

Agenda

- Challenges
- SCAP
- Use cases
- Open-scap library
- OVAL
- Future

redhat.

Challenges

- Number and variety of systems
- Quick response
- Lack of interoperability

What is SCAP?

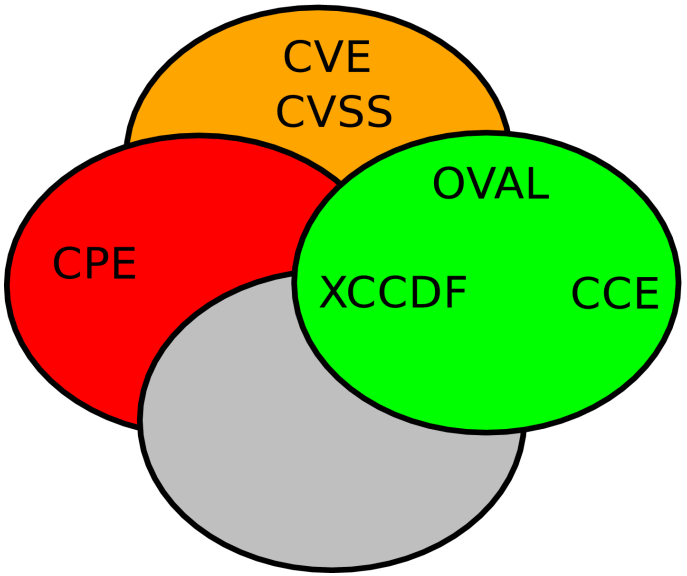
How

Standardizing the format by which we communicate

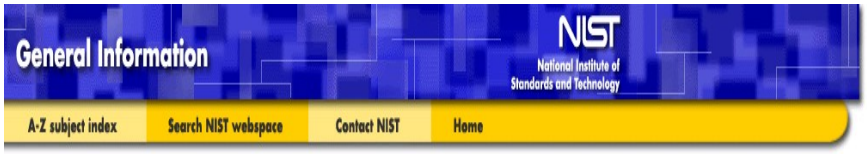
What

Standardizing the information we communicate

Protocol



Content

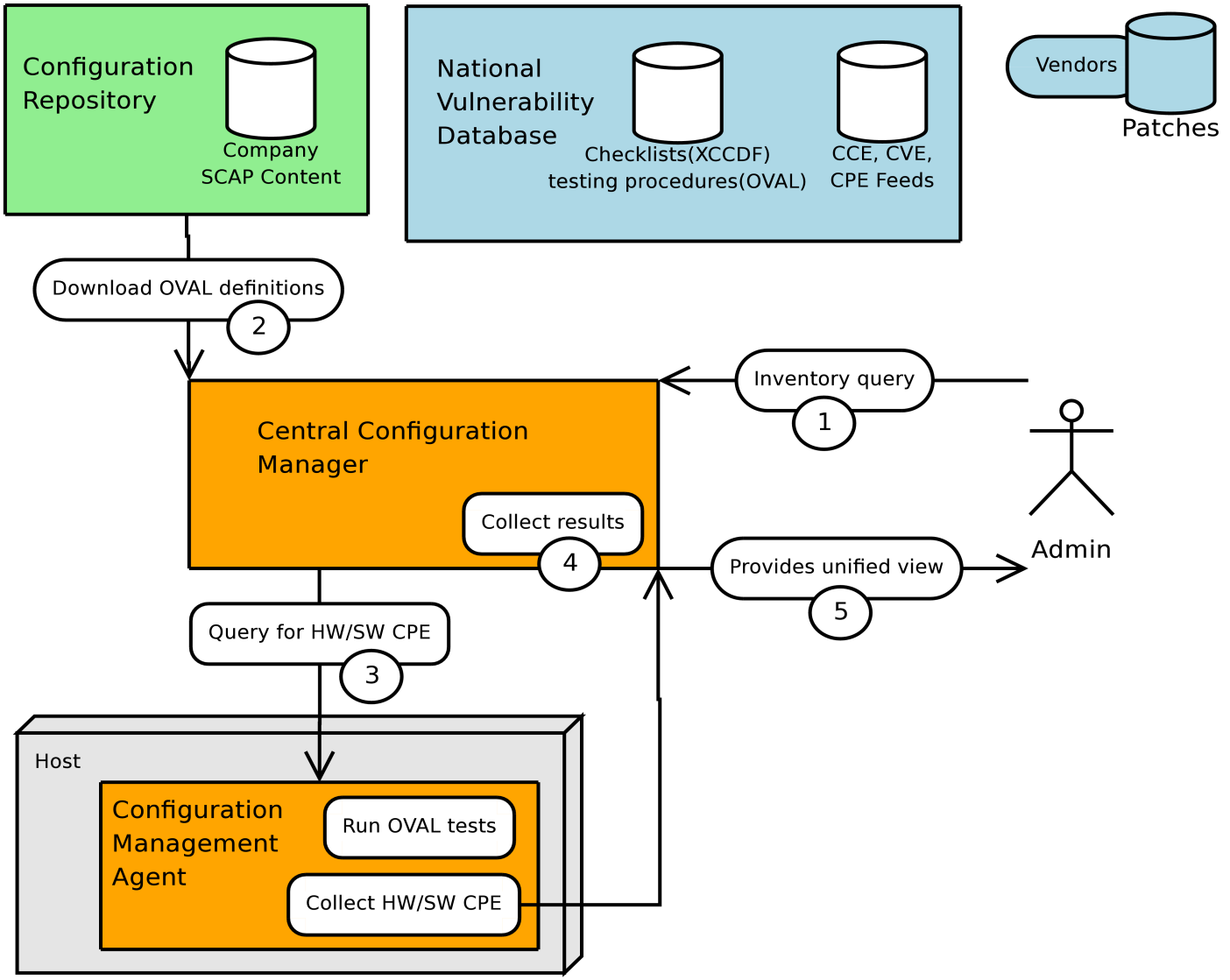


redhat

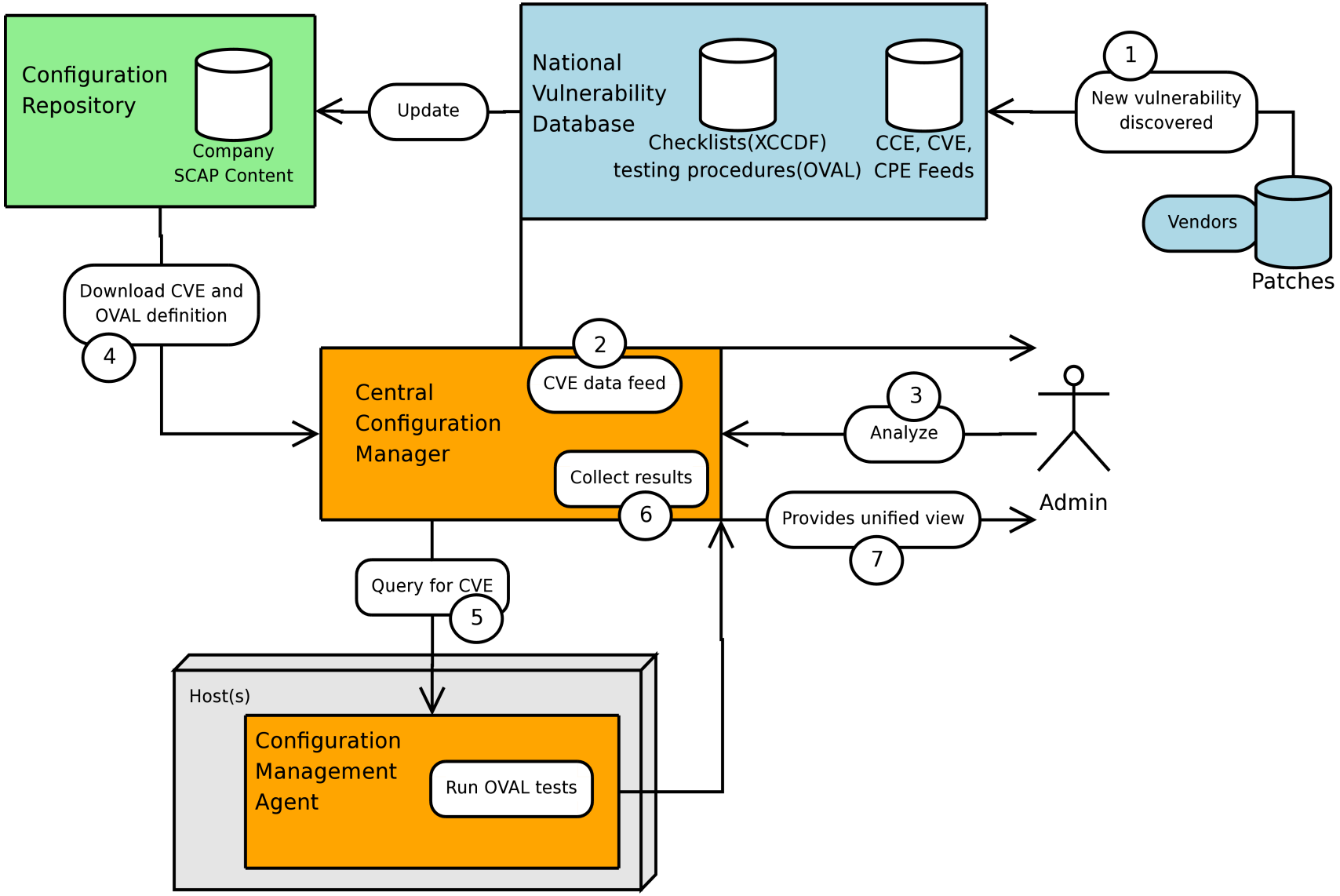
Protocol

SCAP Component	Description	Organization
Enumerations		
Common Configuration Enumeration (CCE)	Terminology and dictionary of system security issues	MITRE Corporation
Common Platform Enumeration (CPE)	Terminology and dictionary of product names and versions	MITRE Corporation
Common Vulnerabilities and Exposures (CVE)	Terminology and dictionary of security related software flaws	MITRE Corporation
Vulnerability Measurement and Scoring		
Common Vulnerability Scoring System (CVSS)	Specification for measuring the relative severity of software flaw vulnerabilities	Forum of Incident Response and Security Teams (FIRST)
Expression and Checking Languages		
Extensible Configuration Checklist Description Format (XCCDF)	Language for specifying checklists and reporting checklist results	National Security Agency (NSA) and NIST
Open Vulnerability and Assessment Language (OVAL)	Language for specifying low-level testing procedures used by checklists	MITRE Corporation

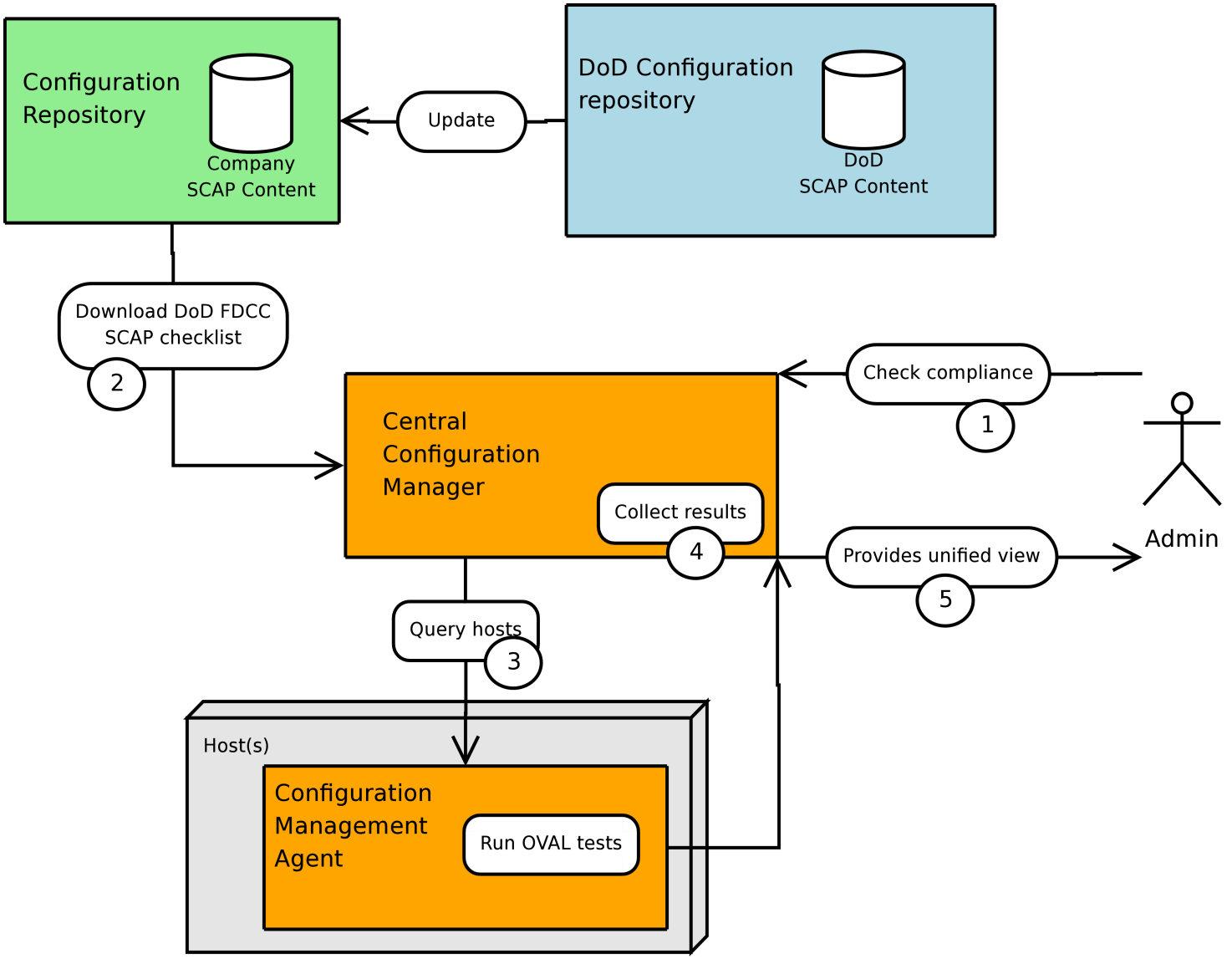
Use case – Asset mngt.



Use case – New vulnerability



Use case – Compliance check



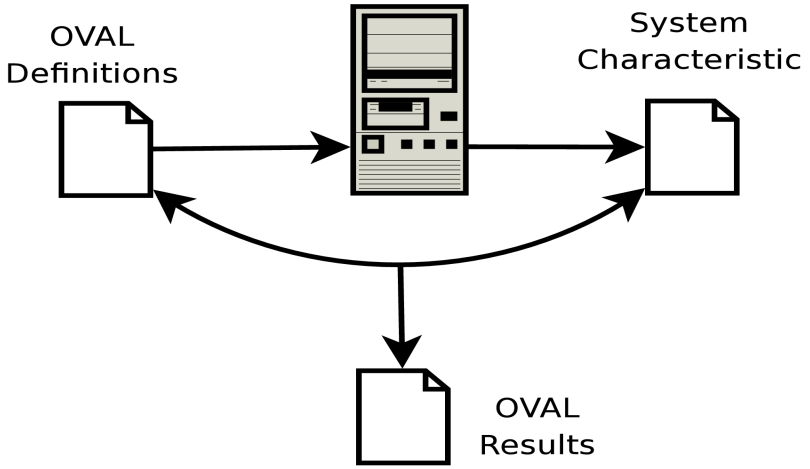
redhat

Open-scap library

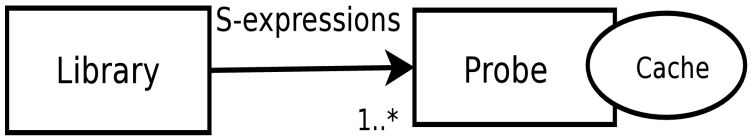
- Open-source framework
- Security technologies + G2
- Web: http://www.open-scap.org
- Email: open-scap-list@redhat.com
- What we have: Enumerations + Scoring + Checklist
- What we do: Checking language

OVAL design

- How it works?



- Probes:



redhat

Future

- Milestones:
  - System characteristic (1 week)
  - References + set objects (2 weeks)
  - Refactoring
  - Oval results
- Local scanning tool
- Content Editor
- Remediation language + Lockdown tool
- http://scap.nist.gov/emerging-specs/listing.html

redhat

Links

- http://makingsecuritymeasurable.mitre.org
- http://oval.mitre.org
- http://nvd.nist.gov
- http://scap.nist.gov


Questions?