

Greenhouse Kick-Off

PlusOne Operations Platform



Menagerie of Tools

Monitoring	Logging	Compliance	Scaling	Tools
Supernova	SEM	CAM Integration	metrics-server	Ingress Controller
Pagerduty	SIEM	Vault	HPA	Cert Manager
Alertmanager	Octobus	Heureka	VPA	u8s
Grafana	Kibana	Doop	Descheduler	Manila Provisioner
Prometheus	ElasticSearch	Gatekeeper		Helm
Exporters		Secure by Default		
		RBAC Provisioning		
		Falco		

Pain Points

Usage

- Step learning curve
- Tool Zoo
- Outdated tools

Automation

- Too much manual work (CAM, Pagerduty, Slack, Github, Vault ,....)
- Too hard to change
- Too hard to onboard additional teams
- Status Quo: Inconsistent, grown configuration. Easy to break.

Operations

- Deployment complexity increasing
- Platform vs Reuse
- Fuzzy responsibilities

Development

- Too many islands
- Not enough framework to extend easily

Inbox

OPERATIONS



Alerts



Compliance



Vulnerabilities



Security Events

OBSERVABILITY



Monitoring



Logging

ADDONS



Ingress



Certificates



Github



Vault

TOOLS



Web Console

ADMIN














Catalog


















Teams













Settings

ap-ae-1	0	24 	85 
ap-jp-2	0	9	141 
eu-de-2	0 	89 	196 
na-ca-1	0 	37 	174 
qa-de-1	32	70 	318 

ap-au-1	0 	25 	92 
ap-sa-1	0 	18 	81 
eu-nl-1	0 	55 	154 
na-us-1	0 	35 	113 

ap-cn-1	0 	23 	102 
ap-sa-2	0	13	131 
eu-ru-1	0	0	0
na-us-2	0 	16 	86 

ap-jp-1	0 	13	84 
eu-de-1	0 	121 	164 
la-br-1	0 	35	95 
na-us-3	0 	15 	134 

Inbox

- Aggregated across Alerts, Violations, Vulnerabilities, Security Events
- Aggregated across cluster fleet
- Prefiltered according to users' responsibilities
- Additional filter by cluster, responsibility and custom metadata



Inbox

OPERATIONS



Alerts



Compliance



Vulnerabilities



Security Events

OBSERVABILITY



Monitoring



Logging

ADDONS



Ingress



Certificates



Github



Vault

TOOLS



Web Console

ADMIN



Catalog



Teams



Settings

3058 alerts(56 critical, 687 warning, 2306 info) updated: 10:39:51

Region	Service	Title	Firing Since	Status	
qa-de-1	neutron	Network probes failed The network <code>r5i3 (00da747e-4e89-4fda-b1a7-775bc1692253)</code> failed all dns probes for more than 10 minutes. (Router <code>d0b0db63-c313-41c4-a2d4-e769bcd8a9a7</code>) - Show details Prometheus Playbook CloudOps <code>cluster = qa-de-1</code> <code>cluster_type = metal</code> <code>context = availability</code> <code>region = qa-de-1</code> <code>service = neutron</code> <code>severity = critical</code> <code>status = active</code> <code>tier = os</code>	10.10.2022 10:39:41	active	Silence
qa-de-1	neutron	Network probes failed The network <code>DapnIP-external-monsoon3-workload02-vcf01 (02521fcb-56d4-495c-ad3a-a5aa24fccbf)</code> failed all dns probes for more than 10 minutes. (Router <code>53235aa1-c281-489e-9845-d100c78d49da</code>) - Show details Prometheus Playbook CloudOps <code>cluster = qa-de-1</code> <code>cluster_type = metal</code> <code>context = availability</code> <code>region = qa-de-1</code> <code>service = neutron</code> <code>severity = critical</code> <code>status = active</code> <code>tier = os</code>	10.10.2022 10:39:11	active	Silence
qa-de-1	neutron	Network probes failed The network <code>DapnIP-external-monsoon3-management-vcf02 (444f4c3f-0798-4721-ad40-6131e50cd70d)</code> failed all dns probes for more than 10 minutes. (Router <code>99a8d7bc-c188-4ed1-95c7-ebe29d7b5165</code>) - Show details Prometheus Playbook CloudOps <code>cluster = qa-de-1</code> <code>cluster_type = metal</code> <code>context = availability</code> <code>region = qa-de-1</code> <code>service = neutron</code> <code>severity = critical</code> <code>status = active</code> <code>tier = os</code>	10.10.2022 10:39:11	active	Silence
qa-de-1	neutron	Network probes failed The network <code>DapnIP-external-monsoon3-01 (b20dfdc5-e31c-4791-b8a1-d7eb97914466)</code> failed all dns probes for more than 10 minutes. (Router <code>8aa6df66-4653-467c-96e1-22261f4540e1</code>) - Show details Prometheus Playbook CloudOps <code>cluster = qa-de-1</code> <code>cluster_type = metal</code> <code>context = availability</code> <code>region = qa-de-1</code> <code>service = neutron</code> <code>severity = critical</code> <code>status = active</code> <code>tier = os</code>	10.10.2022 10:38:41	active	Silence
qa-de-1	asr	Neutron Router mesh BGP peering on `qa-de-1-rt12b` to `10.46.210.197` went down. L3VPN outage! Neutron Router mesh BGP peering on <code>qa-de-1-rt12b</code> to <code>10.46.210.197</code> went down. L3VPN outage! - Show details Prometheus Playbook Grafana <code>cluster = qa-de-1</code> <code>cluster_type = controlplane</code> <code>context = asr</code> <code>job = network/ssh</code> <code>region = qa-de-1</code> <code>service = asr</code> <code>severity = critical</code> <code>status = active</code> <code>tier = net</code>	07.10.2022 22:23:57	active	Silence

Personal Supernova

- Prefiltered according to users' responsibilities
- Additional filter by cluster, region and custom metadata

Inbox

OPERATIONS



Alerts



Compliance



Vulnerabilities



Security Events

OBSERVABILITY



Monitoring



Logging

ADDONS



Ingress



Certificates



Github



Vault

TOOLS



Web Console

ADMIN



Catalog



Teams



Settings

- Check: GkHelm2Releases
- Check: GkHighCPURequests
- Check: GkImagesFromCorrectRegistry
- Check: GkImagesFromNonKeppel
- Check: GkIngressAnnotations
- Check: GkOutdatedImageBases
- Check: GkOwnerInfoOnHelmReleases
- Check: GkPrometheusruleAlertLabels
- Check: GkRegionValueMismatch
- Check: GkRegionValueMissing
- Check: GkResourceLimits

This check finds containers that do not have CPU and memory limits configured.

Why is this a problem?

Such containers could use an unbounded amount of resources (for example, because of a memory leak). Those resources would then not be available to other (potentially more important) containers running on the same node. We have already had API outages because of this.

How to fix?

Configure requests and limits for "cpu" and "memory" as described in [this article](#). Choose values based on historical usage, by looking at the `container_cpu_usage_seconds_total` and `container_memory_working_set_bytes` metrics in prometheus-kubernetes. The Grafana dashboard [Container Resources](#) shows these metrics in the "CPU Usage" and "Memory Usage" panels. **Set the memory request equal to the memory limit to avoid unexpected scheduling behavior.** For CPU, request and limit can and should diverge: The request represents the baseline load, the limit encompasses all expected spikes.

Deployment **2faproxy** in namespace monsoon3: cpu and memory limits not set on some or all containers

[qa-de-1: 2faproxy](#)

CronJob **2faproxy-update-crls** in namespace monsoon3: cpu and memory limits not set on some or all containers

[qa-de-1: 2faproxy-update-crls](#)

Personalized DooP

- Prefiltered according to users' responsibilities
- Policy Bundles
 - Pick and Choose: SGS, GCS, PCI, Kubernetes Community Best Practices
 - Central Maintenance
- Extendable with own policies
- Surfaces Deprecations/Upgrade Blockers

Inbox

OPERATIONS



Alerts



Compliance



Vulnerabilities



Security Events

OBSERVABILITY



Monitoring



Logging

ADDONS



Ingress



Certificates



Github



Vault

TOOLS



Web Console

ADMIN



Catalog









Teams



Settings

Vulnerability Analysis

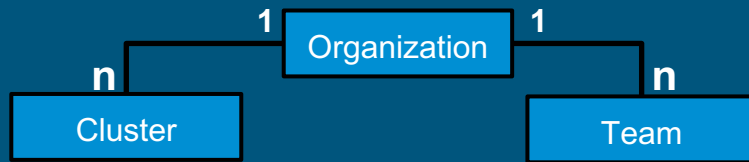
- Scans Images
- Guides through ramification workflow
- Creates compliance documentation

SCN/CVE	Threat level	Component	Last modified	State
SCN-2022-3114235 CVE-2022-3043	 High	absent-metrics-operator	27/09/2022, 14:50	New
SCN-2022-3114235 CVE-2022-3043	 High	cc-cablecheck-exporter	27/09/2022, 14:50	New
SCN-2022-3114235 CVE-2022-3043	 High	cc-cablecheck-exporter-vpod	27/09/2022, 14:50	New
SCN-2022-3114235 CVE-2022-3043	 High	cert-manager-controller	27/09/2022, 14:50	New
SCN-2022-3114235 CVE-2022-3043	 High	cinder-csi-plugin	27/09/2022, 14:50	New
SCN-2022-3114235 CVE-2022-3043	 High	cinder-csi-plugin	27/09/2022, 14:50	New
SCN-2022-3114235 CVE-2022-3043	 High	cinder-csi-plugin	27/09/2022, 14:50	New

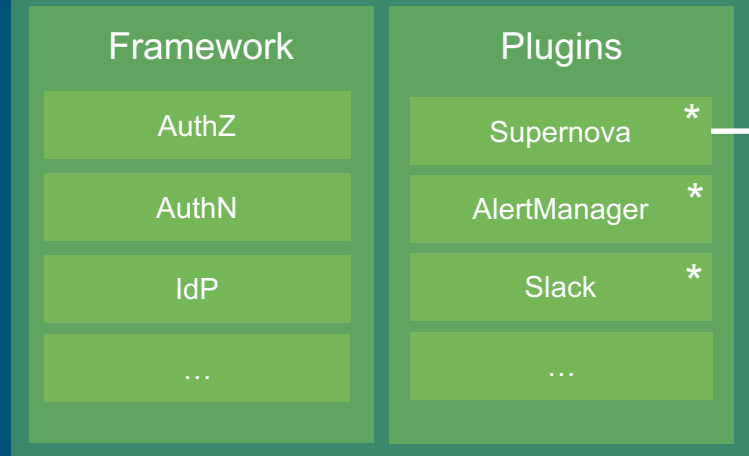
Greenhouse

High Level Architecture

Greenhouse API

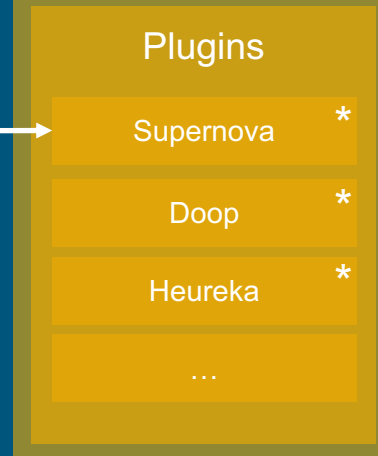


Controllers



Greenhouse Frontend

Dashboard



API

- Kubernetes CRDs and Controllers
- Central framework
- Configuration automation via plugins
- **Decentral Developed Plugins**
- Extendable Plugins

Frontend

- End-user Portal
- Plugins ReactJS MicroApps
- CCloud Design System

Roadmap - Stage 1

Enablement TOM model for CCloud DevOps

- Alerts (Supernova)
- Governance/Compliance (Dooop/Gatekeeper)
- Vulnerabilities (Heureka)
- SIEM/SEM

Framework

- UI Framework (Application L)
- Authorization model (CAM/IAS)
- CAM integration
- Data model (Org, team, membership)
- Plugins
 - Specification
 - Authentication

Next steps

Weekly greenhouse sync meeting

- Initial Audience?

Initial work packages

- Greenhouse data model (Arno & Fabus)
- CAM Concept for Profiles, Support Groups, Teams (DavidR)
- Spike CAM Integration (Arno & Fabus)
- UI Concept (Esther)
 - Application L
 - Plugin concept
 - Supernova reimplementatation

SAP folgen auf



www.sap.com/germany/contactsap

© 2022 SAP SE oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere sind die SAP SE oder ihre Konzernunternehmen in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen. Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen der SAP SE oder ihrer Konzernunternehmen können von der SAP SE oder ihren Konzernunternehmen jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.

SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite www.sap.com/corporate/de/legal/copyright.html.

