DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Detailstandard 54: Vorgaben Monitoring für Kubernetes

Version 1.0 (24.06.2025)

Inhaltsverzeichnis

> **INFO**
>
> Zusätzlich gibt es allgemeine Vorüberlegungen und insbesondere Betrachtungen zur Ableitung und Austausch von "Sicherheitsrelevanten Vorfällen"; letzterer Punkt wird gesondert in einem Detailstandard 19 "Systematik des Austauschs von sicherheitsrelevanten Vorfällen" behandelt.

Zusammenfassung

Plattformbetreiber in der DVC stellen potentiell Produkte auf Basis Kubernetes bereit. Dies sind im Sinne der DVC "PaaS"-Lösungen, am Markt werden entsprechende Lösungen als "KaaS" (Kubernetes as a Service) bzw. "CaaS" (Container as a service) kategorisiert. Dabei geht dieser Detailstandard vom Umstand aus, dass ein Plattformbetreiber ENTWEDER einen kompletten Kubernetes Cluster für einen Kunden bereitstellt im Modell "(Kubernetes) Cluster as a Service") ODER einen Namespace für den Kunden bereitstellt ("Namespace as a Sevice"; dies in einem Cluster, den sich dieser Kunde potentiell mit anderen Kunden teilt).

Das eigentliche **Anwendungsmonitoring** obliegt nicht dem Plattformbetreiber, sondern dem Cloud-Service-Kunden (z.B. Softwarebetreiber).

Anforderung

Monitoringkategorie	Für Eigenbedarf Plattformbetreiber für den gesamten Cluster	Für relevante Vorfälle des Kunden in seinen Namespaces
Cluster Node CPU Usage für vom Kunden genutzte Nodes	✅	⚠ Nur bei Buchung eines dedizierten Clusters
Cluster Node RAM Usage für vom Kunden genutzte Nodes	✅	⚠Nur bei Buchung eines dedizierten Clusters
Namespace CPU Usage für vom Kunden genutzte Namespace	✅	✅
Namespace RAM Usage für vom Kunden genutzte Namespaces	✅	✅
Pod CPU Usage für vom Kunden genutzte Pods	✅	✅
Pod RAM Usage für vom Kunden genutzte Pods	✅	✅
Anzahl Kunden Namespaces	✅	✅
Anzahl der laufenden Pods des Kunden	✅	✅
Anzahl Kunden Deployments	✅	✅
Kunden Namespace: CPU request/limits	✅	✅
Kunden Namespace: RAM request/limits	✅	✅
Kunden Pods: CPU request/limits	✅	✅

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

Monitoringkategorie	Für Eigenbedarf Plattformbetreiber für den gesamten Cluster	Für relevante Vorfälle des Kunden in seinen Namespaces
Kunden Pods: RAM request/limits	✅	✅
Pod: Badget: Health	✅	✅

Standardisierung

Aus dem Detailstandard ergeben sich folgende Detailanforderungen:

ID	Rolle	Modal-verb	Detailanforderung
DS_54_A001	Plattform-betreiber	MUSS	die **inhaltlichen Metriken** aus der Sektion / Tabelle **Anforderung** erheben.
DS_54_A002	Plattform-betreiber	MUSS	dem Softwarebetreiber einen **Endpunkt/eine Möglichkeit für den Abruf des Datenset** zur Verfügung stellen
DS_54_A003	Plattform-betreiber	KANN	dem Softwarebetreiber Zugriff auf das **Monitoring-System bzw. eine dedizierte Monitoring-Instanz** zur Verfügung stellen
DS_54_A004	Plattform-betreiber	MUSS	Die Speicherung der **Protokollierungsdaten** der Container MUSS außerhalb des Containers, **mindestens auf dem Container-Host**, erfolgen. (BSI SYS.1.6.A7)
DS_54_A005	Plattform-betreiber	MUSS	Um auf Pod-Ebene nach Bezug durch die Cloud-Service-Kunden eine **Health-Badget im Monitoring** durchzureichen, muss der Plattformbetreiber per Policy sicherstellen, dass sein **Kunde diese Information entsprechend konfiguriert im Rahmen des Deployments**.
DS_54_A006	Plattform-betreiber	MUSS	weitere **Qualitätmerkmale** vom Kunden einfordern durch entsprechend **gesetzte und dokumentierte Policies**

Referenzdokumente

Kapitel	Seite	Dokument	Link	PDF
SYS.1.6.A7	(n/a)	BSI Grundschutz	nur PDF	BSI Grundschutz
		DVC Detailstandards - (19) Systematik des Austauschs von sicherheitsrelevanten Vorfällen	in Erstellung für Folgeversion der DVC-Dokumentation	in Erstellung für Folgeversion der DVC-Dokumentation