DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Detailstandard 53: Vorgaben Logging für Kubernetes

Version 1.0 (24.06.2025)

Inhaltsverzeichnis

> **INFO**
>
> Dieser Detailstandard regelt das "Logging für Kubernetes" (PaaS-Umgebungen ("Containerorchestrierung auf Basis Kubernetes")). Er ergänzt damit den Detailstandard 44 "Logging von Containern", der von den Softwarebetreibern aus der Sicht der bereitgestellten "Containerisierten Anwendungen" beschrieben wird.
>
> 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).

In diesem Dokument werden im Kapitel „**Anforderungen**" vorgegebene **Mindestmetriken für Monitoring** qualifiziert. Im Kapitel "**Standardisierung**" werden die zu erfüllenden **fachlichen Anforderungen** in diesem Standardisierungsbereich beschrieben. Diese stellen eine Konkretisierung der beschriebenen Anforderungen dar. Es steht den Plattformbetreibern frei, über den Standard hinausgehende Informationen und Schnittstellen bereitzustellen.

Anforderung

Der Plattformbetreiber arbeitet grundsätzlich für das Logging auf Basis der eigenen Betriebsprozesse. Für die DVC wollen wir an dieser Stelle darauf hinweisen, dass a) die Erwartungshaltung besteht, dass jeder Plattformbetreiber bestimmte Informationen im Rahmen der eigenen Auditierungsverpflichtungen zur Eigenauswertung nachhält und b) TEILE der Informationen für die in Kundenhoheit befindlichen Namespaces an die Kunden auskoppelt. Dabei muss sichergestellt sein, dass jeder Kunde nur die für ihn relevanten Informationen erhält.

Loggingkategorie	**Für Eigenbedarf Plattformbetreiber für den gesamten Cluster**	**Für relevante Vorfälle des Kunden in seinen Namespaces**
Der Plattformbetreiber MUSS **Änderungen der Compute Ressourcen** im Cluster für eigene Auditierung loggen	✅	❌
Der Plattformbetreiber MUSS **Zustandsänderungen aller Cluster-Komponenten** für eigene Auditierung loggen	✅	❌

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

Loggingkategorie	**Für Eigenbedarf Plattformbetreiber für den gesamten Cluster**	**Für relevante Vorfälle des Kunden in seinen Namespaces**
Der Plattformbetreiber MUSS **Deployments** in den Cluster global für die eigene Auditierung loggen	✅	✅
Der Plattformbetreiber MUSS **Warnungen & Fehlermeldungen des Clusters** und aller dort betriebenen Namespaces für die eigene Auditierung loggen	✅	✅
Der Plattformbetreiber MUSS **Benutzeranmeldungen** am Cluster (eigene sowie von Kunden für die durch die Kunden betriebenen Namespaces) für die eigene Auditierung loggen	✅	✅

Standardisierung

Aus dem Detailstandard ergeben sich folgende Detailanforderungen:

ID	**Rolle**	**Modal-verb**	**Detailanforderung**
DS_53_A001	Plattform-betreiber	MUSS	die **inhaltlichen Metriken** aus der Sektion / Tabelle **Anforderung** erheben.
DS_53_A002	Plattform-betreiber	MUSS	dem Cloud Service Kunden (z.B. Softwarebetreiber) einen **Endpunkt/eine Möglichkeit für den Abruf des Datenset** zur Verfügung stellen
DS_53_A003	Plattform-betreiber	KANN	dem Softwarebetreiber optionalen Zugriff auf das **Logging-System bzw. eine dedizierte Logging-Instanz** zur Verfügung stellen
DS_53_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)

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
		DVC Detailstandards - (44) Logging von Containern	Detailstandard 44: "Logging von Containern"	Detailstandard 44 PDF