

Technologiedefinitionen

Enterprise Core Services

der

BARMER und der HEK

Inhaltsverzeichnis

1	Rechtskonforme Bereitstellung der Infrastruktur	3
2	Spezifische Anforderungen an die Bereitstellung Infrastruktur Leistungen	3
2.1	Betriebssystem	3
2.2	Storage.....	3
3	Job Scheduling (aktuell Automic UC4)	4
4	Anforderungen an die Verfügbarkeit und Disaster Recovery Klasse	4
4.1	Hochverfügbarkeit.....	4
4.2	Zonenredundante und Hochverfügbare Architektur	4
4.3	Datensicherung	5
5	Containerplattform	6
6	Event-Streaming-Plattform.....	6

1 Rechtskonforme Bereitstellung der Infrastruktur

On-Prem Hosting-Ansatz: Die IT-Infrastruktur wird in einem externen Rechenzentrum innerhalb eines physisch isolierten Bereichs exklusiv für den jeweiligen *Auftraggeber* betrieben. Die Umgebung muss dedizierte oder virtualisierte Ressourcen bereitstellen, die ausschließlich dem jeweiligen *Auftraggeber* zur Verfügung stehen. Eine Nutzung der dedizierten Hardware durch andere Unternehmen ist nicht gestattet und muss technisch verhindert werden.

Für alle Services im Leistungsumfang stellt der *Auftragnehmer* sicher, dass die zur Leistungserbringung genutzten Infrastrukturkomponenten durch den *Auftraggeber* rechtskonform genutzt werden können. Das heißt, alle vertraglichen Vorgaben, Richtlinien und Anforderungen werden durch den *Auftragnehmer* berücksichtigt und eingehalten.

Der *Auftragnehmer* erbringt Infrastruktur Leistungen für den *Auftraggeber* unter Berücksichtigung aller Vorgaben, Richtlinien und Anforderungen des *Auftraggebers* und entsprechend der Leistungsausprägung, die in **01-02 Leistungsbeschreibung** sowie **01-02-01 Service Katalog** spezifiziert sind.

Der *Auftragnehmer* berücksichtigt bei der Leistungserbringung die folgenden spezifischen Anforderungen des *Auftraggebers* und stellt deren Einhaltung sicher.

2 Spezifische Anforderungen an die Bereitstellung Infrastruktur Leistungen

2.1 Betriebssystem

Der *Auftraggeber* setzt folgende Betriebssystem Distributionen ein:

Betriebssystem	Version	Hinweis
RedHat Enterprise Linux	8.x und 9.x	
SuSE Enterprise Linux	12.x 15.x	12.x: zukünftig keine weitere Bereitstellung dieser Version durch den <i>Auftragnehmer</i> . SLES 12.5 LTSS evtl. erforderlich SLES 15.5 LTSS erforderlich
Windows Server 2016	R2 Datacenter Edition, Standard Edition	Der <i>Auftragnehmer</i> muss diese Version nur initial bereitstellen, sofern nicht vor SCD eine Umstellung auf eine neue Version erfolgt ist.
Windows Server 2022	Datacenter Edition, Standard Edition	
Windows Server 2025	Datacenter Edition, Standard Edition	

2.2 Storage

Der *Auftraggeber* unterscheidet bei den einzusetzenden Storage Typen Block-, File- und Object Storage drei Storage Klassen, die durch den *Auftragnehmer* entsprechend den

Vorgaben an die Verteilung der Klassen je Storage Typ in **01-02-01 Service Katalog** zu berücksichtigen sind:

Tier Storage Klasse	Storage Kategorie	Technische Anforderungen
A+ Highest Performance	Solid State Drive (SSD), All-Flash-Array	SR: 11,5 GB/s SW: 10 GB/s IOPS 4KQD1: 125 MB/s
A - High Performance	Fibre Channel (FC), Storage Area Network (SAN), Network attached storage (NAS)	SR: 6,5 GB/s SW: 5,5 GB/s IOPS 4KQD1: 120 MB/s
B - Midrange	Storage Area Network (SAN), Network attached storage (NAS)	SR: 4,5 GB/s SW: 3,5 GB/s IOPS 4KQD1: 90 MB/s
C - Low-End	Content Addressable Storage (CAS)	Keine spezifischen Anforderungen

Tabelle 1: Storage-Klassen

3 Job Scheduling (aktuell Automic UC4)

Der *Auftraggeber* erhält die uneingeschränkte Möglichkeit, eigene Automicagenten und Technologien der Komponenten, Anwendungen und Services auf den durch den *Auftragnehmer* für den *Auftraggeber* bereitgestellten Systemen zu etablieren.

Der *Auftragnehmer* unterstützt den *Auftraggeber* bei der automatisierten Installation sowie Konfiguration der Automicagenten und Technologien der Komponenten.

4 Anforderungen an die Verfügbarkeit und Disaster Recovery Klasse

4.1 Hochverfügbarkeit

Systeme gelten als hochverfügbar, wenn sie eine Verfügbarkeit von mindestens 99,5% (Silber-Level) erreichen, was einer maximalen jährlichen Ausfallzeit von etwa 44 Stunden entspricht. Dies erfordert die Redundanz kritischer Komponenten, sodass ihre Funktionen bei einem Ausfall automatisch von anderen Systemteilen übernommen werden. Alle Maßnahmen zur Sicherstellung der Hochverfügbarkeit sind kontinuierlich zu überwachen und regelmäßig zu optimieren, um die notwendige Systemstabilität und Verfügbarkeit zu garantieren.

4.2 Zonenredundante und Hochverfügbare Architektur

Der *Auftragnehmer* legt seine Infrastruktur in Form von mindestens zwei getrennten Verfügbarkeitszonen aus, inklusive zonenübergreifendem Load Balancing (z. B. Active-Active oder Active-Passive Betrieb). Eine Failover-Strategie muss implementiert sein, um den Betrieb im Falle eines Zonenausfalls sicherzustellen. Die Infrastruktur erfüllt die Anforderungen an die automatische Skalierung je nach Last (horizontal und vertikal). Die Bereitstellung erfolgt automatisiert zum Beispiel über Scripts und mit Hilfe geeigneter Tools. Unterbrechung des Betriebs der Infrastruktur ist weitestgehend verhindert, z.B. durch Blue-Green-Deployments.

4.3 Datensicherung

Der *Auftragnehmer* ist berechtigt und aufgefordert, eigenständige und sinnvolle Anpassungen der Datensicherung -Prozesse vorzunehmen, solange die vereinbarten Wiederherstellungsklassen und Verfügbarkeitsziele uneingeschränkt gewährleistet bleiben.

Die Datensicherung erfüllt die folgenden Anforderungen:

- Sicherstellung der Datensicherheit durch verschlüsselte Speicherung aller Datensicherung.
- Durchführung regelmäßiger Test-Wiederherstellungen (Vorgaben je Wiederherstellungsklasse).

Vorgaben je Wiederherstellungsklasse:

Klasse DR 5

- Echtzeit-Snapshots
- Continuous Data Protection (CDP)
- Speicherung der Datensicherung redundant an unterschiedlichen Standorten
- Tägliche Integritätsprüfung und wöchentliche Test-Wiederherstellung

Klasse DR4

- Stündliche inkrementelle Datensicherung
- Tägliche vollständige Datensicherung
- Speicherung der Sicherungen auf dedizierten Backup-Systemen sowie an externen Standorten
- Monatliche Integritätsprüfung und Wiederherstellungstest

Klasse DR3

- 12 stündliches inkrementelle Datensicherung
- Wöchentliche vollständige Backups
- Speicherung der Sicherungen auf lokalen und externen Medien
- Quartalsweise Integritätsprüfung und Testwiederherstellung

Klasse DR1-DR2

- Tägliche inkrementelle Datensicherung
- Monatliche vollständige Datensicherung
- Speicherung der Sicherungen auf lokalen Medien
- Quartalsweise Integritätsprüfung und Testwiederherstellung

5 Containerplattform

- Die Plattform hat eine Kubernetes-kompatible API bereitzustellen, die vollständig der offiziellen Kubernetes-API-Spezifikation entspricht.
- Proprietäre Abweichungen, Forks oder inkompatible Erweiterungen sind unzulässig, soweit sie eine Migration auf andere Kubernetes-Implementierungen oder Standard-Kubernetes-Distributionen erschweren.
- Die Plattform muss eine standardisierte Kubernetes-API unterstützen, die uneingeschränkt mit den offiziellen Kubernetes-Versionen kompatibel ist.
- Der *Auftraggeber* erhält administrativen Zugang auf Cluster-Ebene, um Operatoren und zusätzliche Erweiterungen zu integrieren.

Die Plattform muss über geeignete Schnittstellen verfügen, die eine automatisierte Bereitstellung und Verwaltung von Clustern und zugehörigen Ressourcen ermöglichen.

Diese Schnittstellen müssen mindestens folgende Funktionen unterstützen:

- Automatisierte Bereitstellung von Clustern auf Basis deklarativer Konfigurationen
- Selbstheilung und automatische Skalierung (Self-Healing und Auto-Scaling) zur effizienten Ressourcennutzung
- Integration von Netzwerk- und Service-Mesh-Komponenten (z. B. Cilium) für eine einheitliche Kommunikation zwischen Clustern und Workloads.

Die Plattform muss mindestens folgende Speicheroptionen bereitstellen:

- ReadWriteOnce (RWO): Persistenter Blockspeicher für einzelne Pods (z. B. Datenbanken oder StatefulSets).
- ReadWriteMany (RWM): Geteilter Speicher für mehrere Pods (z. B. NFS-basierte Speicherlösungen oder Cluster-Dateisysteme).
- XFS: Speziell für Anwendungen mit umfangreichen Datenmengen oder einer großen Anzahl kleiner Dateien.
- Object Storage (S3-kompatibel): Skalierbarer Objektspeicher für Artefakte und unstrukturierte Daten.

Anforderungen an die Storage-Integration:

- Dynamische Storage-Provisionierung über z.B. Kubernetes Storage Classes.
- Multi-Tenant-Fähigkeit und Isolation zur getrennten Verwaltung verschiedener Workloads.

6 Event-Streaming-Plattform

Die Plattform muss mindestens folgende Anforderungen erfüllen:

- Unterstützung für verschiedene Eventgrößen und -formate (z. B. JSON).
- Unterstützung von Kafka APIs (Producer, Consumer, Streams).
- Bereitstellung von Kafka Connect für die Integration externer Systeme (z. B. Datenbanken, Message Queues).
- Bereitstellung & Konfiguration z.B. mit Zookeeper