Service Katalog

IX.Cloud
SWISS FINANCIAL CLOUD

Version: 2026-06-08 09:42

Inhaltsverzeichnis

        - Service Umfang
        - Service Optionen
- **Network Services**
    - Firewall
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Server Proxy
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Load Balancer
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Web Application Firewall
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Private DNS
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Secure Mail-Relay
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Hosted Software-Appliance
        - Service Architektur
        - Service Umfang
        - Service Optionen
- **Storage Services**
    - File Storage
        - Service Architektur
        - Service Umfang
        - Service Optionen
    - Object Storage
        - Service Architektur
        - Service Umfang
        - Service Optionen
- **Compute Services**

- Virtual Machine
  - Service Architektur
  - Service Umfang
  - IT-Grundschutz
  - Service Optionen
- **System Management Services**
  - Managed OS
    - Service Architektur
    - Service Umfang
    - Service Optionen
  - Metrics Monitoring
    - Service Architektur
    - Service Umfang
    - Service Optionen
  - Software Deployment
    - Service Architektur
    - Service Umfang
    - Service Optionen
  - Software und Release-Zyklen
    - Linux Software
    - Windows Software
    - Umgang mit 3rd Party Software
    - Betriebssystem- und Software Release-Zyklen
- **Database Services**
  - Managed xSQL-Instance
    - Service Architektur
    - Service Umfang
    - Service Optionen
  - PostgreSQL HA Managed Service
    - Service Architektur
    - Service Umfang
  - Managed noSQL-Instance
    - Service Architektur
    - Service Bereitstellung
    - Service Umfang
    - Service Optionen
  - Managed Service Database Security Audit
    - Service Architektur
    - Service Umfang
  - IT Grundschutz Database Service
    - Patch Management

        - Logging
        - Malware Schutz
- **Container Services**
    - IT-Grundschutz
        - Upgrade und Patching
        - Logging
    - Container Registry
        - Service Architektur
        - Service Umfang
        - IT-Grundschutz
        - Service Optionen
    - Agile Factory
        - Service Architektur
        - Service Umfang
        - IT-Grundschutz
        - Service Optionen
    - AnyCloudK8s
        - Service Architektur
        - Service Umfang
        - IT-Grundschutz
        - Service Optionen
    - Container Namespace
        - Service Architektur
        - Service Umfang
        - Service Optionen
- **Splunk Index**
        - Verfügbare Service-Optionen
        - Verfügbare Meta-Informationen
- **Enterprise Streaming Service**
    - Leistungsumfang Inventx
        - Managed Streaming Cluster
        - Schema Registry
        - Zugriffskontrolle & Mandantentrennung
        - Topic Management
        - Monitoring & Alerting
        - Security
        - Topic Monitoring & Logs
    - Verantwortung Kunde
        - Anbindung von Applikationen
        - Netzwerkkonnektivität
        - Schema-Registrierung

        - Monitoring-Nutzung
    - Service Level Parameter (SLP)
- **Zeichenlegende**

Einführung

Dieser Servicekatalog beschreibt die Leistungen, welche durch Inventx als standardisierte Cloud-Services im Rahmen der Produktlinie ix.Cloud erbracht werden.

Die Services der ix.Cloud werden auf der Inventx eigenen Community Cloud und ausschliesslich in schweizer Datacentern produziert. Die Architektur der Community Cloud folgt dem Ansatz einer Shared Infrastruktur, in welcher sich die Tenants den Hypervisor und die darunterliegende Hardware (Netzwerk, Storage und Compute) teilen.

Inventx definiert einen Tenant als die oberste Ordnungsinstanz, die datentechnisch und organisatorisch eine abgeschlossene Einheit darstellt. Dadurch wird die notwendige Isolierung zwischen Kunden sichergestellt. Jeder Tenant ist immer einem expliziten Kunden zugeordnet und dient nebst der Isolierung auch der Nutzung von Ressourcen und Services.

Die folgende Grafik veranschaulicht im mittleren Bereich die verfügbaren Service-Modelle (IaaS, PaaS, SaaS) und Service-Kategorien sowie im oberen Bereich die digitalen Kundenschnittstellen (Digital Customer Interfaces) zur Verwaltung der Services. Flankierend sind im unteren Bereich die allgemeinen Inventx Standards im Bereich Informationssicherheit und Compliance aufgeführt.

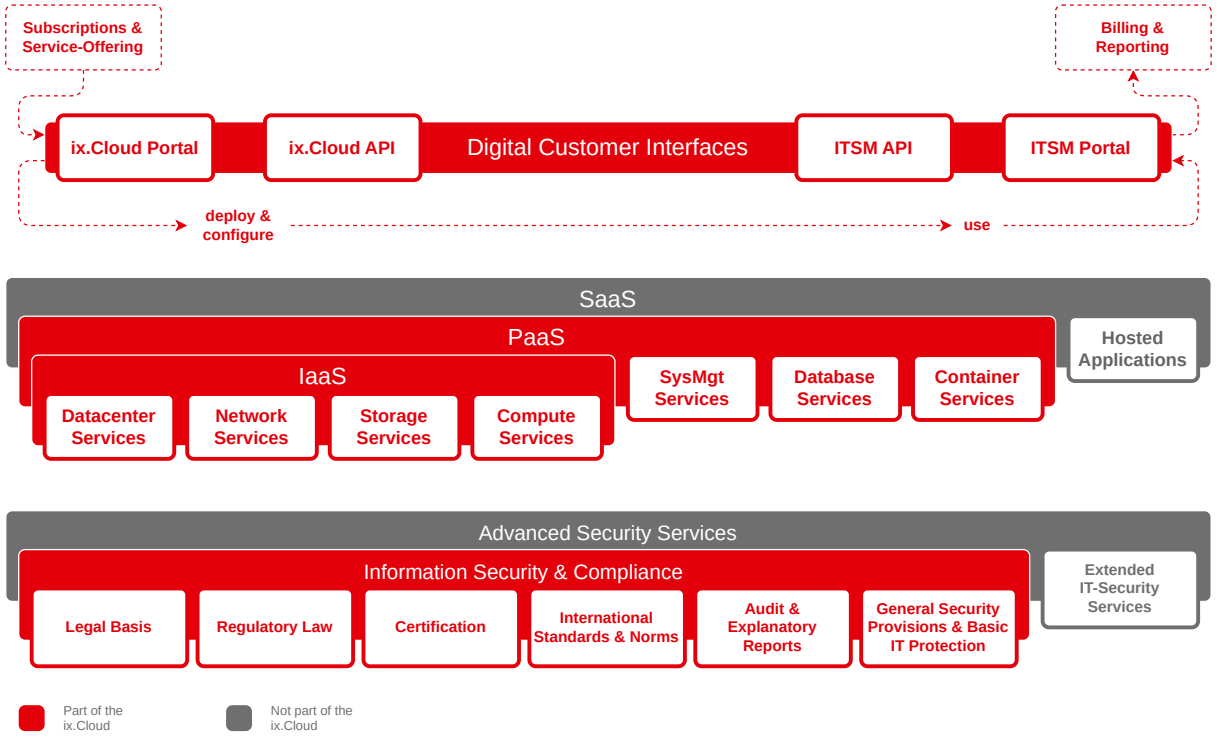


Bild: ix.Cloud Map

Service-Modelle und Service-Kategorien

Die Tabelle unten zeigt die in der ix.Cloud verfügbaren Service-Modelle und Service-Kategorien.

Tabelle: Service-Modelle und Service-Kategorien

Modell	Kategorie	Beschreibung
Infrastructure as a Service (IaaS)	Datacenter Services	Infrastruktur in den Inventx eigenen Rechenzentren (RZ). Dank gesichertem Zutritt, Brandschutz, sicherer Stromversorgung und Kühlung bleiben Anwendungen jederzeit verfügbar und Daten gesichert.
	Network Services	Bietet höchste Servicequalität durch Vernetzung von Cloud und On-Premises Infrastrukturen.
	Storage Services	Stellt sicheren, skalierbaren Cloudspeicher für Daten, Apps und Workloads bereit.
	Compute Services	Vorgefertigten Availability Sets und Rechenpower aus der Cloud on demand, nutzungsbasiert abgerechnet.
Plattform as a Service (PaaS)	System Management Services	Betriebsoptimierte Operation Services zum effizienten Bereitstellen und Betreiben von Businessanwendungen auf Virtuellen Maschinen.
	Database Services	Vollständig verwaltete Datenbankdienste ermöglichen barrierefreies und hoch skalierbares Daten-Management.
	Container Services	Continuous Delivery mit einfachen und zuverlässigen Tools für noch schnellere Entwicklung - Innovation im Zentrum.

Abhängig vom Service-Modell unterscheiden sich die Beistellpflichten von Kunde und Inventx. Dies bedeutet, dass beidseitig entsprechende Verantwortlichkeiten wahrgenommen werden müssen, damit eine Zielanwendung in der gewünschten Fertigungstiefe und mit den geforderten Sicherheits-Merkmalen bereitgestellt werden kann.

Die folgende Grafik veranschaulicht die Verantwortlichkeiten pro Service-Modell.

Bild: Verantwortlichkeitsmatrix

:::tip Managed Services

Zu allen Service-Modellen und Service-Kategorien können zusätzliche Managed Services zwischen Kunde und Inventx vereinbart werden. Dabei handelt es sich um individuelle Dienstleistungen, die nicht oder nur teilweise durch diesen Servicekatalog abgedeckt werden.

:::

Digitale Kundenschnittstellen

Inventx bietet den Kunden hochverfügbare digitale Schnittstellen im SLA Rhodium an, über welche die ix.Cloud Services und Ressourcen rund um die Uhr bezogen und verwalten werden können.

Die Autorisierung auf die digitalen Kundenschnittstellen wird über ein separates Onboarding Projekt definiert und umgesetzt.

ix.Cloud Portal

Mit dem ix.Cloud Portal steht den autorisierten Benutzern des Kunden ein Webportal zur Verfügung, wo die entsprechenden Services rund um die Uhr bestellt und verwaltet werden können. Jeder Kunde verfügt nach erfolgtem Onboarding-Projekt über mindestens einen Benutzer für das ix.Cloud Portal. Die

kundenindividuelle Benutzerverwaltung wird über einen Identity-Provider des Kunden (bspw. Active Directory) gesteuert und über einen Identity-Proxy (bspw. AD Federation Services) an das Portal übermittelt, welcher die Autorisierung sicherstellt.

Die zu übermittelnde Attribute sind:

Tabelle: Benutzermanagement ix.Cloud Portal

Kriterium	Beschreibung
Benutzername	Übermittlung des User Principal Names
Gruppenname	Übermittlung des Gruppennames

ix.Cloud API

Die ix.Cloud API bildet die Basis für eine standardisierte und automatisierte Verwaltung der ix.Cloud Services und zugleich die Voraussetzung zur Einbindung von IaC (infrastruktur as code). IaC ist der Prozess der Verwaltung und Bereitstellung von Ressourcen via Code anstelle von physischen Konfigurationen oder Einsatz von Konfigurations-Tools.

ITSM Portal

Das ITSM Portal der Inventx steht den definierten Benutzern des Kunden zur Abwicklung der gemeinsamen IT Service Management Prozesse im Rahmen von Service Requests und Incidents zur Verfügung.

ITSM API

Die ITSM API bildet die Grundlage für das Verknüpfen und Automatisieren der ITSM-Prozesse zwischen Kunde und Inventx.

Löschvorgang einer Ressource

Die Löschung einer Ressource erfolgt automatisiert über einen asynchronen Job. Unter normalen Bedingungen werden folgende Schritte durchgeführt: 1. Die entsprechenden Ressourcen werden auf dem Zielsystem entfernt. 2. Zugehörige Einträge in den umliegenden Systemen, wie zum Beispiel DNS, Monitoring, Backup und Billing, werden ebenfalls gelöscht. 3. Im IT-Service-Management-System (ITSM) wird der Status des Datensatzes auf „gelöscht“ gesetzt.

Im Fehlerfall gelten folgende Prozeduren: 1. Die Jobausführung wird automatisch in festgelegten Intervallen wiederholt. 2. Sollten die Wiederholungen nicht zum Erfolg führen, wird automatisch ein Incident erstellt. 3. Die Bearbeitung des Incidents erfolgt durch die zuständigen Fachteams, die auch die Vollständigkeit der Massnahmen sicherstellen.

Subscriptions und Service-Offering

Die ix.Cloud basiert auf drei grundlegenden Elementen - Tenant, Subscription und Ressourcen. Ein Tenant repräsentiert ein Unternehmen, welches sich in mehreren organisatorischen Einheiten - Subscriptions - unterteilen lässt. Eine Ressource ist ein verwaltbares Service-Element, das über das Portal bestellt werden kann und über eine Subscription konsumiert wird.

Ein Tenant muss mindestens eine Subscription beinhalten. Eine Subscription dient der Trennung und Abbildung von organisatorischen Strukturen durch folgende Punkte:

- Benutzer- und Rechteverwaltung
- Verwalten des Service-Offerings
- Verwalten und bestellen von Ressourcen
- Ausweisen und zuordnen von Kosten

Billing und Reporting

Billing und Reporting bezieht sich auf die Verrechnung der in diesem Service Katalog beschriebenen konsumierten Leistungen.

Die Verrechnung der Services erfolgt basierend auf dem Consumption Report (Metered Services) und die Rechnungstellung erfolgt monatlich nachschüssig.

Backup

Der Backup Service basiert auf einer hoch verfügbaren, skalierbaren und performanten Plattform in den Datacentern von Inventx, mit dem die Sicherung von Daten und bei Bedarf auch deren Wiederherstellung für einen Service oder eine komplette VM sichergestellt wird.

Service Architektur

Bild: Berechnung der Wiederherstellungszeit

Service Umfang

Tabelle: Backup Service Umfang

Leistungsmerkmale	
Zugriffskontrolle	■
Datenverschlüsselung	■
Unveränderbare Backups	■
Backup Profile	■
Monitoring & Logging	■
Datenintegrität	■
Datenwiederherstellung	■
Disaster Recovery (RTO und RPO)	■

Service Optionen

Zugriffskontrolle

Der Zugriff auf die Backup-Infrastruktur erfolgt rollenbasiert (RBAC/ixPAM) sowie mit einer Multifaktor-Authentifizierung (MFA).

Datenverschlüsselung

Die Backup Daten sind sowohl beim Transfer als auch über die gesamte Aufbewahrungsdauer verschlüsselt (AES-256, FIPS 140-2 compliant encryption of data in flight and at rest).

Unveränderbare Backups

Die Backup Daten können während der gesamten Aufbewahrungsdauer weder verändert noch gelöscht werden (Immutable Backup & DataLock/WORM). Dies bietet somit einen wirksamen Schutz gegen Ransomware oder mutwilliges Löschen von Backup Daten.

Backup Profile

Folgende Backup Profile können gewählt werden:

Tabelle: Backup Profile

Service Level	Bronze	Silber	Gold	Platin*	Rhodium
Backup Location	Local	Remote		Remote & DR-Datacenter	
Backup Intervall	Täglich				
Backup Retention	No Backup, 14, 40, 100, 200 oder 400 Tage				

* der Service Level Platin ist der Community ix.Cloud nicht verfügbar

Backup Location

Die Primärdaten werden grundsätzlich auf die Backup-Infrastruktur im entfernten Datacenter gesichert. Beim Service Level Platin*/Rhodium erfolgt eine zusätzliche Replikation (Kopie) der Daten in das DR-Datacenter.

:::info Als Option können zusätzliche Backup-Kopien innerhalb oder auch ausserhalb der Inventx Datacenter mittels "Generic Request" beauftragt werden. :::

Backup Intervall

Das Intervall definiert den Zeitabstand, in dem jeweils eine Datensicherung erstellt wird. Es erfolgt mindestens einmal täglich ein inkrementeller Backup, bei Datenbanken werden die Logs (Archive-, Transaction-Logs, etc.) mehrmals stündlich gesichert.

Backup Retention

Die Retention bestimmt die Aufbewahrungsdauer der Datensicherungen in Tagen. Nach Ablauf der gewählten Frist, werden die Daten nichtwiederherstellbar gelöscht.

:::caution Beim Backup-Profile “No Backup” verzichtet der Kunde gemäss explizitem Wunsch auf eine Datenwiederherstellung! Dies gilt sowohl für die primären Daten auf Stufe OS, Datenbank, Applikation, etc. und beinhaltet auch das Cloning mittels Backup-Restore auf eine VM/DB, bei welcher das Backup-Profile “No Backup” gewählt wurde! :::

Monitoring & Logging

Die Inventx überwacht den Backup-Prozess und stellt sicher, dass dieser in der geplanten Regelmässigkeit durchgeführt wird. Alle relevanten Zugriffe, Änderungen an Konfigurations- oder Systemparameter werden in einem Audit-Log festgehalten.

Datenintegrität

Die eingesetzte Backup Lösung stellt sicher, dass die Daten während der Übertragung verschlüsselt und nach der Speicherung der Kopie auch vor versehentlichen oder böswilligen Änderungen sowie vorzeitigem Löschen durch WORM-Technologie geschützt sind.

Datenwiederherstellung

Die monolithische Wiederherstellung einer kompletten VM erfolgt im Self-Service über das ix.Cloud-Portal. Datei- oder Datenbankbasierte Wiederherstellungen müssen in der Regel via "Generic Request" beauftragt werden.

Wiederherstellung im Notfall (RTO und RPO)

RTO und RPO definieren im Rahmen eines Notfalls die maximale Dauer der Wiederherstellung (RTO) einer Anwendung, eines Systems und/ oder Prozesses und den maximalen Datenverlust (RPO).

Tabelle 1: SLA - Wiederherstellung im Notfall (RTO und RPO)

Service Level	Bronze	Silber	Gold	Platin	Rhodium
Recovery Time Objective (RTO)	-	Best Effort	48h	2h	2h
Recovery Point Objective (RPO)	Best Effort	24h	15min	0min	0min

Recovery Time Objective (RTO)

Die Konstellation bei einem Notfall kann sehr unterschiedlich sein und einen Einfluss auf diesen Service Level haben. Der Wert hängt dabei sehr stark von der Anzahl gleichzeitiger Wiederherstellungen ab, d.h. bei mehreren gleichzeitigen Wiederherstellungen kann der Wert pro Wiederherstellung geringer sein. Bei einer Wiederherstellung kann von einem Richtwert im Bereich 200-400 MB/s ausgegangen werden.

Recovery Point Objective (RPO)

Schadenereignisse hervorgerufen durch manipulierte, respektive korrupte Daten werden ausschliesslich durch die Backup relevanten Qualitätselemente im SLA abgedeckt. Dies bedeutet, dass falls korrupte Daten im Live-System vorhanden sind, diese lediglich aus einem Backup korrigiert werden können und der angegeben RPO somit nicht zur Anwendung kommt.

{/* Do not remove this is only used in the PDF the current date */} export const Datum = ({}) => (

Version: {new Date().toISOString().replace(/T/, ' ').replace(/.. /, '').slice(0, -8)}

);

This document is machine translated. German language is contractual binding.

Service Level Framework

:::info

Die vertraglich verbindlichen Service Levels werden im Rahmenvertrag zwischen dem Kunden und Inventx geregelt. Die in diesem Kapitel aufgeführten Werte sind nicht vertragsverbindlich, sondern dienen ausschliesslich dazu, den Kontext für die im Service Catalog beschriebenen Services herzustellen.

:::

Leistungsübergabepunkt

Der Leistungsübergabepunkt (LÜP) definiert die technische Schnittstelle, an welcher die Leistungserbringung von Inventx endet und die Verantwortung an den Kunden übergeht. Je nach Service-Modell wird der LÜP auf unterschiedlichen Ebenen festgelegt, woraus sich pro Ebene eigene Service Level Targets ergeben.

Leistungsübergabepunkt Infrastructure

Der LÜP Infrastructure gilt für alle Services, deren Leistungserbringung auf Ebene der Infrastruktur (IaaS) endet – also dort, wo Inventx die zugrundeliegenden physischen und virtualisierten Ressourcen bereitstellt. Die nachfolgenden Service Level Targets beziehen sich auf die Verfügbarkeit auf dieser Ebene und gelten für sämtliche Services, die auf diesem Leistungsübergabepunkt aufsetzen.

Tabelle: LÜP Infrastructure

SLP	Bronze	Silber	Gold	Platin	Rhodium

Availability	n.a.	99.40%	99.40%	99.90%	99.90%
Outage Frequency p.m.	n.a.	2	2	1	1
Outage Frequency p.a.	n.a.	6	6	4	4

Leistungsübergabepunkt Platform

Der LÜP Platform gilt für alle Services, deren Leistungserbringung auf Ebene der Plattform (PaaS) endet – also dort, wo Inventx zusätzlich zur Infrastruktur auch die betriebsbereite Plattform bereitstellt und verantwortet. Die nachfolgenden Service Level Targets beziehen sich auf die Verfügbarkeit auf dieser Ebene und gelten für sämtliche Services, die auf diesem Leistungsübergabepunkt aufsetzen.

Tabelle: LÜP Platform

SLP	Bronze	Silber	Gold	Platin	Rhodium
Availability	Best Effort	99.20%	99.60%	99.80%	99.95%
Outage Frequency p.m.	Best Effort	1	1	1	1
Outage Frequency p.a.	Best Effort	9	9	6	4
Max. Net Downtime per Incident	Best Effort	Best Effort	Best Effort	Best Effort	Best Effort

Service Time

Für jedes in den vorangehenden Abschnitten aufgeführte Service Level Target gilt – unabhängig vom Leistungsübergabepunkt – folgende Service Time:

Tabelle: Service Time pro Service Level

Abstufung	Service Time
Bronze, Silber	Standard
Gold, Platin, Rhodium	7 x 24

ix.Cloud Edge

Service-Beschreibung: Public DNS Service ix.Cloud Edge

Der Public DNS Service ist Teil des Internet-Perimeters ix.Cloud Edge und ermöglicht die autoritative Namensauflösung öffentlicher Zonen. Die Zonen-Verteilung erfolgt global über ein Anycast Network. Der Service erfüllt regulatorische Vorgaben (revDSG / FINMA) durch lokalisierte Datenhaltung und revisionssichere Prozesse.

Der Service steht ausschliesslich im SLA Rhodium zur Verfügung und muss via "Generic Request" bestellt werden.

Service Architektur

Die Verwaltung der Zonendaten erfolgt zentral auf der Inventx-Infrastruktur über einen nicht aus dem Internet erreichbaren Server (Hidden-Primary). Die Beantwortung der weltweiten DNS-Anfragen wird über ein vorgeschaltetes Anycast Network ausgeliefert.

Diese verteilte Architektur eliminiert Single Points of Failure und reduziert Latenzen.

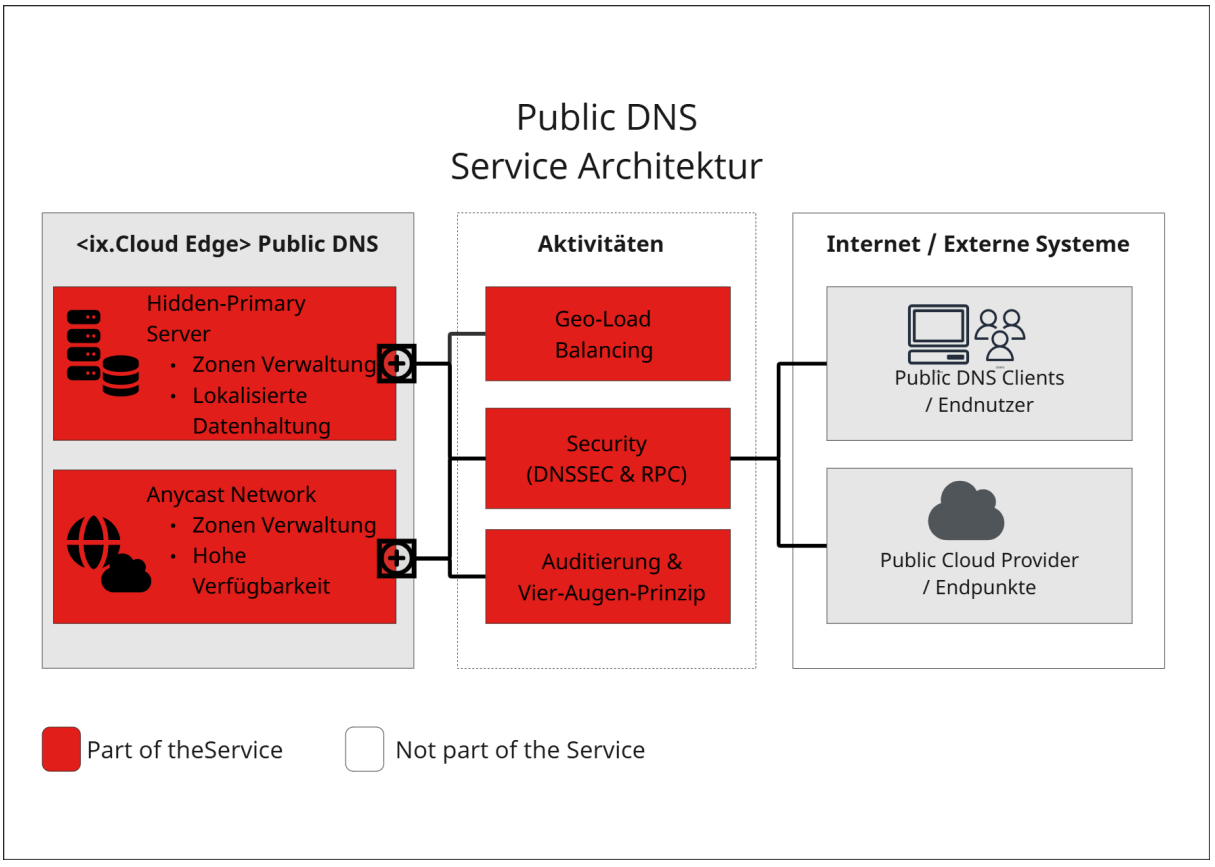


Bild: Public DNS Service Architektur

Service Umfang

Tabelle: Public DNS Service Umfang

Leistungsmerkmal	SLA Rhodium
Initiales Setup	■
Hidden-Primary Architektur	■
Anycast Zonen-Verteilung	■
GeoLoad-Balancing	■
Security (DNSSEC & RPC Listen)	■
Revisionssicherheit & Compliance	■

(■ = Im Standard-Service enthalten, □ = Projektbasierte / Einmalige Leistung)

Service Optionen

Die folgenden Leistungselemente definieren den Service und seinen Betrieb:

Initiales Setup

Die initiale Spezifikation, Konfiguration sowie die Migration bestehender öffentlicher Zonen erfolgen im Rahmen eines initialen Setups in Zusammenarbeit mit dem Kunden.

Hidden-Primary & Zonen-Verteilung

Die Zonenverwaltung erfolgt auf einem internen Primärserver (Hidden-Primary) zur Reduzierung der Angriffsfläche. Die Verteilung der Zonen-Informationen an Clients erfolgt ausschliesslich über das Anycast Network. Souveräner Fallback läuft über den Hidden-Primary.

GeoLoad-Balancing

DNS-Anfragen können dynamisch an Internet-Endpunkte über verschiedene Standorte hinweg delegiert werden. Dies umfasst ix.Cloud-Standorte sowie angebundene Public Cloud Provider zur verteilten Lastensteuerung.

Security & Administration

- **DNSSEC:** Kryptografische Absicherung der DNS-Antworten gegen Manipulation.

- **RPC Listen:** Einspielen von Response Policy Zones zur aktiven Filterung und Steuerung von Namensauflösungen.
- **Administration:** Zonenverwaltung strikt nach dem Vier-Augen-Prinzip inklusive revisionssicherer Auditierung.

Unterstützte Record-Typen

Für die öffentlichen Zonen (Forward-Mapping) werden folgende DNS-Records unterstützt:

Tabelle: Unterstützte Record-Typen

Record Typ	Forward-Mapping	Reverse Mapping	Einsatzzweck / Beschreibung
A Record	■		Auflösung eines Hostnamens in eine IPv4-Adresse.
AAAA Record	■		Auflösung eines Hostnamens in eine IPv6-Adresse.
CNAME Record	■		Alias-Eintrag, der einen Hostnamen auf einen anderen verweist.
MX Record	■		Definition der zuständigen Mailserver für den E-Mail-Empfang der Domain.
NS Record	■		Definition der zuständigen Nameserver für eine Zone oder Subzone (Delegierung).
PTR Record		■	Auflösung einer IP-Adresse in einen Hostnamen (Reverse-Mapping), häufig genutzt zur Verifizierung von Mailservern zur Spam-Vermeidung.
SRV Record	■		Definition der Erreichbarkeit spezifischer Dienste (inkl. Port und Protokoll).
TXT Record	■		Hinterlegung von Textinformationen, häufig genutzt für Sicherheits- und Verifizierungszwecke (z. B. SPF, DKIM, DMARC).
CAA Record	■		Festlegung, welche Zertifizierungsstellen (CAs) berechtigt sind, TLS/SSL-Zertifikate für die Domain auszustellen.

Datacenter Services

Die Datacenter Services von Inventx umfassen den gesamten Lebenszyklus von der Planung (Plan) über den Aufbau (Build) bis hin zum Betrieb (Run) der zentralen Datacenter Infrastruktur in den Datacenter ix.DC1 (Chur), ix.DC2 (St. Gallen) und ix.DC3 (Gais). Die folgende Tabelle liefert eine Übersicht der Leistungsmerkmale pro Service-Modell. Diese bildet die Basis für alle in diesem Servicekatalog beschriebenen Services.

Tabelle: Datacenter Service Umfang

Leistungsmerkmal	IaaS	PaaS
Datacenter Standorte auf Schweizer Staatsgebiet	✓	✓
Rechenzentrumskomplex verteilt auf zwei geographisch separate Geländekammern mit wegredundanter Backbone-Erschliessung	✓	✓
Autonomes Alarmierungssystem für alle wichtigen Infrastruktur-Komponenten	✓	✓
Zugangskontrollsysteme gegen unberechtigten Zutritt zusätzlich mit Vereinzelungssystemen und Personenschleusen	✓	✓
Interventions- und Fluchtmöglichkeiten im Ereignisfalls	✓	✓
Alle Zugänge einbruchdämmend ausgeführt	✓	✓
Einbruchmeldeanlage	✓	✓
Videoüberwachung	✓	✓
Zwei unabhängige, getrennte Stromversorgungen	✓	✓
Redundante Unterbrechungsfreie Stromversorgung (USV)	✓	✓
Stromgeneratoren mit Netzersatzanlage (Diesel)	✓	✓
Überspannungsschutz und Blitzschutz	✓	✓
Redundante Stromversorgung innerhalb des Racks	✓	✓
Klimaüberwachung	✓	✓
Redundante Kühlung der Racks	✓	✓
Brandfrüherkennung	✓	✓

Handfeuerlöscher	✓	✓
Wassersensoren	✓	✓

Folgende Datacenter Services stehen zur Verfügung:

Tabelle: Datacenter Services

Service Name	Service Kurzbeschreibung
Cloud Connect	Anbindung der OnPremise-IT mit der ix.Cloud
Rack Collocation	Miete von Rack-Space im Inventx Rechenzentrum

Cloud Connect

Dieser Service umfasst den Betrieb und die Administration der Kommunikationsinfrastruktur in den Datacentern von Inventx als Bindeglied der Systemhardwarekomponenten untereinander bzw. deren Kommunikationsschnittstellen zum Ein- und Ausgang der Datacenter.

Service Architektur

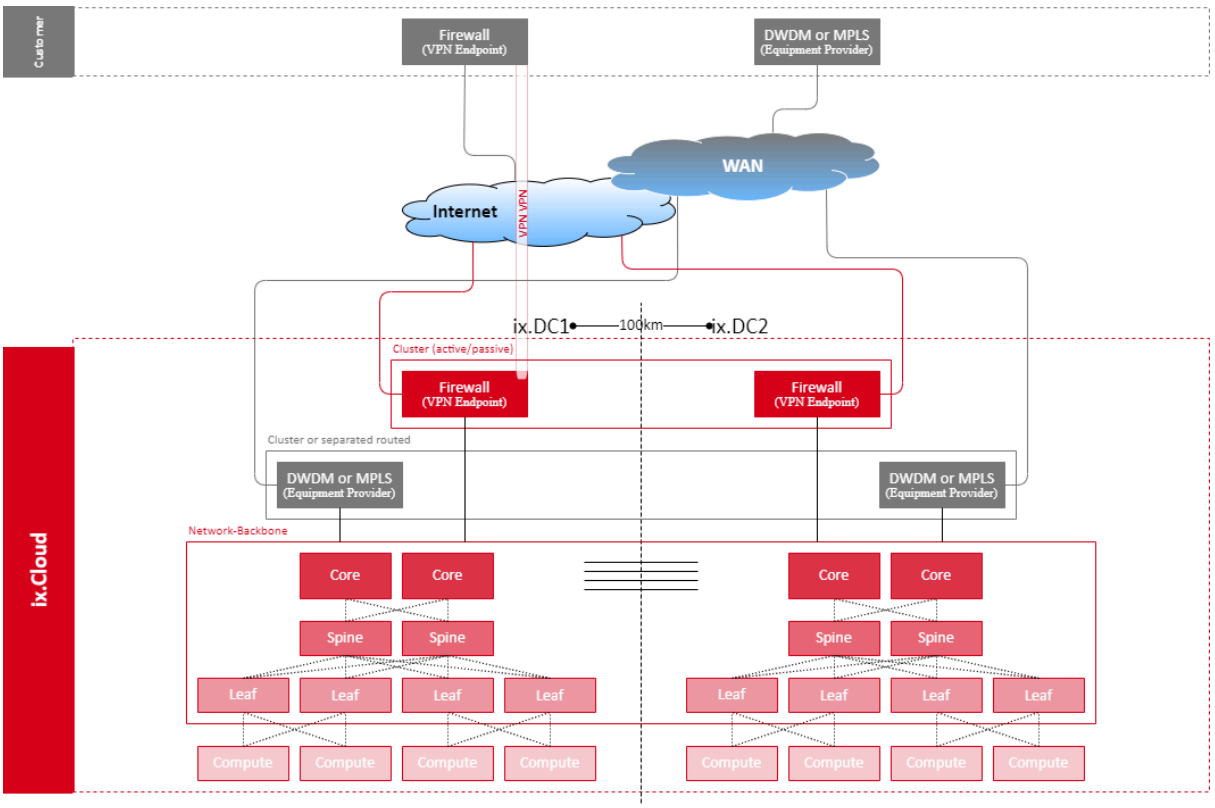


Bild: Cloud Connect Service Architektur

Service Umfang

Tabelle: Cloud Connect Service Umfang

Leistungsmerkmal	IaaS	PaaS
Datacenter LAN-Infrastruktur	■	■
Datacenter Interconnect	■	■
Private Connectivity Provider Equipment	□	□
Shared Internet Access	□	□

Service Optionen

Mit dem "Cloud Connect" Service kann der Kunde eine private Verbindung zu seinen Services in der ix.Cloud herstellen, die je nach Anforderung unterschiedlich ausgeprägt ist.

Datacenter LAN-Infrastruktur

Die Services der Service-Modelle IaaS und PaaS werden mittels der durch Inventx betriebenen Datacenter LAN-Infrastruktur auf Basis der folgenden Leistungsmerkmale betrieben:

Tabelle: Cloud Connect Datacenter LAN-Infrastruktur

Leistungsmerkmal	IaaS	PaaS
Striktes Zonenkonzept auf Infrastruktur und Sicherheitsebene	■	■
Zonentrennung durch Firewalls	■	■
Kein Sharing von Infrastrukturkomponenten über Zonen hinweg	■	■
Dedizierte Kunden-Zonen	■	■
Dedizierte und gesharte Service-Zonen	■	■
Skalierbare und redundante Sicherheitskomponenten	■	■

Datacenter Interconnect

Die Rechenzentren der Inventx werden durch den Datacenter Interconnect sicher und performant verbunden. Diese WAN-Verbindung wird wie folgt und als integraler Bestandteil der entsprechenden IaaS- und PaaS-Services durch Inventx betrieben:

Tabelle: Cloud Connect Datacenter Interconnect

Leistungsmerkmal	IaaS	PaaS
Wegredundante, private Verbindung zwischen den Datacentern von Inventx	■	■
Verschlüsselte Kommunikation	■	■

Private Connectivity Provider Equipment

Der Kunde kann über die WAN-Infrastruktur seines Connectivity-Providers eine nach seinen Anforderungen ausgestaltete, private Netzwerkanbindung in die Rechenzentren der Inventx realisieren. Der Kunde stellt dabei eine Verbindung über MPLS/DWDM oder Dark Fiber zur Verfügung, die dann im Rechenzentrum von Inventx terminiert und so die in der ix.Cloud betrieben Services erschliesst. Die dazu nötige Infrastruktur des Connectivity-Providers des Kunden wird auf Basis des Rack Collocation Service im Datacenter von Inventx betrieben. Der Kunde muss dabei die für die Finanzindustrie üblichen Standards der IT-Security sicherstellen, insb. Distributed Denial of Service (DDoS) und 1. Firewall Stufe.

Shared Internet Access

Der Shared Internet Access basiert auf dem Inventx eigenen IP-Range inkl. BGP-Peerings zu zwei unterschiedlichen Providern und terminiert mit je einer Anbindung auf die globale Firewall-Instanz in den georedundanten Datacentern der Inventx. Diese globale, transparente Firewall-Instanz von Inventx ist zwingendes Verbindungselement zur ersten Firewall-Stufe des Kunden, die als VPN-Endpoint dient. Auf dieser globalen, transparenten Firewall-Instanz werden die folgenden Firewall-Richtlinien umgesetzt:

Tabelle: Cloud Connext Shared Internet Access Firewall Richtlinien

Leistungsmerkmal	IaaS	PaaS
Distributed Denial of Service (DDoS)	■	■
Botnet Control Services	■	■
Application Control Analytics	■	■

Die IP-Adressierung zwischen der globalen, transparenten Firewall-Instanz und der ersten Firewall-Stufe des Kunden wird von Inventx geliefert. Diese kostenpflichtigen IP-Adressen können blockweise in folgenden Mengen bezogen werden: 2/4/8/12/16/20/30/40/50 Adressen. Die Anzahl der IP-Adressen kann unter Einhaltung einer Frist von 3 Arbeitstagen mittels "Generic Request" jeweils per 1. des Folgemonats verändert werden.

Dieser Service wird ausschliesslich im SLA Platin angeboten. Es gilt dabei zu beachten, dass Inventx die Verantwortung für den OnPremise VPN-Endpoint des Kunden nicht übernimmt und den VPN-Endpoint in der ix.Cloud nur übernimmt, wenn dieser auf einer Komponente endet, die Inventx betreibt.

Die gewünschte Bandbreite kann für den Kunden reserviert und unter Einhaltung einer Frist von 3 Arbeitstagen mittels "Generic Request" jeweils per 1. des Folgemonats verändert werden. Folgende Bandbreiten stehen zur Verfügung:

Tabelle: Cloud Connect Shared Internet Access Bandbreiten

Leistungsmerkmal	IaaS	PaaS
20 Mpbs	■	■
50 Mpbs	■	■
100 Mpbs	■	■
200 Mpbs	■	■

Rack Collocation

Beim Service Rack Collocation mietet der Kunde via "Generic Request" ein komplettes, dediziertes Rack oder den gewünschten Bedarf an Höheneinheiten in einem geteilten Rack in den Rechenzentren der Inventx. Die Systeme werden in diesem Fall durch den Kunden selbst verwaltet. Der Stromverbrauch wird individuell und nach effektivem Verbrauch abgerechnet. Der Strompreis wird jährlich gemäss Preisniveau der Stromlieferanten angepasst.

Dieser Service steht nicht als Einzelservice zur Verfügung, sondern nur in Kombination mit weiteren Services dieses Servicekatalogs. Kunden profitieren durch diesen Service in den Fällen, in denen nebst dem Cloud-Service auch eine Lösung für das Hosting nicht cloud-fähiger Applikationen, Systeme oder Appliances nötig ist.

Service Architektur

n/a

Service Umfang

Tabelle: Rack Collocation Service Umfang

Leistungsmerkmal	Shared	Dedicated
Dediziertes Rack	-	■
Einzelne Höheneinheiten (HE)	■	-

Netzwerk Verbindungen in die entsprechend definierten Kunden-Netzwerkzonen und nach Aussen (z.B. Internet)	■	■
Strom on Demand	■	■
Remote Hands and Eyes	□	□
Kundenzugang	□	□

Service Optionen

Als Ergänzung zum Rack Collocation Service kann der Kunde weitere Dienstleistungen nach Absprache und wie folgt beziehen:

Remote Hands and Eyes

Benötigte Hands- und Eyes-Dienstleistungen gilt es mittels "Generic Request" anzumelden. Diese werden gemäss vereinbartem Stundensatz in Regie abgerechnet.

Kundenzugang

Der Zugang durch Kunden ist ausschliesslich nach Voranmeldung via "Generic Request" und nur nach strikt über einen definierten Prozess zu genehmigenden Ausnahmefällen möglich. Die folgenden Richtlinien sind dabei zu berücksichtigen:

- Kunden werden in mindestens 1:1 Begleitung durch Inventx-Mitarbeiter begleitet.
- Die angemeldeten Personen des Kunden müssen sich vor dem Zugang ins Datacenter mit einem amtlichen Ausweisdokument identifizieren.
- Es wird ein Journal über die Zugänge geführt.
- Personen dürfen keine Handys oder Smartwatches mit Fotofunktion oder Fotoapparate in die Datacenter-Räume mitbringen.
- Sämtliche Arbeiten durch Inventx werden in Regie gemäss Rahmenvertrag abgerechnet.

Network Services

Die Network Services in der ix.Cloud umfassen die folgenden Optionen, um Services innerhalb der ix.Cloud untereinander zu vernetzen und externe Services mit Services in der ix.Cloud zu verbinden:

Tabelle: Network Services

Service Name	Service Kurzbeschreibung

Firewall	Elementare Sicherheit zwischen verschiedenen Subnetzen
Server Proxy	Indirekte und restriktive Kommunikation für Server der ix.Cloud
Load Balancer	Verteilung eingehender Verbindungen auf Anwendungen oder Service-Endpunkte
Web Application Firewall	Bietet Sicherheit für online Dienste vor böswilligem Internetverkehr und filtert Bedrohungen wie OWASP TOP 10 welche Online-Anwendungen negativ beeinträchtigen
Private DNS	Auflösung von IP-Adressen zu DNS-Namen innerhalb der ix.Cloud
Secure Mail-Relay	Sichere E-Mail-Zustellung aus all Ihren Systemen innerhalb der ix.Cloud
Hosted Software-Appliance	Virtuelle Server für Software-Appliances, ohne Support für Microsoft Hyper-V

Firewall

Der Firewall-Service ist ein von Inventx verwalteter, cloudbasierter Netzwerksicherheitsdienst, über den die virtuellen Netzwerk-Ressourcen innerhalb der ix.Cloud geschützt werden können. Dieser Service ist ausschliesslich im SLA Platin verfügbar.

Die Richtlinien zur Anwendungs- und Netzwerkkonnektivität werden übergreifend für sämtliche Abonnements der ix.Cloud und virtuellen Netzwerke zentral erstellt und protokolliert. Es können Netzwerke und IP-Adressen zwischen verschiedenen Quellen (Sources) und Zielen (Destinations) freigeschaltet werden. Die Verbindungen werden auf definierte Services (insb. TCP/UPD-Ports) eingeschränkt.

Service Architektur

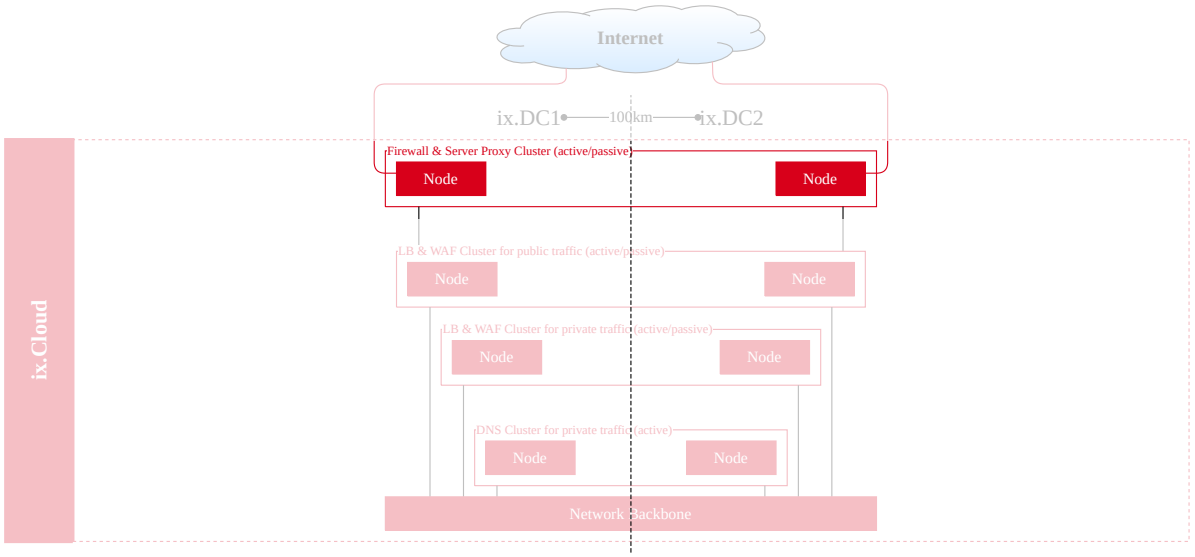


Bild: Firewall Service Architektur

Service Umfang

Tabelle: Firewall Service Umfang

Leistungsmerkmal	Platin
Initiales Setup	☐
IT Grundschutz	■
FQDN-Anwendungsfilterregeln	■
Filterregeln für Netzwerkdatenverkehr	■
SNAT-Unterstützung	■
Protokollierung (Logging)	■
DNAT-Unterstützung	☐
UTM-Features	☐

IT Grundschutz

Upgrade/Patching

Die Firewall-Infrastruktur wird halbjährlich aktualisiert, es sei denn, es treten kritische Sicherheitslücken auf, welche ein sofortiges Upgrade erfordern.

Logging

Das Logging erfolgt über eine zentrale Instanz, an die sämtliche Logs zur Analyse und Auswertung gesendet werden. Die Logs werden 14 Tage lang live aufbewahrt und anschliessend für 800 Tage archiviert.

Malware Schutz

Der Malware-Schutz basiert auf gehärteten Appliances die beim booten durch secure boot auf ihre Integrität geprüft werden. Secure Boot stellt sicher, dass nur vertrauenswürdige und signierte Firmware und Software auf der Hardware geladen wird. Der Boot-Prozess startet mit einem unveränderlichen, in die Hardware eingebetteten Code und verifiziert nachfolgende Komponenten. Die Geräte überprüfen regelmässig die Integrität der installierten Firmware durch kryptografische Signaturen. Firewall-ASICs sind speziell entwickelte Hardware-Sicherheitsprozessoren, die viele der Sicherheitsfunktionen wie Verschlüsselung und Deep Packet Inspection (DPI) hardwareseitig beschleunigen. Die Systempartitionen, die für die Ausführung der Betriebssystem- und Konfigurationsdaten verantwortlich sind, sind von den Benutzerdaten und Anwendungen isoliert.

Service Optionen

Beim Firewall Service kann der Kunde weitere Dienstleistungen nach Absprache beziehen:

Initiales Setup

Die Umsetzung der initialen Konfiguration des Firewall-Service wird im Rahmen eines Projekts verrechnet. Dabei wird das kundenindividuelle Ruleset in Zusammenarbeit mit dem Kunden spezifiziert und anschliessend implementiert. Sämtliche Änderungen sind mit einem "Generic Request" zu beauftragen.

FQDN-Anwendungsfilterregeln

Kunden können den ausgehenden HTTP/S-Datenverkehr auf eine angegebene Liste vollständig qualifizierter Domänennamen (FQDN) beschränken, wobei Wildcard-Einträge über die UTM-Feature Option abgebildet werden müssen. Das FQDN-Feature erfordert keine SSL-Terminierung.

Filterregeln für Netzwerkdatenverkehr

Die kundenspezifischen Netzwerkfilterregeln zum Zulassen oder Verweigern nach Quell- und Ziel-IP-Adresse, Port und Protokoll werden von Inventx zentral gepflegt. Die Firewall ist zustandsbehaftet (stateful), so dass zwischen legitimen Paketen für verschiedene Arten von Verbindungen unterschieden werden kann. Die Regeln werden übergreifend für sämtliche Abonnements der ix.Cloud und virtuellen Netzwerke forciert und protokolliert.

SNAT-Unterstützung

Alle IP-Adressen für ausgehenden Datenverkehr des virtuellen Netzwerks in der ix.Cloud werden in die öffentliche IP-Adresse der Firewall übersetzt (Source Network Address Translation). Sie können Datenverkehr aus Ihrem virtuellen Netzwerk an Remoteziele im Internet identifizieren und zulassen. Die

SNAT-Funktionalität kann optional auch für den internen Datenverkehr in der ix.Cloud implementiert werden.

Protokollierung (Logging)

Alle auf der Inventx terminierende und von der Inventx verantwortende Verbindungen werden protokolliert. Dies bedeutet, dass alle eingehenden sowie ausgehenden Verbindungen externer wie auch interner Herkunft aufgezeichnet werden.

Die Aufbewahrungsdauer beträgt 2 Jahre. Ein Log-Reporting an den Kunden ist bei Bedarf via "Generic Request" zu beauftragen.

DNAT-Unterstützung

Der eingehende Netzwerkdatenverkehr zur öffentlichen IP-Adresse der Firewall in der ix.Cloud, wird in die privaten IP-Adressen in den virtuellen Netzwerken des Kunden übersetzt (Destination Network Address Translation) und gefiltert. Die DNAT-Funktionalität kann optional auch für den internen Datenverkehr in der ix.Cloud implementiert werden.

UTM-Features

Die optionalen UTM-Features (Unified Threat Management) werden zusammen mit dem Kunden spezifiziert und danach durch Inventx betrieben.

Server Proxy

Sollen die Server in der ix.Cloud zur Erhöhung der IT-Sicherheit nicht direkt mit dem Internet kommunizieren, so ermöglicht der Server Proxy den Server-Systemen der ix.Cloud über definierte Regeln nur gewisse Adressen im Internet aufzurufen. Auf diesem Explizit-Proxy wird der Zugriff über verschiedene Technologien wie Web-Filter, Viren-Filter, Kategorien und Anwendungssteuerung kontrolliert und eingeschränkt. Alle Zugriffe (Ausnahmen möglich) werden mittels Deep-Inspection (Aufbrechen des Traffics) überprüft, wobei sich Inventx an die gesetzlichen Vorgaben des Datenschutzes hält.

Der Server Proxy steht als Shared Service ausschliesslich im SLA Platin zur Verfügung und muss über den "Generic Request" bestellt und verwaltet werden. Der Server Proxy kann nur von serverbasierten Systemen genutzt werden und steht für Clients nicht zur Verfügung.

Service Architektur

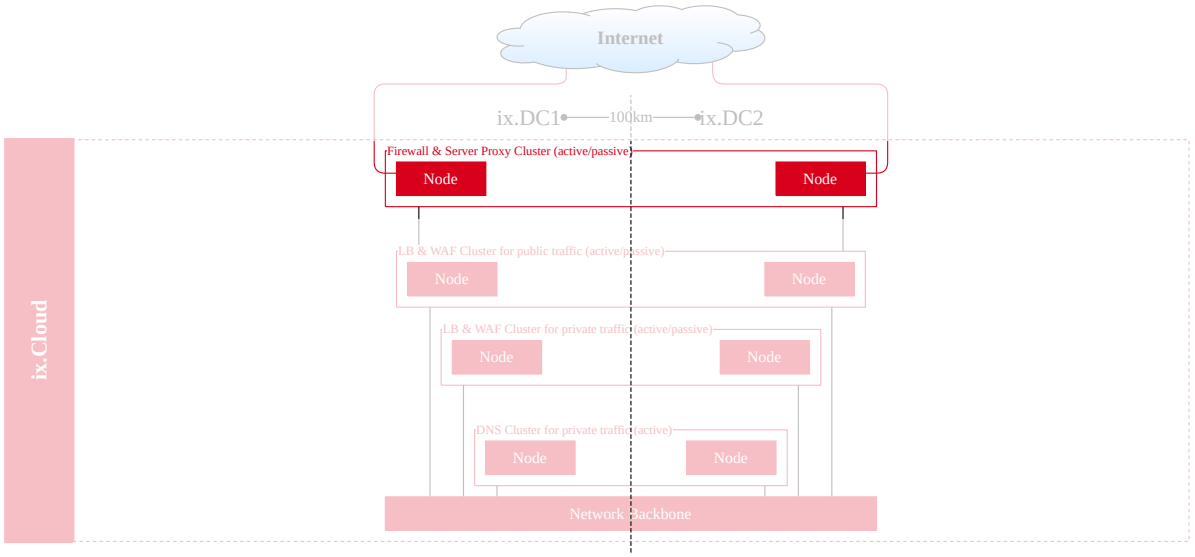


Bild: Server Proxy Service Architektur

Service Umfang

Tabelle: Server Proxy Service Umfang

Leistungsmerkmal	Platin
Initiales Setup	□
IT Grundschutz	■
Standard-Richtlinie für Protokolle und Ports	■
Standard-Richtlinie für Web-Filter	■
Standard-Richtlinie für Viren-Filter	■
Standard-Richtlinie für Anwendungssteuerung	■
Standard-Richtlinie für Deep-Inspection	■

IT Grundschutz

Siehe Beschreibung Kapitel Firewall IT Grundschutz.

Service Optionen

Beim Server Proxy Service kann der Kunde aktuell keine optionalen Dienstleistungen beziehen.

Initiales Setup

Der Server Proxy als Shared Service kann nicht individuell an Kundenbedürfnisse angepasst werden und es stehen ausschliesslich globale Filterkonfigurationen zur Verfügung.

Ist eine individuelle Konfiguration des Server Proxy Services gewünscht, so wird dies im Rahmen eines Projekts erarbeitet und verrechnet. Während dem Projekt wird das kunden-individuelle Ruleset in Zusammenarbeit mit dem Kunden auf Basis des Inventx Standard Rulesets spezifiziert und auf einem privaten Server Proxy implementiert.

Standard-Richtlinie für Protokolle und Ports

Inventx pflegt eine Standard-Richtlinie für alle serverbasierten Systeme der ix.Cloud. Im Inventx-Standard werden die folgenden Services und Ports zugelassen:

Tabelle: Server Proxy Standard-Richtlinie für Protokolle und Ports

Protokoll	Proxy-Port(s)	Socks-Port(s)
HTTP	80	-
HTTPS	443	-
SSH	-	22

Standard-Richtlinie für Web-Filter

Der Web-Filter kategorisiert alle Internetseiten anhand vordefinierter Algorithmen (Hersteller Vorgabe), welche erlaubt oder blockiert werden. Die globale Konfiguration basiert auf Inventx Standards, wobei folgende Kategorien zugelassen sind:

Tabelle: Server Proxy Standard-Richtlinie für Web-Filter

Web-Kategorie	Zugelassen
Business	■
Finance and Banking	■
Information Technology	■
Information and Computer Security	■

Standard-Richtlinie für Viren-Filter

Die globale Standard-Policy von Inventx entscheidet, welche ein- und ausgehenden Inhalte auf Viren untersucht werden und vermeidet so das Eindringen von schädlicher Software, wobei sämtlicher HTTP- und FTP-Datenverkehr analysiert wird.

Standard-Richtlinie für Anwendungssteuerung

Mithilfe der Anwendungssteuerung (Application Control) werden unerwünschte Funktionen von Webseiten ausgeschaltet. So kann zum Beispiel das Streamen von Audio- und Video-Dateien, das Chatten und das Hoch- und Herunterladen von Dateien verhindert werden. Das globale Ruleset von Inventx ist wie folgt definiert:

Tabelle: Server Proxy Standard-Richtlinie für Anwendungssteuerung

Web-Kategorie	Gesperrt
Webmail (z.B. Gmail oder GMX)	■
Game	■
Mobile	■
P2P	■
Remote Access	■
Social Media	■
Video/Audio	■
VOIP	■
Unknown Applications	■

Standard-Richtlinie für Deep-Inspection

Der Server Proxy überprüft die HTTPS-Pakete, wobei die Kategorien "Health and Wellness", "Finance and Banking" aus datenschutzrechtlichen Gründen nicht analysiert werden. Dabei wird der HTTPS-Verkehr entschlüsselt, überprüft, wieder verschlüsselt und an das Ziel weitergeleitet.

Load Balancer

Ein Load Balancer verteilt den Datenverkehr eines bestimmten Service-Endpunkts auf mehrere Ziele. Dabei werden fehlerhafte Ziele erkannt und der Datenverkehr nur an intakte Ziele weitergeleitet. Dadurch können die Verfügbarkeit und Performance einer Anwendung optimiert werden.

Für HTTP/HTTPS-Anwendungen empfiehlt sich ein Load Balancer auf Layer 7, während bei Anwendungen mit TCP/UDP-Protokoll ein Load Balancer auf Layer 4 empfohlen wird.

Dieser Service ist nur im SLA Platin verfügbar. Layer 4 Load Balancer können über das Portal im Self-Service bestellt und verwaltet werden. Die übrigen Load Balancer müssen über den Service Request

"Load Balancer" bestellt und verwaltet werden.

Service Architektur

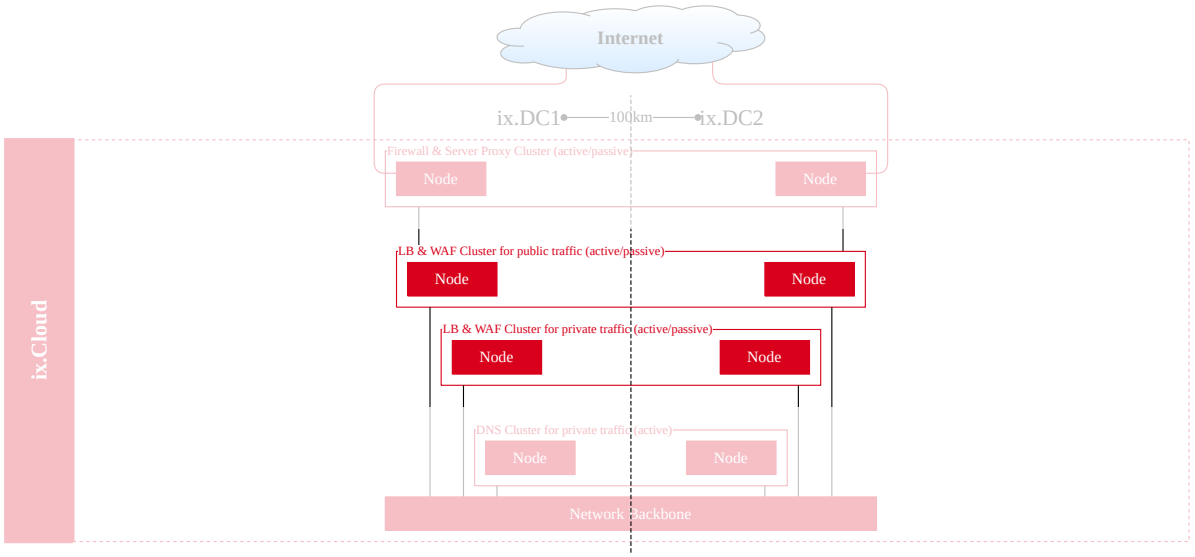


Bild: Load Balancer Service Architektur

Service Umfang

Tabelle: Load Balancer Service Umfang

Leistungsmerkmal	Layer 4	Layer 7
Initiales Setup	☐	☐
IT Grundschutz	■	■
Service Management	■	■
Bandbreite (5 MBit/s)	■	■
Service IP-Adresse	■	■
Service FQDN	-	■
Protokolle/Ports	■	■
Load Balancing	■	■
Persistence	■	■
X-Forwarded-For	■	■

Default DDoS Profile	■	■
Health Monitoring	■	■
Error Page	-	■
Maintenance Page	-	■
SSL Offloading/Bridging	-	■
Host Header Forwarding/Rewriting/Redirecting	-	■

IT Grundschutz

Patch Management

Die Loadbalancer-Infrastruktur wird mindestens halbjährlich aktualisiert, es sei denn, es treten kritische Sicherheitslücken auf, welche ein sofortiges Upgrade erfordern.

Malware Schutz

Der Malware-Schutz basiert auf gehärteten Appliances die beim booten auf ihre Integrität geprüft werden. Die Infrastruktur der Load Balancer nutzt Secure Boot und Image Signing, um sicherzustellen, dass nur signierte und vertrauenswürdige Softwarekomponenten ausgeführt werden. Die Load Balancer unterstützten RASP-Funktionalitäten (Runtime Application Self-Protection), die Anwendungen während der Laufzeit überwachen und schützen.

Service Optionen

Durch die in diesem Kapitel aufgeführten Optionen, kann ein Load Balancer auf unterschiedliche Weise konfiguriert werden.

Initiales Setup

Der Aufwand für die Einrichtung eines Load Balancers ist stark abhängig von den gewünschten individuellen Anforderungen des Kunden. Daher wird das initiale Setup eines Load Balancers nach Aufwand verrechnet.

Service Management

Im Service Management ist die Aktualisierung der verwendeten Softwarekomponenten und Security Patterns, das Ressourcenmanagement und das Backup der Infrastruktur inbegriffen. Das Zertifikats-Lifecycle Management (Erstellung/Beantragung, Integration, Austausch/Erneuerung von Zertifikaten) wird separat nach Aufwand verrechnet.

Bandbreite

Die Bandbreite (Datendurchsatz) ist pro Service individuell konfigurierbar. Im Basispreis ist eine Bandbreite von 5 Megabit per Second (MBit/s) inkludiert. In Schritten von 5 MBit/s kann der Service auf maximal 40 MBit/s gemäss separater Preisliste skaliert und den Anforderungen gerecht bestellt werden (siehe Tabelle unten). Die Verrechnung erfolgt nach Anzahl bestellter 5 Mbit/s Einheiten.

Wenn mehr Daten über den Load Balancer transportiert werden als die bestellte Bandbreite es erlaubt, werden Paketverluste (Paket-Drops) generiert. Wenn Paketverluste festgestellt werden, kann eine Erhöhung der Bandbreite bestellt/beauftragt werden. Bei einem Layer 4 Load Balancer kann die Erhöhung der Bandbreite direkt im Portal vorgenommen werden. Bei einem Layer 7 Load Balancer muss die Erhöhung der Bandbreite via Load Balancer Service Request beauftragt werden.

Tabelle: Load Balancer Bandbreiten

Bankdbreite	Layer 4	Layer 7
5 MBit/s	■	■
10 MBit/s	□	□
15 MBit/s	□	□
20 MBit/s	□	□
25 MBit/s	□	□
30 MBit/s	□	□
35 MBit/s	□	□
40 MBit/s	□	□

Service IP-Adresse

Pro Service kann eine IP-Adresse hinterlegt werden. Handelt es sich um eine private IP-Adresse ist diese kostenlos. Bei einer öffentlichen IP-Adresse fallen zusätzliche Kosten gemäss Preisliste an. Private IP-Adressen werden im Internet nicht geroutet und sind somit nur innerhalb eines lokalen Netzwerks verwendbar. Öffentliche IP-Adressen werden im Internet geroutet.

Service FQDN

Auf eine Layer 7 Service IP-Adresse (VIP) kann eine oder mehrere URLs verwiesen (DNS-Eintrag) werden. Ein DNS-Eintrag für die jeweilige URL ist Voraussetzung für die End-to-End (Client-Server) Kommunikation.

Protokolle/Ports

Wenn bei der Bestellung nichts anders angegeben, werden bei Layer 4 die Standard Ports 80/443 und bei Layer 7 das Protokoll HTTPS für den Serviceaufbau verwendet.

Die folgende Tabelle zeigt die möglichen Protokolle und Ports pro Service und Layer an.

Tabelle: Load Balancer Protokolle/Ports

Protokoll/Port	**Layer 4**	**Layer 7**
TCP (alle möglichen Ports)	■	□
HTTP	-	□
HTTPS	-	■

Load Balancing

Standardmässig ist None (Round-Robin) aktiviert. Die Option Load Balancing dient der Lastverteilung mit dem Ziel die Endsysteme gleichermassen zu belasten.

Tabelle: Load Balancer Load Balancing Optionen

Load Balancing Option	**Layer 4**	**Layer 7**
None (Round Robin) Jede neue Anfrage wird an einen Server im Pool gesendet, anschliessen top-down von neuem.	■	■
Least Connection Verbindungen werden jeweils an den Server gesendet, welcher aktuell am wenigsten Verbindungen offen hat.	□	□
Least Load Verbindungen werden jeweils an den Server gesendet, welcher aktuell am wenigsten ausgelastet ist.	□	□
Fastest Response Verbindungen werden jeweils an den Server gesendet, welcher am schnellsten antwortet.	□	□

Fewest Servers Per Algorithmus wird berechnet welche Anzahl von Servern für die Bewältigung der Anfrage notwendig ist. Es werden somit nur dem ersten Server im Pool Anfragen gesendet, sobald dieser die Kapazitätsgrenze erreicht hat wird top down der Traffic an den jeweils Nächsten weitergereicht.	☐	☐

Persistence

Standardmässig ist keine "Persistence" konfiguriert. Durch Verwendung der Option Persistence, wird die Sitzung an ein bestimmtes Endsystem gebunden. So wird sichergestellt, dass die Anfragen während einer Sitzung immer vom selben Endsystem verarbeitet werden.

Tabelle: Load Balancer Persistence Optionen

Persistence Option	Layer 4	Layer 7
Client IP Die Client-IP wird als Kennung verwendet und dem Server zugeordnet.	☐	☐
TLS Die Informationen sind in die SSL/TLS-Ticket-ID des Clients eingebettet.	-	☐
APP Cookie Liest vorhandene Server-Cookies oder eingebettete URI-Daten wie JSessionID.	-	☐
HTTP Cookie Fügt ein Cookie in die HTTP-Anwort(en) ein.	-	☐
Custom HTTP Header Der Kunde kann benutzerdefinierte Vorgaben zur Zuordnung von Header-Werten zu bestimmten Servern erstellen.	-	☐

X-Forwarded-For

Mit dem X-Forwarded-For ist es möglich, Client IP-Adressen (original IP) mit dem Header an das Zielsystem zu übertragen. Das Zielsystem kann diese Information verwenden, um beispielsweise

aufzuzeigen, woher die Anfrage stammt oder serverseitig Black-/White-Lists aufzuschalten. Diese Option ist nur bei Load Balancer Layer 7 einsetzbar.

Default DDOS Profile

Standardmässig ist ein DDoS Profil (Build-in) aktiviert, welches auf Layer 3, 4 und Layer 7 Netzwerkattacken erkennt und verhindert.

Tabelle: Load Balancer Default DDOS Profile

Default DDOS Profil	Layer 4	Layer 7
Layer 3 SMURF, ICMP Flood, Unknown Protocol, Tear Drop, IP Fragementation	■	■
Layer 4 SYN Flood, LAND, Port Scan, X-mas Tree, Bad RST Flood, Fake Session, Bad Sequence Number, Malformed/Unexpected Flood, Zero/Small Window, Rate Limiting CPS per IP, SSL Errors, SSL Renegotiation	■	■
Layer 7 Request Idle Timeout (10'000ms), SlowPost (30'000ms), SlowLoris (30'000ms), Invalid Requests	-	■

Health Monitoring

Beim Health Monitoring sendet der Load Balancer innerhalb eines Intervalls Anfragen an das Zielsystem, für welche er jeweils eine Antwort innerhalb eines gesetzten Zeitfensters erwartet.

Werden die jeweiligen Anfragen an einem Zielsystem nicht beantwortet, so wird das Zielsystem als nicht erreichbar markiert. Folglich werden Client-Server Anfragen nicht mehr an das Zielsystem weitergereicht.

Tabelle: Load Balancer Health Monitoring Optionen

Health Monitoring Option	Layer 4	Layer 7
TCP (custom-client-request/custom-server-response) Wartet auf eine vollständige TCP Verbindung, auf einem spezifisch angefragten Port.	☐	☐

ICMP Sendet einen Ping und erwartet eine Rückmeldung vom "angepingten" Server.	-	☐
DNS (request/response) Prüft den "Name Server" ob eine korrekte Namensauflösung auf einen spezifizierten Eintrag möglich ist.	-	☐
HTTP/S (custom-client-request-header/-body, custom-server-response) Prüft den spezifizierten "Respond Code" auf deren Korrektheit.	-	☐
External Per Script-Befehl können Kundenspezifizierte Health-Checks vorgenommen werden. (wget, netcat, curl, dig, mysql-client, snmpget)	-	☐

Error Page

Standardmässig wird bei einem Layer 7 Service eine "Default Error Page" ausgegeben, welche den Client über den Verbindungsfehler in Kenntnis setzt. Entspricht das Layout oder der Inhalt der Page nicht den Bedürfnissen, kann eine "Custom Error Page" erstellt und der Inventx zur Einbindung zur Verfügung gestellt werden.

Maintenance Page

Soll eine Maintenance Page für den Wartungsmodus geschalten werden, kann dies Anhand eines Auftrages an die Inventx, oder durch den Kunden selbst veranlasst werden. Im Zweiten fall, muss ein Skriptbasierter Lösungsanasatz gefahren werden, hierfür bitten wir Sie Ihren konkreten UseCase bekanntzugeben.

SSL Offloading/Bridging

Wenn ein Layer 7 Service bestellt wird, wird standardmässig das SSL-Offloading aktiviert. Diese Option ermöglich, dass der Load Balancer der verschlüsselte Traffic aufbrechen kann um z.B. Netzwerkangriffe erkennen zu können und anhand WAF-Richtlinien zu verhindern.

Beim SSL Offloading wird der Traffic entschlüsselt:

- Client zum Load Balancer = verschlüsselt
- Load Balancer zum Ziel = unverschlüsselt

Beim SSL Bridging hingegen wird der Traffic entschlüsselt und wieder verschlüsselt:

- Client zum Load Balancer = verschlüsselt
- Load Balancer zum Ziel = verschlüsselt

Für die Zertifikatsausstellung/-einbindung wird eine bestehende PKI-Infrastruktur in der Kundenumgebung vorausgesetzt. Falls Diese nicht zur Verfügung steht, müssen seitens Kunden die benötigten Zertifikate der Inventx zur Verfügung gestellt werden.

Das Lifecycle Management der Zertifikate ist nicht Bestandteil dieses Services und muss durch den Kunde sichergestellt werden.

Host Header Forwarding/Rewriting/Redirecting

Sofern ein Layer 7 Service bestellt wird, besteht die Möglichkeit anhand Host-Header Informationen forwarder, rewrites, redirects vorzunehmen. Zudem kann auf Wunsch eine Umleitung von HTTP auf HTTPS erfolgen.

Web Application Firewall

Mit der von Inventx betriebenen Web Application Firewall (WAF) wird die Serviceanbindung über den Load Balancer dahingehend unterstützt, dass eingehender HTTP-Verkehr auf Sicherheitslücken bzw. unbefugte Datenübertragung überprüft wird, bevor dieser den Anwendungsserver erreicht. Somit dient der WAF-Service als Durchsetzungspunkt für Sicherheitsrichtlinien, welche zwischen Webanwendung und dem Client Anwendung stattfindet.

Die WAF fängt alle HTTP-Anforderungen ab und überprüft diese mithilfe des vorgängig definierten Regelsets (Sicherheitsmodells), um identifizieren zu können ob es sich hierbei um ungewollten Datenverkehr (cross-site scripting, SQL injection, ect.) handelt. Dieses Vorgehen verhindert L7-DDos/Angriffe, bei denen versucht wird die Sicherheitsanfälligkeiten in webbasierten Anwendungen auszunutzen bzw. den Service negativ zu beeinflussen.

Dieser Service ist nur im SLA Platin verfügbar und muss über den Standard Service Request "Web Application Firewall" bestellt und verwaltet werden.

Service Architektur

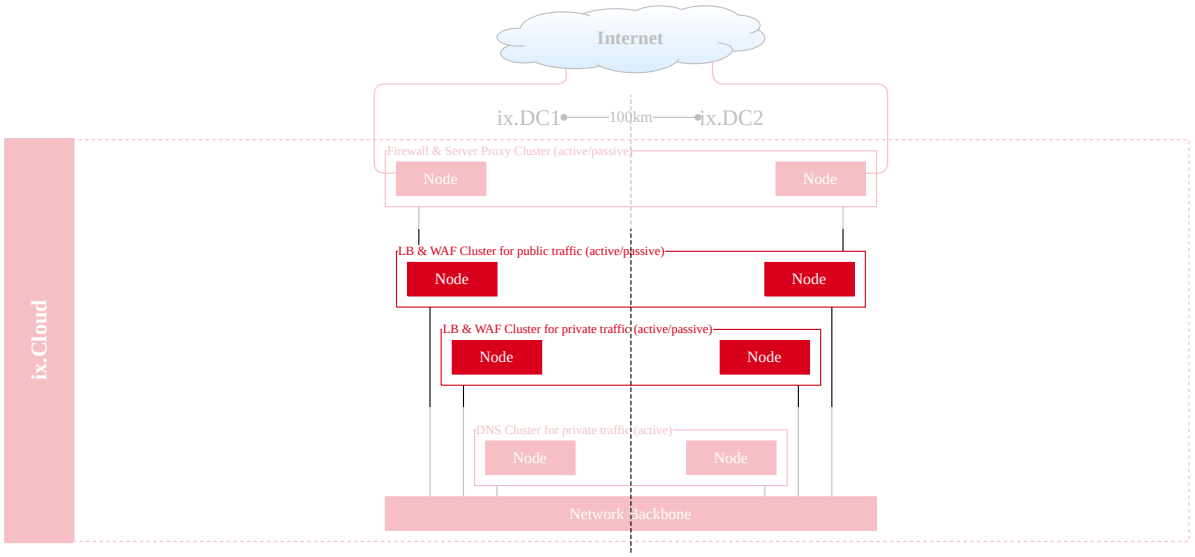


Bild: Web Application Firewall Service Architektur

Service Umfang

Tabelle: Web Application Firewall Service Umfang

Leistungsmerkmal	Platin
Initiales Setup	☐
IT Grundschutz	■
Load Balancer Layer 7	■
Service Management	■
OWASP TOP 10 Rule-Set	■
Kundenindividuelles Rule-Set	☐
Betriebsmodus Enforcement	■

IT Grundschutz

Siehe Beschreibung Kapitel Load Balancer IT Grundschutz.

Service Optionen

Beim WAF-Service kann der Kunde weitere Dienstleistungen nach Absprache beziehen.

Initiales Setup

Der Aufwand für die Einrichtung eines WAF Services ist stark abhängig von den gewünschten individuellen Anforderungen des Kunden, im speziellen bei den zu definierenden Rule-Sets. Daher wird das initiale Setup einer WAF nach Aufwand verrechnet.

Load Balancer Layer 7

Die Basis-Konfiguration für den WAF bildet ein Load Balancer Layer 7. Entsprechende Service Optionen werden beim Load Balancer in der Ausprägung Layer 7 beschrieben.

Service Management

Im Service Management ist unter anderem die Aktualisierung der verwendeten Softwarekomponenten und Security Patterns, das Ressourcenmanagement und das Backup der Infrastruktur inbegriffen.

Das WAF-Lifecycle Management (Analyse/Anpassung von Regelsätzen) wird separat nach Aufwand verrechnet.

OWASP TOP 10 Rule-Set

Als Standard Rule-Set dienen die OWASP Top 10 Schwachstellen. Das Open Web Application Security Projekt (OWASP) ist eine internationale non-profit Organisation, die sich der Sicherheit von Webanwendungen verschrieben hat. Das bekannteste Projekt nennt sich OWASP Top 10. Hierbei handelt es sich um einen Report, der die 10 kritischsten Risiken abdeckt.

Kundenindividuelles Rule-Set

Gewisse Anwendungen benötigen für den einwandfreien Betrieb eine individuelle Konfiguration des Rule-Sets. Hierfür werden beispielsweise Ausnahmen für das OWASP Rule-Set für unerwünschte Detektionen erstellt. Anpassungen am Regelwerk sind mit einem "Generic Request" zu beauftragen.

Betriebsmodus Enforcement

Der WAF-Service wird im Betriebsmodus Enforcement betrieben. Dabei wird das konfigurierte Rule-Set produktiv angewendet und die Web-Anwendungen entsprechend geschützt, gleichsam ob der WAF-Service für die Test- oder Produktionsstufe genutzt wird.

Private DNS

Der Private DNS (Domain Name System) Service ermöglicht es, Server und Client-Systemen eine autoritative/reverse Auflösung von IP-Adresse zu DNS-Namen und vice versa. Die Zugriffe eines Kunden werden in einer privaten View (Zone) des globalen DNS-Systems abgebildet, die von Inventx gepflegt und betrieben wird.

Der Private DNS Service steht ausschliesslich im SLA Platin zur Verfügung und muss via "Generic Request" bestellt werden.

Service Architektur

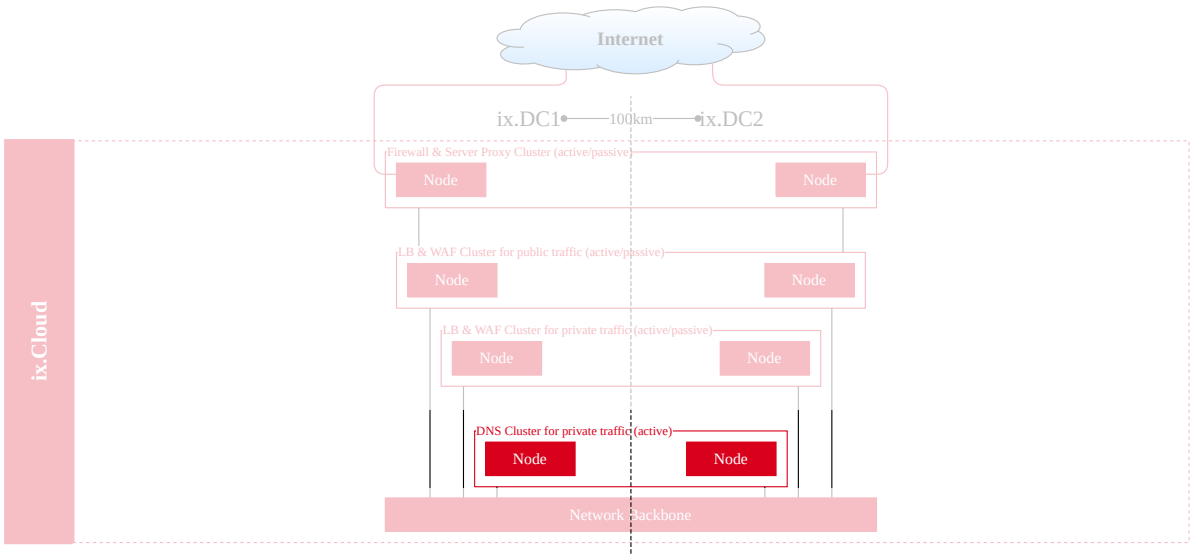


Bild: Private DNS Service Architektur

Service Umfang

Tabelle: Private DNS Service Umfang

Leistungsmerkmal	Platin
Initiales Setup	□
Authoritive Zone	■
Weiterleitung	■

Service Optionen

Durch die in diesem Kapitel aufgeführten Leistungselemente, kann der DNS Service auf unterschiedliche Weise individualisiert betrieben werden.

Initiales Setup

Die Umsetzung der initialen Konfiguration des Private DNS Service wird im Rahmen eines Projekts verrechnet. Dabei wird die Konfiguration in Zusammenarbeit mit dem Kunden spezifiziert und anschliessend implementiert.

Authoritive Zone

Eine autoritative Zone ist eine Zone, für die der lokale (primäre oder sekundäre) DNS-Server auf seine eigenen Daten verweist, wenn er auf Abfragen antwortet. Der lokale DNS-Server ist für die Daten in dieser Zone verantwortlich und antwortet auf Abfragen, ohne auf einen anderen Server zu verweisen. Es gibt zwei Zonenarten:

- **Forward-Mapping**: Eine Forward-Mapping-Zone ist ein Bereich des Domain-Namensraums, für den ein oder mehrere Nameserver die Verantwortung haben, auf Anfragen von Name-zu-IP-Adresse zu antworten.
- **Reverse-Mapping**: Eine Reverse-Mapping-Zone ist ein Bereich des Netzwerkraums, für den ein oder mehrere Namensserver für die Beantwortung der Anfragen von IP-Adresse-zu-Name zuständig sind.

Folgende Record-Typen sind pro Zonenart möglich:

Tabelle: Private DNS Record Types

Record Typ	forward-mapping	reverse-mapping
Host Record	■	-
A Record	■	-
CNAME Record	■	-
Alias Record	■	■
MX Record	■	-
NS Record	■	-
PTR Record	■	■
SRV Record	■	-
TXT Record	■	-

Weiterleitung

Bei einer hybriden Architektur kann durch die DNS-Weiterleitung die ix.Cloud mit einer OnPremise-Umgebung des Kunden logisch verbunden werden. Durch diese Option können Kunden bereits vorhandene, lokale DNS-Server als autoritativ weiterverwenden.

Secure Mail-Relay

Mit dem von Inventx betriebenen Secure Mail-Relay Service können Kunden E-Mail (SMTP Syntax) aus der ix.Cloud sicher ins Internet versenden, wobei als Absender der Nachricht eine Inventx-Adresse hinterlegt wird.

Service Architektur

N/A

Service Umfang

Tabelle: Secure Mail-Relay Service Umfang

Leistungsmerkmal	Platin
Initiales Setup	□
Quelle und Bestimmungsort	■
Malware-Schutz	■
Content-Filtering	■
Session Handling	■
Adressierung	■
Versand über Internet	■

Service Optionen

Der Secure Mail-Relay Service der ix.Cloud weist die folgenden Merkmale aus:

Initiales Setup

Die Inbetriebnahme des Mail-Relay Service wird im Rahmen eines Projekts vollzogen. Dabei wird der Service in Zusammenarbeit mit dem Kunden spezifiziert und anschliessend integriert. Bestellungen und sämtliche Änderungen sind mit einem "Generic Request" zu beauftragen.

Quelle und Bestimmungsort

Der Mail-Relay Service ist nur innerhalb der ix.Cloud erreichbar, denn sämtliche Nachrichten werden auf Basis des IP-Ranges und der Absender-Adresse entgegengenommen. Als Empfänger können alle E-Mail-Adressen angegeben werden.

Malware-Schutz

Nach Entgegennahme der Nachricht findet eine Malware-Prüfung statt. Bei einem positiven Befund, wird die Nachricht abgelehnt (rejected). Zudem ist ein Antivirus-Outbreak-Filter von 20 Minuten hinterlegt, damit Malware zeitnah identifiziert werden kann.

Content-Filtering

Aus Sicherheitsgründen werden sämtliche Nachrichten gefiltert. Dateien vom Typ Video, Audio, Archiv sowie Executables, Scipts und verschlüsselte Files werden gefiltert und mit einem Error-TXT-File ersetzt. Um unerlaubten Datenabfluss zu verhindern, gelten folgende Regeln:

- Anzahl Attachments pro Nachricht: Maximal 5
- Grösse der Nachricht: Maximal 10 MB
- Kompressionslevel der Beilage: Maximal 12

Session-Handling

Es sind maximal 1'200 Nachrichten pro 30 Minuten und pro SMTP-Verbindung maximal drei parallele ELHO-Aufträge möglich. Bei Überschreitung dieser Werte, wird automatisch eine Drosselung (Throttling) ausgeführt.

Adressierung

Vor dem Versand an die Destination wird der Absender mit einer generischen Inventx-Adresse umgeschrieben (noreply@ixcloud.ch).

Versand über Internet

Der Versand der Nachrichten findet stets über das Internet statt. Ein verschlüsselter Versand (TLS) wird dringend empfohlen (preferred), jedoch nicht erzwungen.

Hosted Software-Appliance

Für den Betrieb von Software-Appliances können Virtuelle Server auf Basis der ESX-Virtualisierung von VMware bezogen werden, für den Fall, dass der Software-Hersteller keinen Support für Microsoft Hyper-V anbietet. Solche VM werden ausschliesslich im SLA Rhodium bereitgestellt und können weder über das ix.Cloud Portal noch über die ix.Cloud API verwaltet werden.

Service Architektur

Siehe Virtual Machine Darstellung SLA Rhodium.

Service Umfang

Virtuelle Server auf Basis von VMware können in den Standard Hardware-Profilen gemäss Virtual Machine bestellt werden. Solche VM werden ohne Betriebssystem (OS) ausgeliefert. Der Kunde ist für

Lizenzierung, Betrieb und Wartung des OS selber verantwortlich (vgl. "Customer Owned OS" unter Virtual Machine). Die Off-Funktionalität steht nicht zur Verfügung.

Solche VM müssen via "Standard Service Request" bestellt werden - Mutationen und Dekommissionierungen via "Generic Request". Der Image-Import erfolgt gemäss Beschreibung für "Customer Owned OS" unter Virtual Machine.

Service Optionen

Keine Optionen verfügbar.

Storage Services

Die ix.Cloud "Storage Services" bieten die Möglichkeit, Daten in den hochverfügbaren Rechenzentren der Inventx bereitzustellen oder ein lokales Rechenzentrum mit zusätzlichen Speicherkapazitäten zu erweitern.

Tabelle: Storage Services

Service Name	Service Kurzbeschreibung
File Storage	Datenablage für Office Dokumente, Desktop Profile sowie WORM Archive.
Object Storage	Skalierbarer Objektspeicher für grosse Mengen an unstrukturierten Daten

File Storage

Der File Storage Service bietet verwaltete Dateifreigaben, auf die über branchenübliche Protokolle (NFS oder CIFS/SMB) zugegriffen werden kann. Die Daten auf dem File Storage werden permanent zwischen den Inventx Rechenzentren in der Schweiz synchronisiert.

:::info

Bestellungen und sämtliche Änderungen beim File Storage Service sind mit einem "Generic Request" zu beauftragen.

:::

Service Architektur

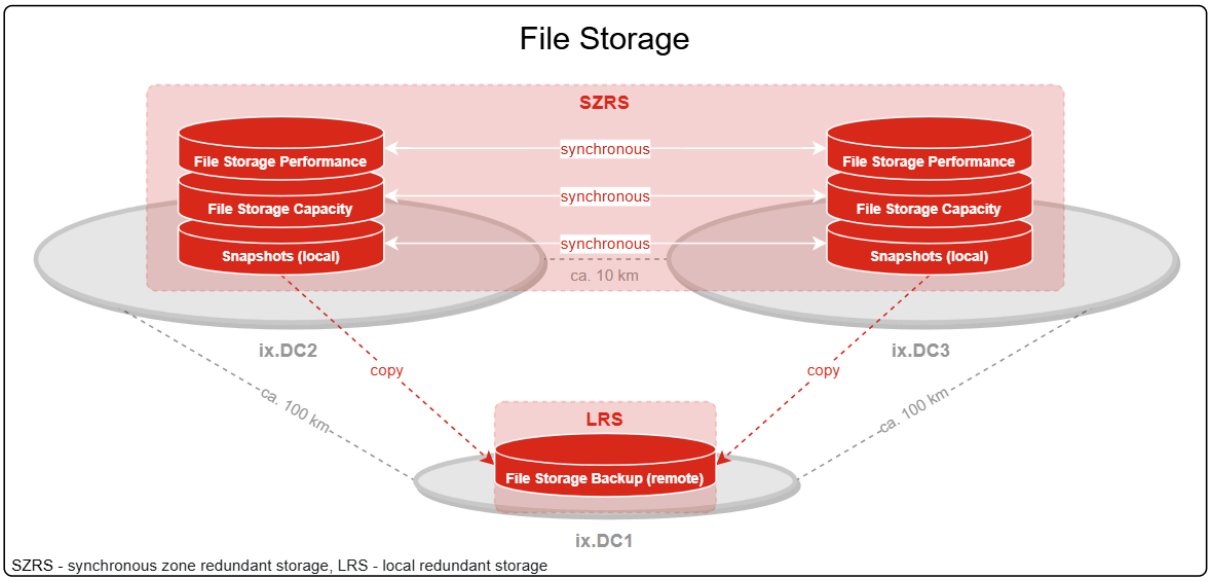


Bild: File Storage Service Architektur

Service Umfang

Tabelle: File Storage Service Umfang

Leistungsmerkmale	
Redundanz und Replikation	■
XTS-AES 256-Bit Verschlüsselung	■
AutoGrow & AutoShrink	■
Zugriffsprotokolle NFS / CIFS (SMB)	■
Datensicherung	■
Datenwiederherstellung	■
Individualisierbares Tiering	■
Antivirus-Schutz	□
Ransomware-Schutz	□
WORM (write-once-read-many)	□

Service Optionen

Der File Storage Service weist die nachfolgend erläuterten Optionen aus.

Redundanz und Replikation

Um eine möglichst hohe Verfügbarkeit der Daten zu erreichen, werden die primären Daten und die Sicherungen (Snapshots) permanent über zwei Rechenzentren synchron repliziert (Zonenredundanz). Und für den Katastrophen-Fall, wird zusätzlich eine Backupkopie in ein drittes Rechenzentrum erstellt.

XTS-AES 256-Bit Verschlüsselung

Die Daten auf dem File Storage werden mit XTS-AES 256-Bit verschlüsselt (Encryption@Rest). Dieser Verschlüsselungs-Algorithmus, ist eine der meist genutzten und zugleich sichersten Methode, um Daten auf einem Storage zu verschlüsseln.

AutoGrow & AutoShrink

Die Vergrösserung und Verkleinerung der Volumes erfolgt dynamisch und die Verrechnung findet auf Basis des täglich erhobenen Datenverbrauchs statt.

:::caution

Vergrösserungen von mehr als 20% der Gesamtkapazität gemäss Consumption Report sind zwei Monate im Voraus anzumelden.

:::

Zugriffsprotokolle NFS / CIFS (SMB)

Der Zugriff auf die Ordnerfreigabe beziehungsweise auf die Daten erfolgt über das NFS- oder CIFS-Protokoll.

Beim NFS-Protokoll wird der Zugriff anhand der Client IP-Adresse oder DNS-Name eingeschränkt und beim CIFS-Protokoll via Active Directory des Kunden freigegeben und verwaltet.

:::caution

Ein Multiprotokoll-Zugriff (NFS und CIFS) auf eine Ordnerfreigabe wird nicht unterstützt.

:::

Datensicherung

Die Sicherung der primären Daten wird via Snapshot Technologie in regelmässigen Abständen (stündlich und täglich) durchgeführt und über zwei Rechenzentren synchron repliziert. Der tägliche Snapshot wird zusätzlich in ein drittes Rechenzentrum kopiert.

Mit den folgenden vier Backup-Profilen kann die Sicherung der Daten bedürfnisgerecht eingerichtet werden.

- 40d Backup

- 200d Backup (Standard)
- 400d Backup
- No Backup

:::caution

Beim Backup-Profile "No Backup" wird auf expliziten Wunsch keine Sicherung der primären Daten erstellt. Der Kunde verzichtet somit auf die Möglichkeit der Datenwiederherstellung.

:::

Die Aufbewahrungsdauer bei den Backup-Profile ist gemäss unten stehenden Angaben eingerichtet. Sofern beim Backup die Option "40d Backup", "200d Backup" oder "400d Backup" gewählt wurden, erfolgt eine regelmässige Erstellung von unveränderbaren (immutable) SnapShots der Primärdaten. Daraus resultiert ein bedingter Schutz gegen Ransomware, da man auf vorherige Sicherungen zugreifen kann.

Tabelle: File Storage Aufbewahrungsdauer "40d Backup"

Aufbewahrungsdauer "40d Backup"		**Standort**	
		local (snapshot)	**remote**
Intervall	**stündlich**	2 Tage	-
	täglich	20 Tage	40 Tage (mit WORM 20 Tage)

Tabelle: File Storage Aufbewahrungsdauer "200d Backup"

Aufbewahrungsdauer "200d Backup"		**Standort**	
		local (snapshot)	**remote**
Intervall	**stündlich**	10 Tage	-
	täglich	40 Tage	200 Tage (mit WORM 40 Tage)

Tabelle: File Storage Aufbewahrungsdauer "400d Backup"

Aufbewahrungsdauer "400d Backup"		**Standort**	
		local (snapshot)	**remote**
Intervall	**stündlich**	20 Tage	-

	täglich	80 Tage	400 Tage (mit WORM 80 Tage)

Datenwiederherstellung

Die Wiederherstellung der primären Daten erfolgt im Self-Service über die Funktion "Vorgägerversionen" im Windows Datei-Explorer. Eine Wiederherstellung von einem Remote-Backup muss via "Generic Request" beauftragt werden.

:::caution

Wird beim Backup-Profile die Option "No Backup" gewählt (siehe Datensicherung), ist die Wiederherstellung von primären Daten nicht möglich.

:::

Individualisierbares Tiering

Durch das individualisierbare Tiering ist es möglich, inaktive Daten auf einen kostengünstigeren Storage-Tier auszulagern. Im File Storage Service stehen folgende zwei Storage-Tiers zur Verfügung:

Tabelle: File Storage Tiers

Storage Tier	Durchsatz / Volume	IOPs / Volume
Performance	max. 200 MB/s	max. 5'000
Capacity	max. 50 MB/s	max. 1'000

:::info

Die oben erwähnten KPI's "Durchsatz" und "IOPs" sind als Richtwerte zu betrachten und grundsätzlich von der Filegrösse und dem verwendeten Protokoll abhängig. Beim Performance-Tier sind Antwortzeiten von durchschnittlich <5ms zu erwarten (gemessen über 4 Stunden am Storage Controller).

:::

Alle Daten verbleiben zuerst auf dem Performance-Tier und können dann mittels "Auto Tiering" regelbasiert und automatisch auf das Capacity-Tier ausgelagert werden. Folgende Profile stehen zur Auswahl:

- No Tiering (die Daten verbleiben im Performance-Tier)
- Auto Tiering (inaktive Daten werden nach 40 Tagen auf das Capacity-Tier verschoben)

Antivirus-Schutz

Die CIFS (SMB) Dateifreigaben können optional mit einem Antivirus Scanner überprüft werden. Bekannte Dateiendungen von Ransomware werden zusätzlich gesperrt.

:::note

Für die Option Antivirus-Schutz werden im Netzwerk des Kunden zwei VMs mit einer Antivirus-Software installiert. Je nach Last auf die Dateifreigaben kann es sein, dass mehr als zwei VMs notwendig sind.

:::

Ransomware-Schutz

Als Option kann eine KI-basierte Anomalie-Erkennung und Pattern Recognition mit Notfall-SnapShot Erzeugung ausgewählt werden. Dank dieser Option kann eine frühzeitige Erkennung von Ransomware sichergestellt werden. Vgl. beiliegende Grafik zur 2-Layer Abwehr.

Im Funktionsumfang enthalten ist auch die Möglichkeit einer konfigurierbaren User-Sperrung, die Möglichkeit der differenziellen Wiederherstellung sowie weitere Analyse Optionen.

Zusätzlich lassen sich individuelle Patterns und Response Policies definieren. Die Konfiguration von Honeypots ist ebenfalls verfügbar.

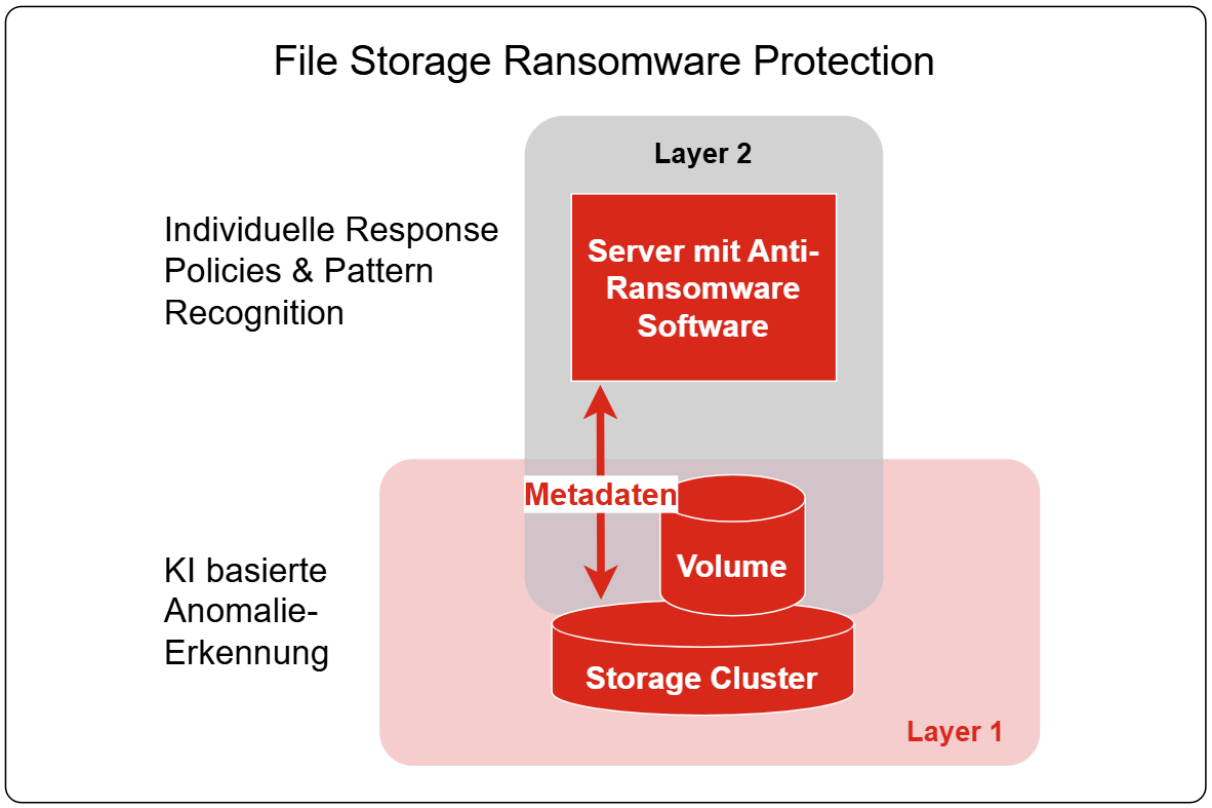


Bild: File Storage Ransomware Protection

:::note Für die Option Ransomware-Schutz wird im Netzwerk des Kunden eine VM mit der entsprechenden Software installiert. Je nach Last auf die Dateifreigaben kann es sein, dass mehr als

eine VM notwendig ist. Die Option zum Ransomware-Schutz wird in Zusammenarbeit mit dem ix.CRC für den Kunden umgesetzt. Technisch auch bei WORM Volumes möglich. Da die WORM Volumes meistens im Zusammenhang mit Archive-Applikationen verwendet werden, ist dort eine vertiefte Analyse der Aktionen und die Auswirkungen davon abzuklären. Auf Request kann dies zusammen mit dem Kunden umgesetzt werden. :::

:::caution

Diese Option ist nur bei Non-WORM Volumes einsetzbar, da bei WORM die Daten bereits unveränderbar abgespeichert sind.

:::

WORM (write-once-read-many)

Um das Löschen, Ändern und Umbenennen von Dateien zu verhindern, kann bei Bedarf die Option WORM gewählt werden.

:::caution

Vor einem initialen Setup müssen die Abhängigkeiten und Anforderungen einer Archiv-Lösung geprüft werden.

:::

Object Storage

Der Object Storage der ix.Cloud ist ein S3-kompatibler, skalierbarer und georedundanter Datenspeicher. Die Daten werden dabei in sogenannten Vaults gruppiert. So können Speicher-Objekte effizient abgerufen werden, ohne den physischen Speicherort eines Objektes zu kennen - komplexe Verzeichnisstrukturen entfallen. Beim Upload der Daten werden die Daten mittels dem Erasure Code Verfahren automatisch in einzelne Stücke zerlegt, mit redundanten Informationen erweitert und an physikalisch unterschiedlichen Orten im Speichersystem abgelegt. Damit können korrumpierte oder verloren gegangene Daten mit Hilfe der noch an anderer Stelle vorhandenen Informationen rekonstruieren werden.

Der Object Storage ist ideal, um grosse Mengen an unstrukturierten Daten zu speichern, wodurch er vielfältig einsetzbar ist: z.B. Ablage von Files, Medien, Webinhalte, Datenarchivierung, Backup und Restore.

Service Architektur

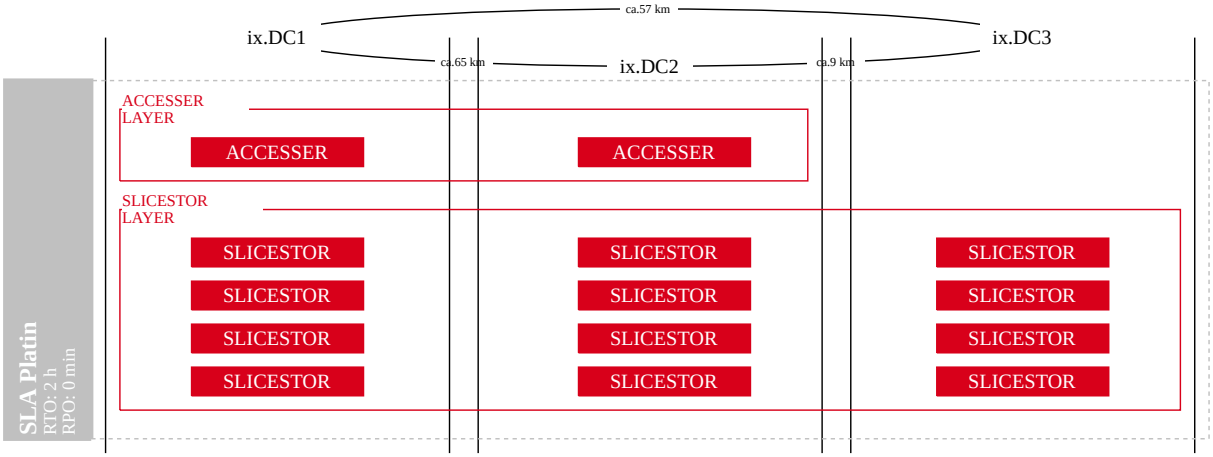


Bild: Object Storage Service Architektur

Service Umfang

Tabelle: Object Storage Service Umfang

Leistungsmerkmal	
Initiales Setup	☐
Zugriff und Authentifizierung	■
Verschlüsselung	■
Storage Management	■
Malware-Schutz	☐

Service Optionen

Bestellungen und sämtliche Änderungen sind mit einem "Generic Request" zu beauftragen.

Zugriff und Authentifizierung

Die logische Trennung und Administrations-Integrität findet über einen individuellen Vault statt. Der Zugriff erfolgt nach initialer Aufschaltung via S3-API über HTTPS mittels User-Name (Access Key ID) und Passwort (Secret Access Key).

Verschlüsselung

Die Datenübertragung (Upload und Download) findet verschlüsselt mit TLS (ehemals SSL) statt. Auf dem Storage-System werden alle Daten mittels Secure-Slice-Algorithmus (256 Bit) abgelegt, wobei die Storage-Applikation die Datenverschlüsselung beim Speichervorgang umsetzt.

Storage Management

Das Storage Management des ix.Cloud Object Storage basiert auf AutoGrow resp. AutoShrink. Folglich wird keine explizite Storage-Grösse pro Kunde reserviert. Optional kann pro Kunde beim Initial Setup oder nachträglich via "Generic Request" jedoch eine maximale Storage-Grösse pro Vault konfiguriert werden, wobei das Capacity Management solcher Vaults der Kunde selbst verantwortet. Die Verrechnung findet jeweils monatlich auf Basis des täglich erhobenen Datenverbrauchs statt.

Compute Services

Mit den "Compute Services" können Kunden auf Basis unterschiedlicher Compute-Technologien und Service-Modellen benötigte Compute Leistungen on demand in den hochverfügbaren Rechenzentren der Inventx beziehen und entlang der geforderten SLA Anforderungen ausrichten.

Compute Services werden dazu verwendet, um Workload zu deployen, zu hosten und zu verwalten. In diesem Abschnitt werden die unterschiedlichen Services und deren Optionen in Bezug auf Compute-Services der ix.Cloud beschrieben.

Tabelle: Compute Services

Service Name	Service Kurzbeschreibung
Virtual Machine	In der ix.Cloud gehostete virtuelle Maschine (VM), optional auch mit Management des Gast-Betriebssystems via "Plus-Services"

Virtual Machine

Durch den ix.Cloud Service "Virtual Machine" kann innerhalb von Minuten ein virtueller Computer (VM) in der geografischen Region bereitgestellt werden, die für den geforderten Workload geeignet ist.

Service Architektur

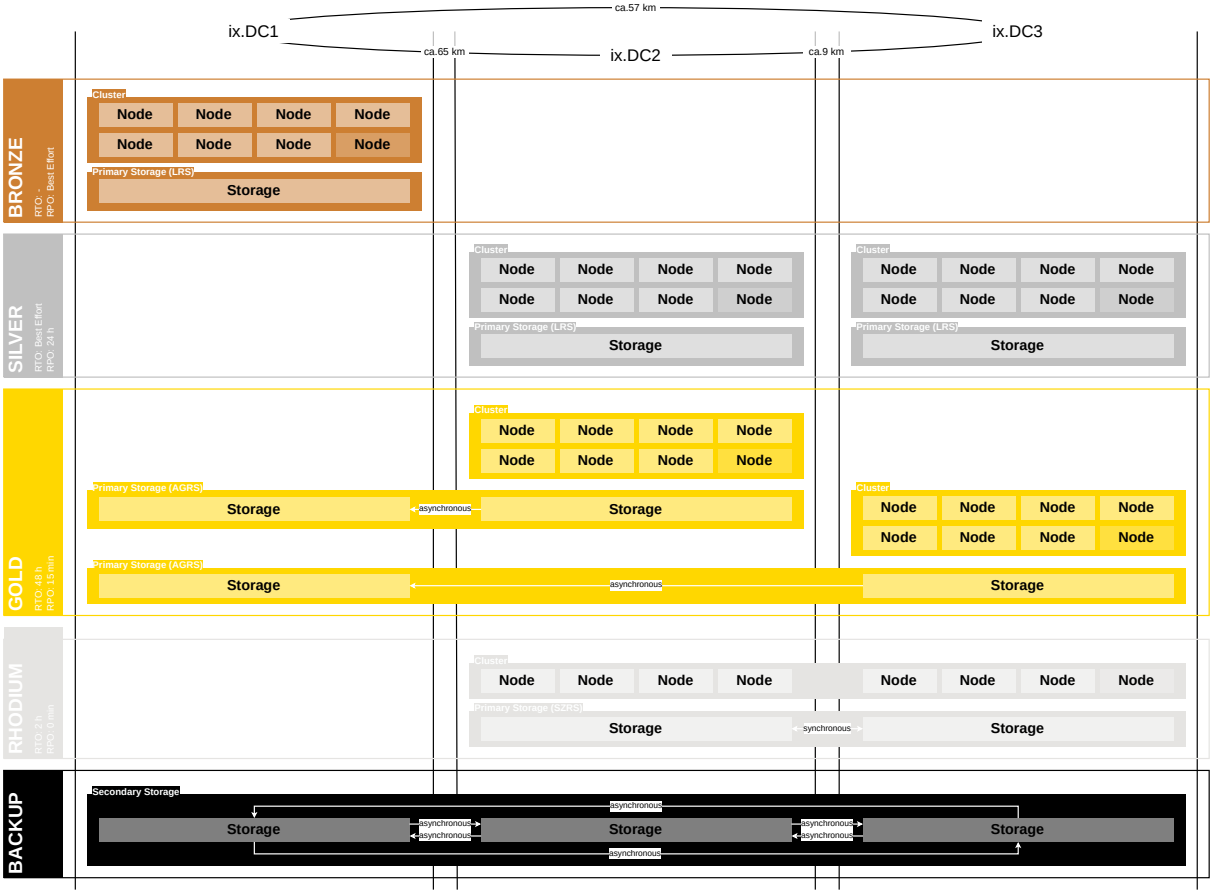


Bild: Virtual Machine Service Architektur

Service Umfang

Tabelle: Virtual Machine Service Umfang

Leistungsmerkmal	Leistungsbeschreibung
Definition, Konfiguration und Bereitstellung von OS-Instanzen (VM mit OS-Image)	• Automatische Provisionierung eines Servers ab Image (siehe Service Optionen) • Dekommissionierung eines Servers • Automatisiertes Deploying von Storage inklusive Wahl der Storage-Klasse • Wechsel des SLA sowie Wechsel der Location via "Standard Service Request"
Management und Überwachung der Computing Systeme und der Virtualisierungskomponenten	• Überwachung und Reporting über das Webportal (die Überwachung enthält pro VM eine Konfigurations- und Kapazitätsübersicht sowie eine Liste der angehängten Ressourcen)

	• Administrative Rechte auf VM Ebene (Start/Stop/Reconfigure) • Administrative Rechte im Gast OS mit lokalen Accounts • Authentisierung an der Kunden-AD via NTLM oder Kerberos • Authentisierung via SAML (z.B. Kunden-AD) • Zugriff auf die Remote Console der VM, sowie je nach ausgewähltem Betriebssystem Zugriff via Remote Desktop oder SSH-Protokoll • Betrieb OS durch Kunde
Management und Überwachung der Storage-Subsysteme und der Storage-Netzwerke	• Änderung der Storage-Klasse • Hinzufügen oder Entfernen von zusätzlichen Daten-Disks
Management und Überwachung der Backup-Systeme	• Sicherung des virtuellen Servers monolithisch auf VM Ebene (Retention 14/40/90 Tage, täglich) • "No Backup" Option • Wiederherstellung VM (monolithisch auf VM Ebene) basierend auf SLA • Verschlüsselung der Backups mit separatem Key pro Kunde
Konfiguration und Bereitstellung von virtuellen Netzwerken	• Konfiguration und Nutzung virtueller Netzwerke (SDN) • Bereitstellung und Betrieb virtueller Netzwerke (VLAN). Beschränkung auf drei VLANs pro Subscription • Zusätzliche VLANs werden nach Aufwand verrechnet
Weitere Leistungen	• Sicherstellung des Herstellersupportes sämtlicher Infrastruktur-Komponenten • Sicherstellen des Capacity Managements aller Infrastruktur-Komponenten (e.g. ist genügend Server-Hardware, Storage- Hardware oder Backup-hardware vorhanden?) • OS-Lizenzen sowie notwendige Lizenzen der Infrastrukturkomponenten enthalten (z.B.

	Backup, OS-Monitoring) • Automatisiertes Reporting • Automatisiertes Billing • Selbständige Verwaltung und Einsicht via Online Portal • ON / OFF Möglichkeit vorhanden

IT-Grundschutz

In diesem Abschnitt werden die allgemeinen Definitionen des IT-Grundschutz für den Compute Service (auf Stufe Host) beschrieben.

Patch Management

- Die Systeme werden im Zyklus von 4 Wochen entlang unseres Wave Konzeptes gepatcht.
- Exclusions sind im Normalfall nicht vorgesehen, da es sich um kritische Sicherheitsupdates handelt. Eine Exclusion käme nur im Falle eines fehlerhaften Patches in Betracht und kann entsprechend konfiguriert werden.
- Beim Emergency Patching wird eine identifizierte kritische Schwachstelle umgehend gepatcht

Logging

- Die Systeme werden durch unser Monitoring protokolliert, einschliesslich Event-Logs, Login's und Aufzeichnungen von Administratorenkonten.
- System Logs werden mindestens 9 Monate aufbewahrt.
- Eine Überwachung stellt sicher, dass die Log's fortlaufend aufgezeichnet werden. Im Fehlerfalle wird automatisch ein Ticket an den Betrieb gesendet.

Malware Schutz

- Ein stehts aktueller Virenschutz ist die Basis unseres Malwareschutzes.
- Updates erfolgen monatlich zusammen mit dem Patchen. Bei kritischen Schwachstellen wird ein aussergewöhnliches Update durchgeführt.

Hardening

- Wir lehnen uns an dem CIS-Standard an, welcher im ATSB abgenommen wurde.
- Alle empfohlenen Sicherheitseinstellungen werden umgesetzt, solange dadurch keine funktionellen Einschränkungen entstehen.
- Die CIS-Empfehlungen werden in regelmässigen Abständen überprüft und bei neuen Software-Release-Zyklen berücksichtigt.

Configuration Management

- Die Erfassung der Systeme (Assets) erfolgt in unserer zentralen CMDB

- Konfigurationen werden im BHB dokumentiert und sind jeweils im Golden-Image des Deployments implementiert

Service Optionen

Eine VM kann via ix.Cloud Portal/API und mittels Service Requests durch eine Vielzahl von Konfigurationen und Optionen auf aktuelle Bedürfnisse angepasst werden.

Hardware-Profile

Bei den Hardware-Profilen wird zwischen zwei Typen (Standard und Highclock) unterschieden. Der Hardware-Typ Standard hat Prozessoren mit einer niedrigen Taktfrequenz und ist für den Einsatz mit multithreading-fähigen Anwendungen geeignet. Beim Hardware-Typ Highclock hingegen, kommen Prozessoren mit erhöhter Taktfrequenz zum Einsatz, sie sind vor allem für nicht multithreading-fähigen Anwendungen geeignet.

Die folgenden Tabellen geben eine Übersicht der verfügbaren Hardware-Profile pro Hardware-Typ. Weitere Hardware-Profile können per "Generic Request" beantragt werden. Eine allfällige Umsetzung sowie der Preis werden von Fall zu Fall durch Inventx geprüft und freigegeben.

Die Hardware-Profile mit 256 GB RAM können nur mittels "Generic Request" bestellt werden.

Tabelle: Virtual Machine Hardware-Profile Standard

Standard		**RAM in GB**								
		4	**8**	**16**	**24**	**32**	**64**	**96**	**128**	**256**
Anzahl vCPU	**2**	■	■	■	■	■	-	-	-	-
	4	-	■	■	-	■	■	-	■	■
	6	-	-	-	-	-	■	-	■	■
	8	-	-	■	-	■	■	■	■	■
	12	-	-	-	-	-	-	-	■	-
	16	-	-	-	-	■	■	-	■	■
	24	-	-	-	-	-	-	-	■	■
Systemdisk		Windows: 100 GB / Linux: 80 GB								

Tabelle: Virtual Machine Hardware-Profile Highclock

Highclock	**RAM in GB**

		4	8	16	24	32	64	96	128	256
Anzahl vCPU	**2**	■	■	■	■	■	-	-	-	-
	4	-	■	■	-	■	■	-	■	■
	6	-	-	-	-	-	■	-	■	■
	8	-	-	■	-	■	■	■	■	■
	12	-	-	-	-	-	-	-	■	-
	16	-	-	-	-	■	■	-	■	■
	24	-	-	-	-	-	-	-	■	■
Systemdisk		Windows: 100 GB / Linux: 80 GB								

:::note

Die Hardware-Profile Highclock werden ausschliesslich im SLA "Rhodium" angeboten.

:::

Storage-Profile

Die Storage-Profile setzen sich aus dem Storage-Typ (Redundanz) und der Storage-Klasse (Geschwindigkeit) zusammen, wobei der Storage-Typ vom ausgewähltem SLA abhängig ist. Pro virtuellem Computer ist für alle Laufwerke immer nur ein Storage-Typ sowie eine Storage-Klasse möglich.

In der Tabelle "Storage-Klassen" sind in der Spalte "max IOPS / vDisc" die Anzahl IOPS ausgewiesen, wie sie durch den Hypervisor limitiert sind. Dies ist die technisch höchstmögliche Anzahl IOPS, die jedoch nicht in jedem Fall garantiert werden kann.

Beim Storage-Typ "SZRS" in Zusammenhang mit den Storage-Klassen "High Performance" und "Ultra Performance" kann der angegebene Throughput nicht erreicht werden, wenn die Blockgrösse kleiner als 32 KB ist. Bei der Storage-Klasse "Ultra Performance" hält sich Inventx das Recht vor, bei Performance Engpässen die Kapazität vorübergehend zu drosseln.

Tabelle: Virtual Machine Storage-Typen

Storage-Typ	Redundanz	Latency (Messdauer 2h)	SLA
LRS	lokal-redundant	< 1 ms	Bronze & Silber
AGRS	asynchron geo-redundant	< 1 ms	Gold

SZRS	synchron zonen-redundant	n/a	Rhodium

Tabelle: Virtual Machine Storage-Klassen

Storage-Klasse	Throughput (MB/s)	max IOPS / vDisk
Standard	40	5'120
Premium	150	19'200
High Performance	300	38'400
Ultra Performance	500	64'000

Betriebssysteme

Als Betriebssystem kann entweder ein durch Inventx vorbereitetes Image oder ein "Custom Owned OS" verwendet werden.

Die durch Inventx bereitgestellten Images werden in regelmässigen Abständen nach Freigabe von Inventx auf den Stand der Wave 3 gepatcht. Dies um sicherzustellen, dass Neubestellungen in Wave 3 oder Neuer angeboten werden können. Ein Update auf Wave 2 oder Wave 1 ist direkt nach dem Bestellvorgang möglich. Die Aktualisierung wird wie folgt umgesetzt:

- Windows: Jeweils 1 Mal pro Quartal
- Linux: Jeweils bei einem neuen Minor-Release (z.B. RHEL V. 7.1 ➔ 7.2)

Nach dem Staging-Prozess einer neuen VM wird diese nicht direkt auf den gewünschten Wave gepatcht. Der erste Update-Prozess erfolgt nach dem vom Kunden definierten "Customer Maintenance Window", also nach der definierten Wave und Time Wahl. Es besteht jedoch die Möglichkeit nach dem Deployment einer VM diese manuell zu patchen.

Unter den durch Inventx bereitgestellten Images sind auch lizenzfreie Betriebssystem aufgeführt. Bei diesen Betriebssystemen ist kein Hersteller-Support vorhanden. Aus diesem Grund kann Inventx den Betrieb dieser VMs nur nach "Best Effort" gewährleisten und behält sich das Recht vor, im Störungsfall (Incident Management) die Wiederherstellungszeit gemäss SLA, bei Fehlern ausserhalb seines Einflusses, ausser Kraft zu setzen.

Bei den Customer Owned OS bringt der Kunde das für die Installation benötigte Image mit. Unterstützt werden die Formate ISO und VHD. Im Falle von ISO können die notwendigen Einstellungen für die Installation ab dem ISO-File direkt im Self-Service-Portal vorgenommen werden. Wird das Format VHD verwendet, müssen die Einstellung für die Installation ab dem VHD-File via "Generic Request" beantragt werden. In beiden Fällen sind manuelle Arbeiten seitens Inventx über den Service Request Preis abgegolten.

Tabelle: Virtual Machine Betriebssysteme

Betriebssystem	Image	Lizenz	Plus-Services
Windows Server 2022 Core	■	■	□
Windows Server 2022 Desktop Experience (DX)	■	■	□
Windows Server 2025 Core	■	■	□
Windows Server 2025 Desktop Experience (DX)	■	■	□
Red Hat Enterprise Linux 9	■	■	□
Red Hat Enterprise Linux 10	■	■	□
AlmaLinux 8	■	-	□
AlmaLinux 9	■	-	□
Customer Owned OS	□	-	-

Backup-Profile

Der Kunde kann mit verschiedenen Backup-Profilen die Datensicherung des virtuellen Servers unterschiedlich und bedürfnisgerecht abbilden. Die Datensicherung wird dabei immer monolithisch über den gesamten virtuellen Server erstellt.

Tabelle: Virtual Machine Backup-Profile

Leistungsmerkmal	Bronze	Silber	Gold	Rhodium
Monolithisches Backup des virtuellen Servers	■	■	■	■
Verschlüsselung mit kundenindividuellem Schlüssel	■	■	■	■
Intervall täglich	■	■	■	■
Standort				
• Am selben Standort der VM (local)	■	-	-	-
• Am einem entfernten Standort (remote)	-	■	■	-
• An zwei Standorte (local & remote)	-	-	-	■
Aufbewahrungsdauer				
• No Backup	■	■	■	■

• 14 Tage	☐	☐	☐	☐
• 40 Tage	☐	☐	☐	☐
• 90 Tage	☐	☐	☐	☐
On-Demand Backup	■	■	■	■

Restore

Falls virtuelle Server gesichert werden (siehe Backup-Profile), können diese auf Basis der verfügbaren Sicherungskopien wiederhergestellt werden. Die monolithische Wiederherstellung des virtuellen Servers kann der Kunde via Self-Service durchführen.

Eine partielle Wiederherstellung (z.B. eine spezifische Datei oder ein spezifischer Ordner) kann via "Standard Service Request" beantragt werden.

Availability Set

Um die Verfügbarkeit einer Anwendung zu erhöhen, empfiehlt es sich zwei oder mehr VMs mit derselben Anwendung aufzusetzen und in einem Availability Set zu gruppieren. Wenn mehrere VMs einem Availability Set zugeteilt sind, wird der Hypervisor diese VMs nach Möglichkeit auf verschiedene Hosts platzieren. Durch diese Konfiguration wird sichergestellt, dass während einem geplanten oder ungeplanten Ausfall eines Hosts mindestens eine VM mit der Anwendung weiterhin verfügbar ist. Pro Availability Set werden 3 Hosts garantiert und maximal einer davon in Maintenance Mode genommen.

Die Availability Sets müssen über einen "Standard Service Request" verwaltet werden, um anschliessend über das ix.Cloud Self-Service-Portal VMs einem Availability Set zuordnen zu können.

System Management Services

Damit IT-Organisationen den Anforderungen resilienter Infrastruktur Umgebungen von der Bereitstellung bis und mit Betrieb erfüllen können, sind nebst der reinen Bereitstellung einer virtuellen Maschine (VM) zusätzlich eine Reihe von Seurity- und Monitoring-Aktivitäten notwendig.

Die System Management Services unterstützen Kunden, VM's und Anwendungen skalierbar auf Infrastruktur-Ebene resilient zu verwalten. Der Applikations Owner kann sich so einem Standard Tool-Set bedienen und sich ganz auf die Erfüllung seiner Kern-Elemente, der Verwaltung seiner Fachanwendungen, konzentrieren.

Die folgende Tabelle listet die einzelnen Services auf, die beim Kontrollieren und Steuern der Server und des Workloads in der ix.Cloud unterstützen.

Tabelle: System Management Services

Service Name	Service Kurzbeschreibung
Managed OS	Erhöht die Sicherheit und die Verfügbarkeit von Betriebssysteme.
Metrics Monitoring	Überwachen von Server, Anwendungen und Dienste um die Leistung und Verfügbarkeit der IT-Dienstleistungen zu optimieren.
Software Deployment	Dank zentraler Softwareverwaltung eine homogene und resiliente Plattform sicherstellen.
Software und Release-Zyklen	Beschreibung über die Software-Repositories, den Umgang mit 3rd Party Software sowie die Support- und Release-Zyklen von Linux- und Windows-Betriebssystemen.

Managed OS

Managed OS ist ein optionales Add-On für [Virtual Machines](./compute-services/#virtual-machine) (VM), die mit einem [Inventx Owned OS](./compute-services/#virtual-machine-operating-systems) betrieben werden. Wird dieses Add-On auf einer VM aktiviert, übernimmt Inventx Aktivitäten, die zur Erhöhung der Sicherheit und Verfügbarkeit des Betriebssystems beitragen.

Service Architektur

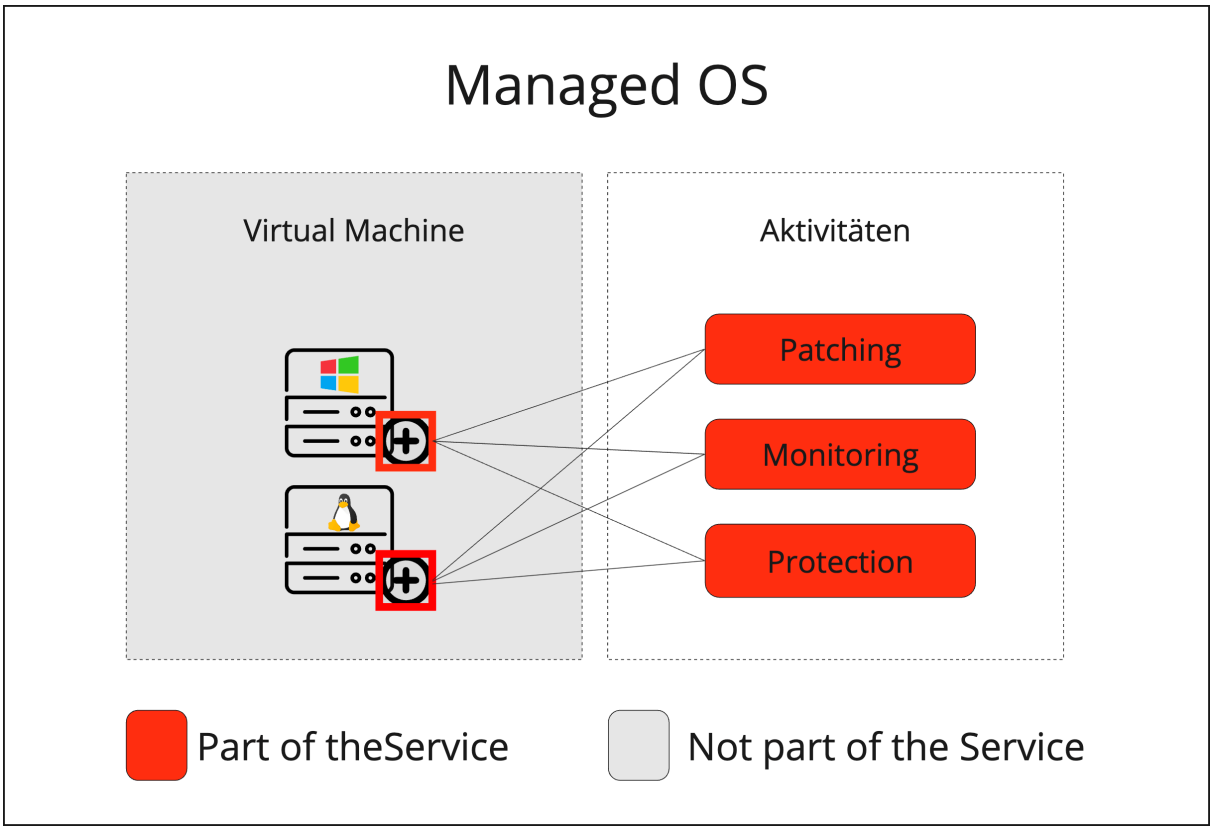


Bild: Managed OS Service Architektur

Service Umfang

Tabelle: Managed OS Service Umfang

Leistungsmerkmale	Windows	Linux
Patching	■	■
Monitoring	■	■
Protection	■	■

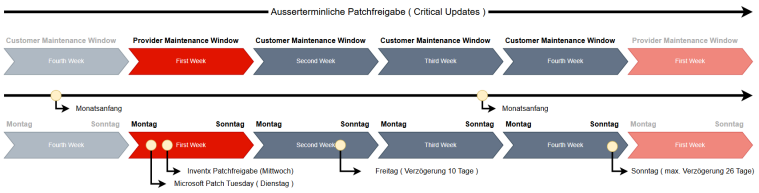
Service Optionen

Patching Addon System Update Das Patching dient der kontinuierlichen Verbesserung von Stabilität, Sicherheit und Aktualität der Server-Betriebssysteme.

Das Addon System Update umfasst einen automatischen Update-Prozess, der alle vom Hersteller freigegebenen Software-Updates berücksichtigt.

Tabelle: Managed OS - Patching

Leistungsmerkmale	Windows	Linux

Update Typen	Fokus OS ohne nachträglich installierte Software durch den Kunden, d.h. mit IE ohne Frameworks. • Critical Updates • Security Updates • Service Pack • Update Rollup	Fokus OS mit aus RHEL-Repo nachträglich installierten Softwarepaketen.
Update Frequenz	Monatlich gemäss definiertem Service Maintenance Windows und auf der VM konfiguriertem Patch-Day. Falls kein automatisches Patchen gewünscht wird, gibt es die Option "No Automatic Patch".	
Update Zyklus	Der Update-Prozess findet ein Mal im Monat statt und kann flexibel konfiguriert werden: • No Automatic Patch ◦ Der System Owner übernimmt die Verantwortung für das Einspielen der Software-Updates. • Scheduling ◦ Der System Owner wählt den gewünschten Tag und das gewünschte Zeitfenster, in dem der automatische Update-Prozess gestartet wird. Dabei konfiguriert der System Owner eine Response-Time (Verzögerung vom Tag der Inventx Patchfreigabe bis zur Installation). ◦ Die Woche des zweiten Dienstags jeden Monats steht nur der Inventx zur Verfügung.  Bild: Out of Scheduled Release	

One Time Update	Darüber hinaus kann der automatische Update-Prozess mittels der Funktion One Time Update jederzeit – auch ausserhalb der regulären Wartungsfenster – über das Cloud-Portal initiiert werden. Das hierfür definierte Zeitfenster muss mindestens 30 Minuten in der Zukunft liegen und eine Mindestdauer von vier Stunden aufweisen.	
Aktualisierte Produkte	• Windows Server 2016 Core • Windows Server 2016 Desktop Experience (DX) • Windows Server 2019 Core • Windows Server 2019 Desktop Experience (DX) • Windows Server 2022 Core • Windows Server 2022 Desktop Experience (DX) • Windows Server 2025 Core • Windows Server 2025 Desktop Experience (DX)	• Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 9 • Red Hat Enterprise Linux 10 • Alma Linux 8 • Alma Linux 9

:::info **Critical Updates**
System Management Services hält sich vor, auch ausserhalb der terminlichen Patchfreigabe (zweiter Dienstag des Monats plus ein Tag), Critical Updates freizugeben.
Nach einer ausserterminlichen Patchfreigabe stehen die Critical Updates allen Systemen zur Verfügung:

- Systeme, welche zwischen der terminlichen und ausserterminlichen Patchfreigabe, bereits gepatcht wurden, können mittels One Time Update nachgezogen werden.
- Systeme, die nach der ausserterminlichen Patchfreigabe gepatcht werden, erhalten direkten Zugriff auf die kritischen Updates.

:::

:::info Um Sicherheitslücken schneller zu schliessen, werden Edge-Updates täglich auf dem WSUS-Server freigegeben.

Nach der Freigabe steht das Update der VM ohne Neustart zur Verfügung.

- Das Update kann durch das monatliche Update oder ein One-Time Update installiert werden, was zu einem Neustart der VM führt.
- Das Update kann manuell durch den User im OS installiert werden.
- Als Alternative kann der Standard Scheduled Task durch den VM Owner für die Installation konfiguriert werden.

:::

Monitoring

Monitoring ist die Überwachung von Vorgängen, durch systematische Erfassung, Messung und Beobachtung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel. Auf Basis der gesammelten Messungen, lassen sich individuelle Alarmierungen einrichten und über einen präferierten Kommunikationskanal benachrichtigen.

Tabelle: Managed OS - Monitoring

Monitoring	**Windows & Linux**
Virtuelle Maschine	Aktive Überwachung des Performanceverhaltens (CPU/RAM/IOPS)
Gast Betriebssystem	Aktive Überwachung und Betrieb des Gast-Betriebssystems
Nutzungs- und Leistungsverhalten	Überwachen und optimieren des Nutzungs- und Leistungsverhaltens von allen Infrastruktur-Komponenten zur Sicherstellung der SLA-Vereinbarung und Vorschlägen von Verbesserungsmöglichkeiten

Protection

Endpoint Protection und Response (EDR)

Endpoint Detection and Response bietet erweiterte Angriffserkennungen, die nahezu in Echtzeit erfolgen und umsetzbar sind. Sicherheitsanalysten können Warnungen effektiv priorisieren, sich einen Überblick über das gesamte Ausmass eines Verstosses verschaffen und Reaktionsmassnahmen zur Behebung von Bedrohungen ergreifen.

Wenn eine Bedrohung erkannt wird, werden im System Warnungen erstellt, welche ein Analyst untersuchen kann. Warnungen mit denselben Angriffstechniken oder demselben Angreifer zugeordnet werden zu einer Entität zusammengefasst, die als Vorfall bezeichnet wird. Die Aggregation von Warnungen auf diese Weise erleichtert Analysten die gemeinsame Untersuchung und Reaktion auf Bedrohungen.

Tabelle: Managed OS – Protection EDR

Leistungsmerkmale	**Windows & Linux**

Cloud Protection	• Block Level
	  ◦ Hohe Blockierungsstufe, aggressives Blockieren unbekannten Elemente bei der Optimierung der Geräteleistung
	• Extended Timeout
	  ◦ Mit dieser Einstellung wird eine verdächtige Datei für eine gewisse Zeit blockiert, um eine zusätzliche Prüfung in der Cloud durchzuführen. Je länger die Blockierung dauert, desto mehr Zeit hat der Cloud Service für eine eingehende Untersuchung.

	• Protection ◦ Microsoft MAPS ist die Online-Community, die Ihnen bei der Auswahl Ihrer Reaktion auf potenzielle Bedrohungen hilft.
Monitoring	Die Verhaltensüberwachung in Echtzeit.
Scanning	• Archivdateien wie PLZ- oder CAB-Format • Heruntergeladene Files und Anhänge • Scripts • Wechseldatenträger
Potenziell unerwünschte Anwendung (PUA)	Der PUA-Schutz ist aktiviert. Potenziell unerwünschte Software wird blockiert. Erkannte Elemente werden blockiert. Sie werden zusammen mit anderen Bedrohungen in der History auftauchen.
Quarantäne	Für die folgenden Bedrohungen • Severe Severity • Moderate High Severity • Moderate Severity • Moderate Low Severity
Ausschlüsse	Ausschlüsse (Exclusions) werden im Self-Service über ix.Cloud Portal vorgenommen. Nur für Windows-Server • Auto Exclusions Für Windows- und Linux-Server • Custom Exclusions • File Extensions und Folder Location Exclusions • Files opened by processes Exclusions • Contextual files and folder Exclusions
Betriebssysteme im Scope	• Windows Server 2016 (SQL / Core / DX) • Windows Server 2019 (SQL / Core / DX) • Windows Server 2022 (SQL / Core / DX) • Windows Server 2025 (SQL / Core / DX) • Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 9 • Red Hat Enterprise Linux 10

	• AlmaLinux 8 • AlmaLinux 9
Incident-Management	Bei Entdeckung einer Bedrohung wird der Incident-Prozess durch einen gemäss definierten Security-Provider sichergestellt.
Reporting	Ein Report wird durch dem vereinbartem Security-Provider ausgehändigt, der das überwachte System und die erkannte Malware ausweist.

Voraussetzungen

Damit Inventx, die in diesem Kapitel definierten Leistungen, ordnungsgemäss ausliefern kann, müssen folgende Rahmenbedingungen erfüllt sein

Voraussetzung	**Windows**	**Linux**
Die VM muss eingeschaltet sein	✔	✔
Die für den Service benötigten Systemkomponenten werden ausschliesslich durch Inventx konfiguriert	Windows Update Agent	✔
Die für den EDR-Service benötigte Azure Subscription wird durch Inventx auf dem Azure Kunden Tenant erstellt und verwaltet	✔	✔
Die für den Service benötigten Netzwerkziele sind von der VM aus erreichbar	✔	✔
Inventx kann über das Netzwerk auf die VM zugreifen	WinRM und RDP	SSH
Inventx kann via Service-Accounts mit benötigten Rechten auf die VM zugreifen	Administrator-Rechte	Root-Rechte
Der Kunde stellt sicher, dass die Disks auf der Systempartition immer genügend Speicherplatz haben und nicht durch Anwendungs-Daten und/oder Anwendungs-Logs vollgeschrieben werden	✔	✔
Zusätzliche Softwarekomponenten dürfen nicht auf den Systemen installiert werden, welche Komponenten zur Sicherstellung der Serviceumfangs beeinträchtigen (bspw. eigene Antiviren- oder Firewall-Software)	✔	✔

:::caution Der Kunde hat administrative Rechte im Betriebssystem und trägt dabei die volle Verantwortung für den Betrieb des virtuellen Servers, falls durch eine falsche Kundenaktion (z.B. Update des Betriebssystems) eine SLA-Verletzung geschieht. :::

Metrics Monitoring

Metriken zu geschäftskritischen Anwendungen sammeln und analysieren Daten, um dadurch die Leistung und Verfügbarkeit von IT-Dienstleistungen zu verbessern. Der Einsatz von Metriken ermöglicht ein proaktives Monitoring, Störungen lassen sich frühzeitig erkennen und über definierte Kontaktpunkte gezielt alarmieren.

Der Service "Metrics Monitoring" basiert auf einer hoch verfügbaren, skalierbaren und performanten Plattform und bietet dadurch die nötige Zuverlässigkeit, die von einer Monitoring Plattform gefordert wird. Inventx stellt mit diesem Plattform-Service alle notwendigen Komponenten rund um das Thema Metrics Monitoring sicher. Der Kunde kann sich somit voll und ganz auf die Überwachung seiner Anwendungen und Dienste konzentrieren.

Die Verrechnung erfolgt pro Subscription nach Active Series und Anzahl aktiver Benutzer pro Monat.

Service Architektur

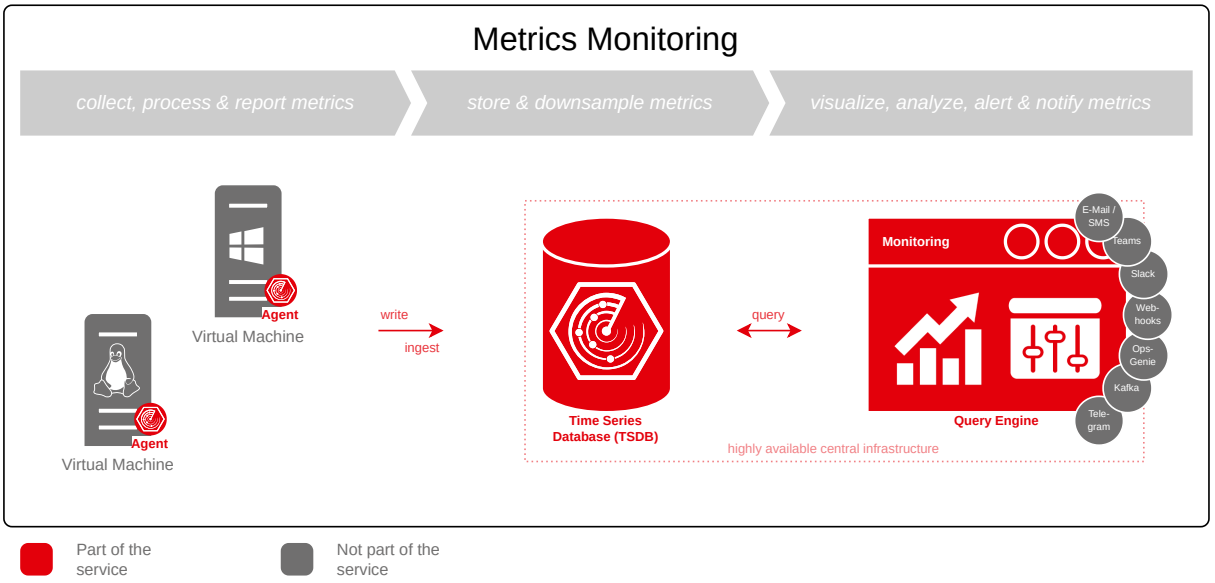


Bild: Metrics Monitoring Service Architektur

Service Umfang

Tabelle: Metrics Monitoring Service Umfang

Leistungsmerkmale

Monitoring Agent	■
Time Series Database	■
Query Engine	■
Default Metrics & Dashboard	■
Custom Metrics & Dashboards	■
Custom Alerts & Notifications	■
Interfaces to Notification Channels	■
Notification Channels	-

Service Optionen

In den folgenden Kapiteln werden die einzelnen Optionen dieses Services genauer erläutert.

Monitoring Agent

Der "Monitoring Agent" ist für die Sammlung, Verarbeitung und anschliessender Weiterleitung an die TSDB zur Speicherung zuständig. Es handelt sich dabei um eine Software zur Überwachung des jeweiligen Systems.

Die Inventx stellt sicher, dass diese Komponente auf den definierten Systemen installiert, jederzeit korrekt konfiguriert und die Sammlung der Metriken sichergestellt ist.

:::danger

Wird die Installation und/oder die Konfiguration des Monitoring Agenten bewusst oder unbewusst, durch Eingriffe Dritter, verändert oder beschädigt, kann Inventx die im Service definierten Leistungen nicht mehr erbringen.

:::

Time Series Database

Die, durch den Monitoring Agent, gesammelten Metriken werden in die Time Series Database (TSDB) geschrieben und während 13 Monate aufbewahrt. Die TSDB ist für die Speicherung und Aufbewahrung von Metriken optimiert und gewährleistet eine performante Bereitstellung der Daten.

:::info

Damit der Monitoring Agent die gesammelten Metriken an die TSDB senden kann, muss die IP-Adresse 10.94.12.36 und der Port 443 erreichbar sein.

:::

Query Engine

Die Query Engine stellt umfangreiche Möglichkeiten dar, um Metriken aus der TSDB zu visualisieren, analysieren, alarmieren und über verschiedene Kontaktpunkte zu notifizieren.

:::info

Die Query Engine ist über die URL https://monitoring.ixcloud.ch erreichbar und folgt dem ix.Cloud Berechtigungskonzept.

:::

Default Metrics & Dashboard

Beim Aktivieren des Addons werden die nachstehenden benutzeroptimierten Metriken aktiviert und in die TSDB geschrieben:

- CPU
- Memory
- Harddisk
- Network
- Services

Custom Metrics & Dashboards

Zusätzlich zu den Default Metrics & Dashboard können eigene Metriken definiert und konfiguriert werden. Dies ermöglicht es, kundenspezifische Metriken von Anwendungen und Dienste in die TSDB zu schreiben. Mittels Query Engine lassen sich diese Metriken individuell und nach eigenem Wunsch aufbereiten und visualisieren.

:::tip

Für die Konfiguration des Agenten stehen auf Github eine Grosszahl verschiedener Plugins zur Verfügung: https://github.com/influxdata/telegraf/tree/release-1.24/plugins

:::

Custom Alerts & Notifications

Auf Basis der gesammelten Metriken lassen sich, mit der Query Engine, individuelle Alarmierungen einrichten und über einen präferierten Kommunikationskanal benachrichtigen.

Interfaces to Notification Channels

Die Query Engine bietet, für die Benachrichtigungen, Schnittstellen zu folgenden handelsüblichen Tools:

- E-Mail / SMS
- Teams
- Slack
- Webhooks
- Ops-Genie
- Kafka
- Telegram

Notification Channels

Die Benachrichtigungskanäle sind nicht Bestandteil des Services, sondern müssen durch den Kunde Bereitgestellt werden.

Software Deployment

Mit Hilfe der Software Deployment Funktion kann die Bereitstellung und Installation von Software automatisiert und via Portal von einer zentralen Stelle aus verwaltet werden. Dank der zentralen Steuerung der Softwareverteilungsprozesse kann eine homogene und resiliente Plattform sichergestellt werden.

Die Standardisierung der Softwareausstattung auf Server ist ein entscheidender Schritt, um die Sicherheit der Systeme zu gewährleisten und dabei den Aufwand wie auch die Kosten zu optimieren.

Dieses Addon ist optional und kann nur auf durch Inventx bereitgestellten Windows-Betriebssysteme aktiviert werden. Die nachträgliche Deaktivierung des Addons ist nicht möglich.

:::danger

Damit Inventx die im Addon "Managed-OS" definierten Leistungen ordnungsgemäss ausliefern kann, darf folgende Software nicht durch den Kunden verteilt werden:

- Windows Updates (dies beinhaltet Windows Security Patches, Windows Feature Updates und Windows Rollup Updates)
- .Net Updates
- Splunk Universal Forwarder
- McAfee Agent
- Zabbix Agent
- Snow Agent
- Telegraf Agent
- Microsoft Defender
- Azure Connected Machine Agent

:::

Service Architektur

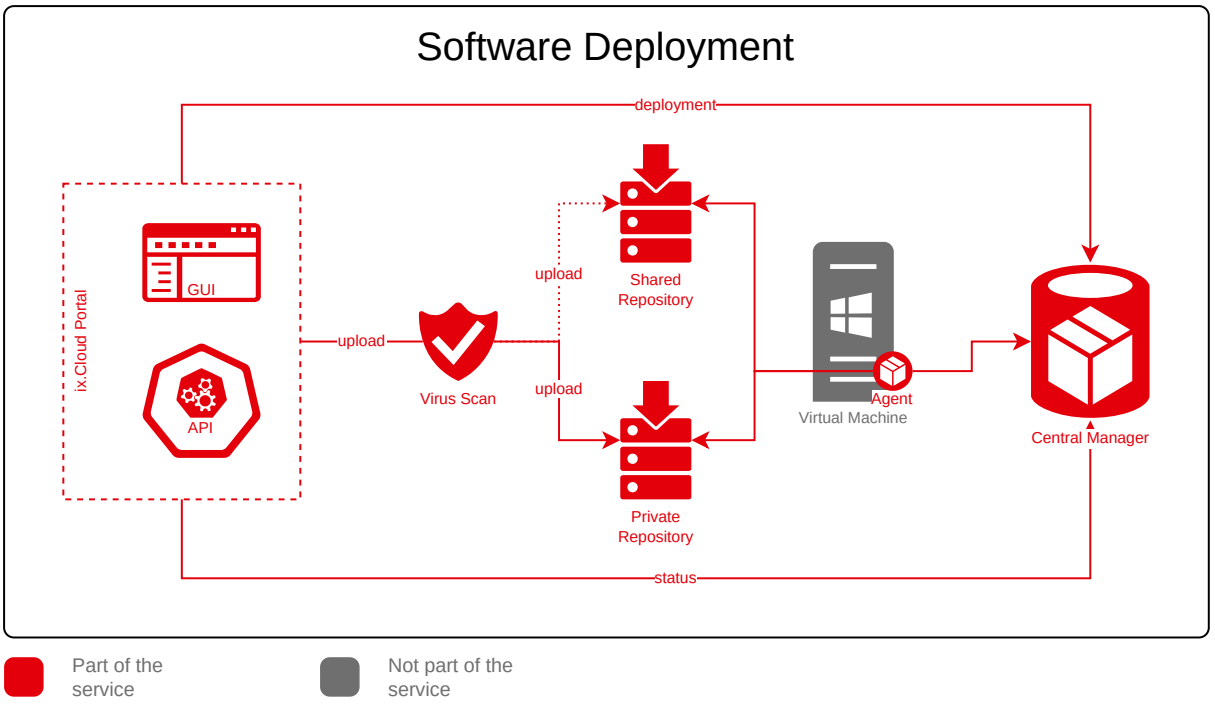


Bild: Software Deployment Service Architektur

Service Umfang

Tabelle: Software Deployment Service Umfang

Leistungsmerkmale	
Shared Repository	■
Private Repository	■
Virus Scan	■
Automatic Update	■
Scheduled Deployment	■

Service Optionen

Die folgenden Kapitel beschreiben die einzelnen Optionen des Addons Software Deployment.

Shared Repository

Über das Shared Repository stellt Inventx auserwählte Software-Pakete ix.Cloud weit zur Verfügung. Folgende Software-Pakete werden über die Shared Repository allen Kunden zur Verfügung gestellt:

- 7-Zip
- Adobe Reader
- Git
- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Notepad++
- Postman
- Visual Studio Code

:::info

Die Software-Pakete in der Shared Repository haben die Option Automatic Update aktiviert.

:::

Private Repository

Als Ablage der kundeneigenen Software-Pakete dient das Private Repository. Um Software-Pakete in dieser Repository abzuspeichern, kann entweder ein Transfer von der Community Repository des Herstellers oder ein Upload vom lokalen Computer durchgeführt werden.

Beim Upload vom lokalen Computer werden die Software-Pakete vor dem Abspeichern auf Viren geprüft (siehe Virus Scan).

:::tip

Bei Software-Pakete aus der Community Repository des Herstellers kann die Option Automatic Update aktiviert werden.

:::

Virus Scan

Als Schutz vor Malware werden dir Software-Pakete beim Upload mittels Viren-Scan auf Viren geprüft. Bei Identifikation eines Virus wird der Benutzer benachrichtigt und der Upload abgebrochen.

Automatic Update

Die Option Automatic Update kann ausschliesslich auf Software-Pakete aktiviert werden, die aus der Community Repository des Herstellers stammen. Auf Software-Pakete, die vom lokalen Computer hochgeladen wurden, kann diese Option nicht aktiviert werden.

Software-Pakete, auf denen diese Option aktiviert ist, werden wöchentlich am Sonntag um 01:00 Uhr gegen die Community Repository des Herstellers auf neuere Versionen geprüft. Sind neuere Versionen verfügbar, werden diese automatisch heruntergeladen und verfügbar gemacht. Dies hat den positiven Nebeneffekt, dass im Portal veraltete Installationen hervorgehoben werden und mit wenige Klicks aktualisiert werden können.

Scheduled Deployment

Ein Deployment kann zeitlich geplant werden. So können Installation, Aktualisierung oder Deinstallation von Software auch während der Nacht durchgeführt werden.

Software und Release-Zyklen

Linux Software

Auf den Linux-Systemen werden grundsätzlich die unten aufgeführten Software-Repositories über das ManagedOS Addon eingebunden und anhand des Update-Prozesses mitberücksichtigt. Falls das EDR Addon auf der VM aktiviert ist, wird zusätzlich das Linux Software Repository von Microsoft miteingebunden. Von diesen Software-Repositories kann jederzeit Software auf dem Zielsystem installiert werden.

Tabelle: Repos auf Linux Systemen

Linux Version	Repos
RHEL 8	• BaseOS, Appstream, CodeReady Linux Builder, EPEL* • Microsoft Software Repository (bei aktiviertem EDR Addon)
RHEL 9	• BaseOS, Appstream, CodeReady Linux Builder, EPEL* • Microsoft Software Repository (bei aktiviertem EDR Addon)
RHEL 10	• BaseOS, Appstream, CodeReady Linux Builder, EPEL* • Microsoft Software Repository (bei aktiviertem EDR Addon)
AlmaLinux 8	BaseOS, Appstream, EPEL*
AlmaLinux 9	BaseOS, Appstream, EPEL*

* Das EPEL-Repository (Extra Packages for Enterprise Linux) ist ein zusätzliches Paket-Repository, das speziell für Enterprise Linux-Distributionen wie Red Hat Enterprise Linux (RHEL), AlmaLinux und Fedora entwickelt wurde. Es bietet eine Vielzahl von zusätzlichen Open-Source-Paketen, die nicht in den Standard-Repositories dieser Distributionen enthalten sind. Das EPEL-Repo ist ein 3rd Party Software-Repo, für das die Grundsätze des Kapitels “Umgang mit 3rd Party Software” gelten.

Windows Software

Nebst den gängigen Installationsverfahren für Software auf Windows (z.B. mit Adminrechten), steht zusätzlich das Software Deployment AddOn im Self-Service zur Verfügung, um Software auf einem Windows System installieren zu können. Für diese Software gelten die Grundsätze des Kapitels “Umgang mit 3rd Party Software”

Umgang mit 3rd Party Software

Zum Umgang mit 3rd Party Software gelten folgende Grundsätze:

Mit Administratoren- bzw. Root-Rechten ist es jederzeit möglich 3rd Party Software oder Pakete zu installieren oder eigene Software-Repositories einzubinden. Für diese Software liegt die Verantwortung, das Releasemanagement und die Auswirkungen auf den Betrieb vollumfänglich beim Kunden.

Wenn durch den Einsatz von 3rd Party Software der ManagedOS Service beeinträchtigt wird, ist der entsprechende SLA ausser Kraft gesetzt. In diesem Fall kann Inventx weder die Funktionsfähigkeit der 3rd Party Software noch einen stabilen ManagedOS-Betrieb gewährleisten. Im Extremfall kann dies dazu führen, dass die komplette betroffene VM ab Backup durch den Kunden selbst oder durch Inventx im Auftrag des Kunden wiederhergestellt werden muss. Mehraufwendungen seitens Inventx aufgrund solcher Vorfälle sind nicht Teil der Geschäftlich Service-Leistungen von Inventx und sind durch den Kunden nach effektivem Aufwand zu vergüten.

Betriebssystem- und Software Release-Zyklen

Die Windows und Linux Major Betriebssystem Release-Zyklen sind grundsätzlich auf 10 Jahre ausgelegt, d.h. in dieser Zeit werden die Systems Management Services inkl. Software-Updates über das ManagedOS Addon zur Verfügung gestellt, welche der Kunde übers Portal für die entsprechende VM konfigurieren kann. Nach diesen 10 Jahren ist das Betriebssystem nicht mehr unterstützt und es stehen keine neuen Updates zur Verfügung und die Systems Management Services werden für diesen Betriebssystem-Release nicht mehr weiterentwickelt. Der Kunde ist selbst in der Verantwortung, vor Ablauf dieser 10 Jahresfrist eine neue VM mit einem neueren Major Betriebssystem-Release zu bauen und seine Applikation zu migrieren. Es werden keine Inplace-Upgrades auf eine neueren Major Betriebssystem-Release auf derselben VM angeboten (z.B. von RHEL 9 auf RHEL 10 oder Windows Server 2022 auf Windows Server 2025). Falls der Kunde selbst einen Inplace-Upgrade durchführt, muss er dafür besorgt sein, dass alle Systems Management Services weiterhin auch auf dem neuen Major Betriebssystem-Release einwandfrei funktionieren. Werden durch den Inplace-Upgrade des Kunden auf einen höheren Major-Release die Systems Management Services beeinträchtigt, dann behält sich die Inventx vor, diese Services für die entsprechende VM abzukündigen.

Support über diese 10 Jahre hinaus z.B. anhand von Extended Lifecycle Support (ELS) bei RHEL oder Extended Security Updates (ESU) bei Windows wird grundsätzlich nicht angeboten. In Ausnahmefällen kann dies über spezielle Vereinbarungen mit dem Kunden trotzdem geschehen. Es gelten dort jedoch die vom Hersteller beschriebenen Bedingungen und es kann nicht garantiert werden, ob die Systems

Management Services weiterhin in gleicher Qualität erbracht werden können. Ebenfalls hat dies allfällige Mehrkosten zur Folge.

Neben den 10-Jahres Major Betriebssystem Release-Zyklen gibt es innerhalb von RHEL auch noch Appstream Release-Zyklen. D.h. man kann über das Appstream Repository diverse Applikationen in verschiedenen Major Versionen installieren (z.B. PostgreSQL 13,15 und 16 oder .NET 6,7 und 8 usw..). Die Verantwortung dieses Major Release-Managements obliegt dem Kunden, da er die entsprechenden Channels auf dem System je nach seinem Bedarf aktivieren kann. Der Update-Prozess des ManagedOS Addons berücksichtigt nur Upgrades innerhalb des aktivierten Major Releases und nicht auf einen höheren Major-Release. Es ist hier zu beachten, dass Appstream Release-Zyklen oft kürzer sind als 10 Jahre im Vergleich zum Betriebssystem Release-Zyklus. Die genauen Angaben zu allen Release-Zyklen sind jeweils beim entsprechenden Hersteller publiziert

---

Database Services

Mit den "Database Services" können Kunden auf Basis unterschiedlicher Datenbank-Technologien und Service-Modellen ihre Geschäftsdaten in Datenbanken speichern und verwalten.

Tabelle: Database Services

Service Name	Service Kurzbeschreibung
Managed xSQL-Instance	Eine durch Inventx vorkonfigurierte und gemanagte MSSQL- oder MariaDB-Instanz mit optionalem Datenbankbetrieb.
Managed noSQL-Instance	Eine durch Inventx vorkonfigurierte und gemanagte noSQL-Instanz.

Managed xSQL-Instance

Der Service "Managed xSQL-Instance" basiert auf dem Service Virtual Machine. Auf der VM wird zusätzlich ein SQL-Server sowie eine SQL-Instanz nach Herstellerangaben und Best-Practice von Inventx installiert, konfiguriert und betrieben.

Optional zu diesem Service übernimmt Inventx das Datenbank-Management.

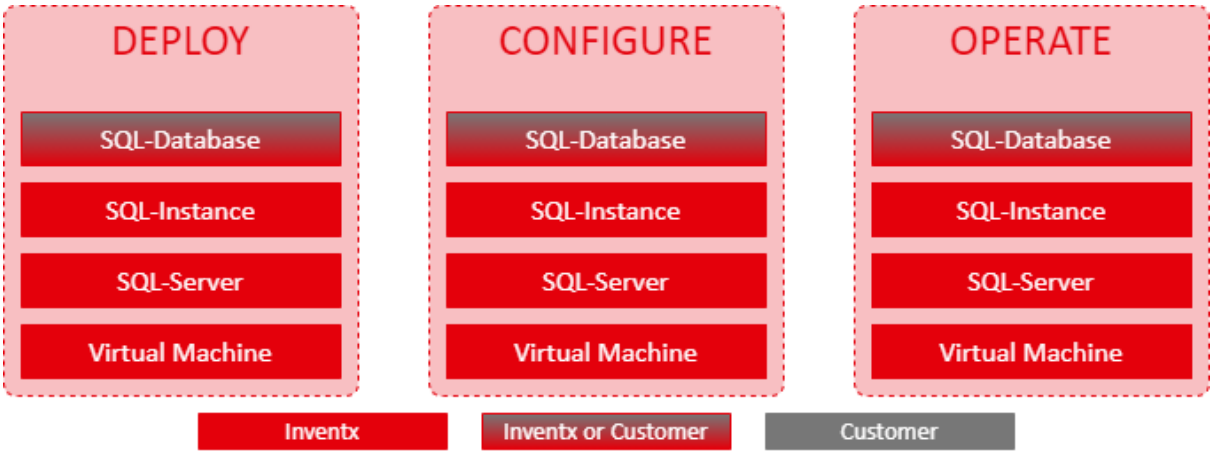


Bild: Managed xSQL-Instance Verantwortlichkeiten

Service Architektur

Siehe Service Architektur vom Service Virtual Machine.

Service Umfang

Tabelle: Managed xSQL-Instance Service Umfang

Leistungsmerkmal	Leistungsbeschreibung
Lizenzierung	Siehe Lizenzierung
Berechtigungen	Der Kunde erhält keine administrativen Rechte auf der Instance. Er wird als DBO (Database Owner) auf den einzelnen Datenbanken berechtigt.
Datenbank-Management	Der Kunde kann innerhalb der Datenbank-Instanz selber Datenbanken anlegen und muss diese selber betreiben. Inventx erbringt keine Wartungsleistungen für solche Datenbanken.
Datenbank-Backup (T-Log)	Datenbank-Backup
Datenbank-Restore	Datenbank-Restore
Datenbank-Clone	Datenbank-Clone
ON/OFF der VM	Für einen reibungslosen Betrieb dieses Services durch Inventx, darf der Kunde die VM nicht ein- und ausschalten.
Authentifizierung	MS-SQL: Die Authentifizierung erfolgt via Active Directory (NTLM oder Kerberos).

	Die Authentifizierung via SQL-User muss als Security Ausnahme (Security Exception) beantragt werden. PostgreSQL, Mariadb: Die Authentifizierung erfolgt via SQL-User.

:::info PaaS MSSQL Instanz:
aus sicherheits- und betriebsrelevanten Gründen steht der MSSQLAgent für etwaige Automatisierungen nicht zur Verfügung. :::

Service Optionen

Im Rahmen des Managed xSQL-Instance Service stehen den Kunden mehrere Technologien mit spezifischen Zusatzeigenschaften wie folgt zur Verfügung:

Lizenzierung

Inventx deckt bei diesem Service auf jeden Fall die Lizenzierung des Betriebssystems des virtuellen Servers ab (siehe Virtual Machine). Bei der Lizenzierung des Database Servers gilt wie folgt:

Tabelle: Managed xSQL-Instance Lizenzverantwortung

Lizenzverantwortung	Inventx	Kunde
Betriebssystem virtueller Server	■	-
Microsoft SQL Server	-	■
MariaDB Server	■	-
PostgreSQL Server	-	-

:::note

- Optional und nach Vereinbarung zwischen Kunde, Inventx und Microsoft sind "Lizenzmobilitäts-Programme" möglich. Diese müssen zwischen den Parteien individuell ausgearbeitet werden.
- Bei Verwendung von mehr als 16 CPU oder mehr als 128 GB RAM ist zwingend eine Microsoft SQL Enterprise Edition notwendig.

:::

Hardware-Typen und Hardware-Profile

Sämtliche Hardware-Profile des Hardware-Typen "Standard" gemäss Service Virtual Machine stehen zur Auswahl bereit.

Die Hardware-Profile der Hardware-Typen "Highclock" und "GPU" stehen nicht zur Verfügung.

Datenbank-Technologien

Dem Kunden stehen folgende Datenbank-Technologien bei diesem Service zur Verfügung:

Tabelle: Managed xSQL-Instance Datenbank-Technologien

Datenbank-Technologie	Community	Developer	Standard	Enterprise
Microsoft SQL Server 2019		■	■	■
Microsoft SQL Server 2022		■	■	■
MariaDB 10.6 als Managed Service	■			
MariaDB 11.8 als Managed Service	■			
PostgreSQL 15.0	■			■
PostgreSQL 16.0	■			■
PostgreSQL 17.0	■			■

Datenbank-Backup

Mit dem Datensicherungs-Service für Datenbanken (Datenbank-Backup) speichert Inventx die Datenbanken des Kunden mit dem Ziel ab, dass die Datenbanken im Falle einer IT-Katastrophe, eines Datenverlusts oder eines Datenfehlers wiederhergestellt werden können.

MS-SQL

Die Datenbanken werden via Service Agent des Backup Service gesichert, dieser Agent Service wird mit gMSA registriert. Der gMSA wird für jede PaaS Instance dediziert generiert und hat auf der MS-SQL Instance die Notwendigen Berechtigungen laut Hersteller.

PostgreSQL, MariaDB, MongoDB

Die Datenbanken werden auf ein NFS-Share des Backup Service gesichert. Der Backup Service triggert die Backupfunktionen der Datenbank Instance Remote über SSH an. Die Sicherung erfolgt auf einem dedizierten Verzeichnis des NFS-Share.

Tabelle: Managed xSQL-Instance Datenbank-Backup

Datenbank-Backup	MSSQL	MariaDB	PostgreSQL
Standort	gemäss SLA	gemäss SLA	gemäss SLA
Intervall			
• Full	täglich	täglich	täglich

• Differential	-	-	-
• Transaction-Log	alle 15min	-	-
• Write-Ahead-Logging	-	alle 15min	alle 15min
Aufbewahrungsdauer			
• No Backup	■	■	■
• 14 Tage	■	■	■
• 40 Tage	■	■	■
• 90 Tage	■	■	■
On-Demand Backup	■	■	■

Datenbank-Restore

Falls die Datenbanken gesichert werden (siehe Datenbank-Backup), können diese auf Basis der verfügbaren Sicherungskopien per "Generic Request" wie folgt wiederhergestellt werden:

Tabelle: Managed xSQL-Instance Datenbank-Restore

Datenbank-Restore	MSSQL	MariaDB	PostgreSQL
Datenbank Restore	Der Kunde kann einzelne Datenbanken aus dem letzten Full-Backup via "Generic Request" durch Inventx wiederherstellen lassen.		
Bedingungen	Die Datenbank muss mit Transaction-Log und einer gültigen Backup-Aufbewahrungsdauer gemäss Tabelle " Leistungsmerkmale Datenbank-Backup" konfiguriert sein, damit ein Point-in-Time-Recovery umgesetzt werden kann.		

Datenbank-Clone

Mit einem Clone wird eine Kopie einer bestehenden Datenbank oder die Kopie von einzelnen Datenbankobjekten erstellt. Inventx stellt die folgenden Varianten zur Verfügung, wobei Clones via "Standard Service Request" kostenpflichtig bestellt werden müssen.

Tabelle: Managed xSQL-Instance Datenbank-Clone

Datenbank-Clone	Umfang	Beschreibung

Full	Vollständige DB-Kopie	1-zu-1 Kopie einer Datenbank, wobei sämtliche Elemente der Datenbank (Schema und Daten) kopiert werden.
Structure	DB-Kopie ohne Inhalt	Entspricht grundsätzlich einer 1-zu-1 Kopie, allerdings nur bezogen auf das Layout einer Datenbank. Die Datenbank-Inhalte (Daten, Jobs, Prozeduren etc.) werden bei diesem Verfahren nicht kopiert, sondern nur die Tabellen.
Individual	Individueller Umfang	Individueller Umfang, der gemeinsam spezifiziert wird: • Partial Clone: Kopie einzelner Tabellen • Delta-Clone: Kopie mit nachträglichen Mutationen • Transaction-Realtime-Replication (TRR): Einzelne Transaktionen in Echtzeit • Multiple Clone: Bereitstellung auf mehreren Target-DB

Ein Cloning bedarf zwingend zwei Datenbanken: Eine Source-DB und eine Target-DB, wobei beide unterschiedliche Namen haben können. Die Source-DB liegt auf einer bestehenden DB-Instanz und muss gesichert werden (aktiver Backup-Service). Als Target-DB kann entweder eine Datenbank auf der DB-Instanz der Source-DB definiert werden oder eine Datenbank auf einer anderen DB-Instanz, wobei diese in derselben Netzwerk-Zone wie die Source-DB betrieben werden muss. Während des Cloning-Prozesses ist die Target-DB nicht verfügbar.

Erweiterte Funktionen

Die folgenden technologiebedingten Zusatzfunktionen stehen dem Kunden optional zur Verfügung.

Tabelle: Datenbank-AddOns Managed Service

Datenbank-AddOns Managed ServiceDatenbank-AddOns Managed Service	**MSSQL**	**MariaDB**	**PostgreSQL**
Always On / DB Clusterung	☐	-	☐
Security Audit	☐	-	☐

Datenbank-Management

Als optionalen Managed Service übernimmt Inventx auf Basis des hier beschriebenen Service das Datenbank-Management. Dabei gilt folgende Leistungsvereinbarung:

Tabelle: Managed xSQL-Instance Datenbank-Management

Leistungsmerkmal	**Leistungsbeschreibung**

Order Management	Neue Datenbanken müssen via "Standard Service Request" bestellt werden.
Berechtigung	Übernimmt Inventx die Betriebsverantwortung für die Datenbanken, so entzieht Inventx dem Kunden die Berechtigungen auf der xSQL-Instanz.
Datenbank-Deplyoment	Es erfolgt vor dem Deployment einer neuen Datenbank eine Prüfung von Inventx, ob diese auf der bestehenden Datenbank-Instanz betrieben werden kann oder ob eine neue Datenbank-Instanz erstellt werden soll.

Datenbank-Betrieb	Inventx stellt im Rahmen der ordentlichen Betriebsverantwortung folgende Leistungen sicher, wobei teils Leistungen separat kostenpflichtig sind (Change oder Service Request):
	• Konzeption und Umsetzung der Datensicherheit
	• Überwachung der Verfügbarkeit der Datenbank
	• Fehleranalysen/-behebungen bzgl. Verfügbarkeit der Datenbank
	• Durchführung der Datenbank-Backups
	• Benutzerverwaltung:
	  ◦ Verwaltung von persönlichen DB-Benutzern (Change Request)
	  ◦ Verwaltung von technischen DB-Benutzern
	• Durchführung von Datenbank-Restores (Change Request)
	• Umsetzung von Datenbank-Optimierungen (Change Request)
	• Clonen von Datenbanken mittels Backup (Service Request)
	• Migration einer Datenbank auf neue Instanz (Change Request)

Erweitere Leistungserbringung	Zusätzliche Arbeiten zur Leistung Datenbank-Betrieb (z.B. Performance-Analysen) können durch Inventx erbracht werden. Diese muss der Kunde jedoch einzeln via Change Request beauftragen und werden in Regie (Time & Material) abgerechnet.

PostgreSQL HA Managed Service

Mit dem PostgreSQL HA Cluster steht eine PostgeSQL Hochverfügbarkeitslösung als Managed Service zur Verfügung.

Der PostgreSQL HA Cluster wird als 2 Nodes (active,passive read only) PostgreSQL Managed Service mit virtueller IP auf Basis eines lizenzpflichtigen Failover Managers bereitgestellt.

Die Cluster Nodes werden auf Basis des PostgreSQL Managed Service bereitgestellt und betrieben.

Der Cluster muss via Change Request bestellt werden.

Service Architektur

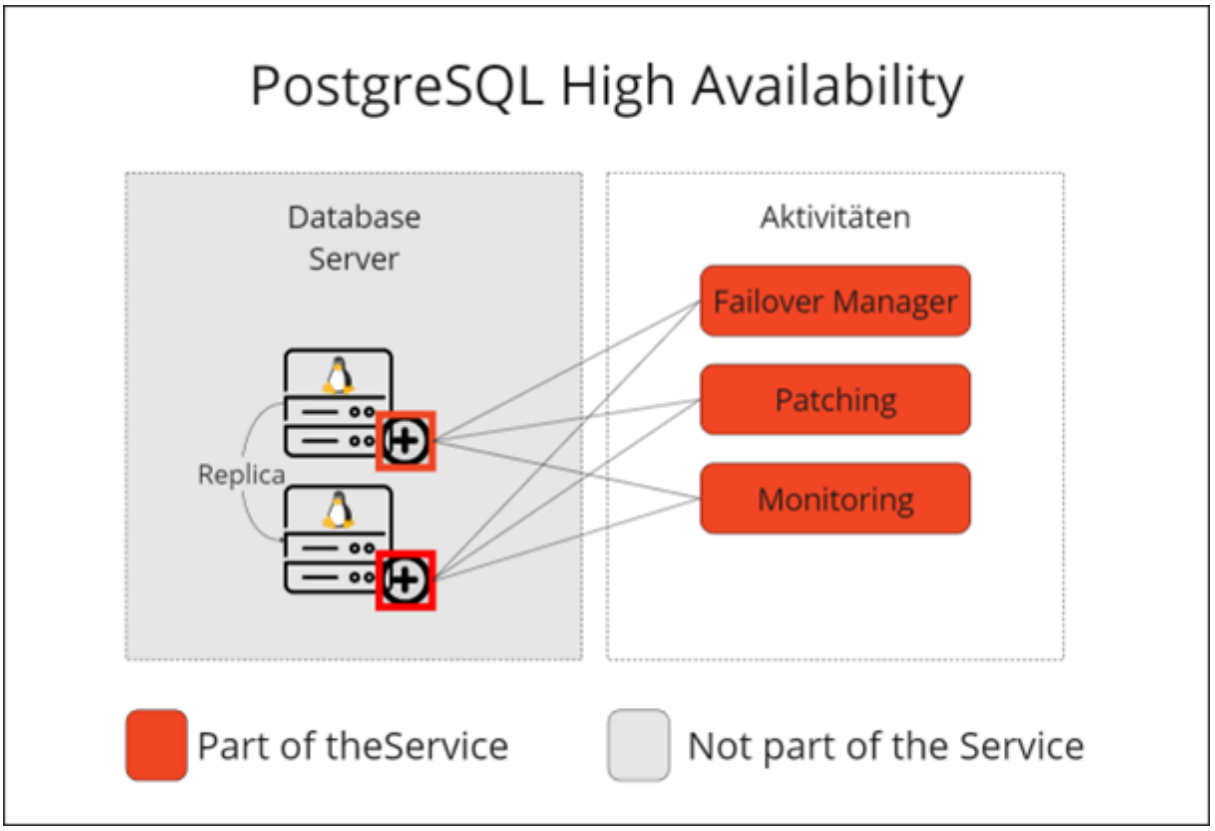


Bild: PostgreSQL HA Managed Service Verantwortlichkeiten

Service Umfang

Tabelle: PostgreSQL HA Managed Service Umfang

PostgreSQL HA Cluster Node	Beschreibung
Primary	Aktive Node für Schreibvorgänge und Lesevorgänge. Virtuelle IP ist dieser Node zugeordnet.
Standby	Standby für den Failover Fall. Passive Node für Lesevorgänge

Managed noSQL-Instance

Der Service "Managed noSQL-Instance" basiert auf dem Service Virtual Machine. Auf der VM werden die Server Binaries sowie die Instanz nach Herstellerangaben und Best-Practice der Inventx installiert, konfiguriert und betrieben.

:::note

Mit zunehmenden Datenwachstum und dem Anspruch Daten flexibel und skalierbar handhaben zu können sind parallel zu den herkömmlichen Relationale-Datenbank-Management-Systemen (RDBMS) noch weitere Datenbank Management Systeme (DBMS) herangewachsen die sich grundlegend von den RDBMS-Systemen unterscheiden. NoSQL DBMS zeichnen sich durch ihre horizontal und vertikale Skalierbarkeit aus, in der Regel sind noSQL Systeme Schemafrei, weswegen Sie sich im Big Data Umfeld und dem Aufbau von Geo-Redundanten Hochverfügbaren – DBMS Clustern eigenen. NoSQL System können i.d.R. nicht nur mit SQL-Syntax umgehen, sie sind oft auch in der Lage eine Vielzahl Unterschiedlicher und Anwendungsspezifische Syntax zu verwenden.

:::

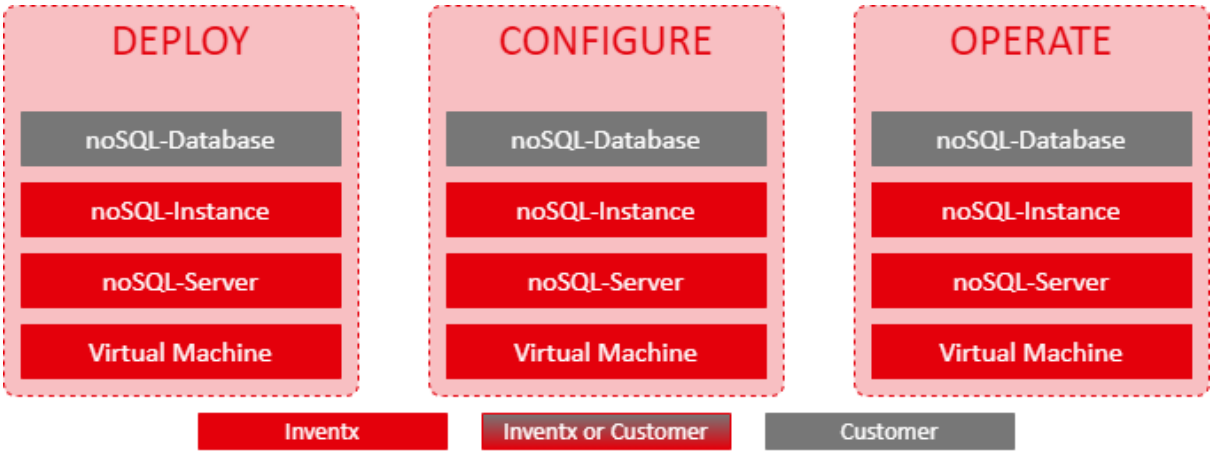


Bild: Managed noSQL-Instance Verantwortlichkeiten

Service Architektur

Siehe Service Architektur vom Service Virtual Machine.

Service Bereitstellung

Die Host Instanz muss als **«Managed OS»** Instanz im IX-Portal bestellt werden.
Die Bestellung der MongoDB Community ist mittels «Standard ServiceRequest» zu beauftragen.

Service Umfang

Tabelle: Managed noSQL-Instance Service Umfang

Leistungsmerkmal	**Leistungsbeschreibung**
Lizenzierung	Siehe Lizenzierung
Berechtigungen	Der Kunde erhält keine administrativen Rechte auf der Instance. Er wird als DBO (Database Owner) auf den einzelnen Datenbanken berechtigt

Datenbank-Management	Der Kunde kann innerhalb der Datenbank-Instanz selber Datenbanken anlegen und muss diese selber betreiben. Inventx erbringt keine Wartungsleistungen für solche Datenbanken.
Datenbank-Backup	Siehe Datenbank-Backup
Datenbank-Restore	Siehe Datenbank-Restore
Datenbank-Clone	Siehe Datenbank-Clone
ON/OFF der VM	Für einen reibungslosen Betrieb dieses Services durch Inventx, darf der Kunde die VM nicht ein- und ausschalten.
Authentifizierung	Die Authentifizierung erfolgt via SQL-User.

Service Optionen

Im Rahmen des Managed noSQL-Instance Service stehen die folgenden Optionen zur Verfügung.

Lizenzierung

Inventx deckt bei diesem Service auf jeden Fall die Lizenzierung des Betriebssystems des virtuellen Servers ab (siehe Virtual Machine). Bei der Lizenzierung des Database Servers gilt wie folgt:

Tabelle: Managed noSQL-Instance Lizenzverantwortung

Lizenzverantwortung	Inventx	Kunde
Betriebssystem virtueller Server	■	-
MongoDB 7 als Managed Service	-	-
MongoDB 8.0 als Managed Service	■	■
MongoDB 8.2 als Managed Service	■	■

Hardware-Typen und Hardware-Profile

Sämtliche Hardware-Profile des Hardware-Typen "Standard" gemäss Service Virtual Machine stehen zur Auswahl bereit.

Die Hardware-Profile der Hardware-Typen "Highclock" und "GPU" stehen nicht zur Verfügung.

Datenbank-Technologien

Dem Kunden stehen folgende Datenbank-Technologien bei diesem Service zur Verfügung:

Tabelle: Managed noSQL-Instance Datenbank-Technologien

Datenbank-Technologie	Community	Enterprise
MongoDB 7 als Managed Service	■	-
MongoDB 8.0 als Managed Service	■	■
MongoDB 8.2 als Managed Service	■	■

:::info Für externe Endkunden steht ausschliesslich die Enterprise Edition (EE) zur Verfügung. Aufgrund einer Lizenzänderung des Herstellers (SSPL) ist es uns nicht mehr möglich, die Community Edition (CE) externen Kunden bereitzustellen.

mongo/LICENSE-Community.txt at master · mongodb/mongo · GitHub :::

Datenbank-Backup

Mit dem Datensicherungs-Service für Datenbanken (Datenbank-Backup) speichert Inventx die Datenbanken des Kunden mit dem Ziel ab, dass die Datenbanken im Falle einer IT-Katastrophe, eines Datenverlusts oder einer Fehlmanipulation wiederhergestellt werden können.

Tabelle: Managed xSQL-Instance Datenbank-Backup

Datenbank-Backup	MongoDB
Standort	gemäss SLA
Intervall	
• Full	täglich
• Differential	-
• Transaction-Log	-
• Write-Ahead-Log	-
Aufbewahrungsdauer	
• No Backup	■
• 14 Tage	■
• 40 Tage	■
• 90 Tage	■

On-Demand Backup	-

Datenbank-Restore

Falls die Datenbanken gesichert werden (siehe Datenbank-Backup), können diese auf Basis der verfügbaren Sicherungskopien per "Generic Request" wie folgt wiederhergestellt werden:

Tabelle: Managed noSQL-Instance Datenbank-Restore

Datenbank-Restore	MongoDB
Datenbank Restore	Der Kunde kann einzelne Datenbanken aus dem letzten Full-Backup via "Generic Request" durch Inventx wiederherstellen lassen.

Datenbank-Clone

Mit einem Clone wird eine Kopie einer bestehenden Datenbank oder die Kopie von einzelnen Datenbankobjekten erstellt. Inventx stellt die folgenden Varianten zur Verfügung, wobei Clones via "Standard Service Request" kostenpflichtig bestellt werden müssen.

Tabelle: Managed noSQL-Instance Datenbank-Clone

Datenbank-Clone	Umfang	Beschreibung
Full	Vollständige DB-Kopie	1-zu-1 Kopie einer Datenbank, wobei sämtliche Elemente der Datenbank (Schema und Daten) kopiert werden.

Ein Cloning bedarf zwingend zwei Datenbanken: Eine Source-DB und eine Target-DB, wobei beide unterschiedliche Namen haben können. Die Source-DB liegt auf einer bestehenden DB-Instanz und muss gesichert werden (aktiver Backup-Service). Als Target-DB kann entweder eine Datenbank auf der DB-Instanz der Source-DB definiert werden oder eine Datenbank auf einer anderen DB-Instanz, wobei diese in derselben Netzwerk-Zone wie die Source-DB betrieben werden muss. Während des Cloning-Prozesses ist die Target-DB nicht verfügbar.

Managed Service Database Security Audit

Die Audits werden durch SQL interne Funktionen erzeugt und auf dem Filesystem abgelegt. Diese Audits werden an einen Splunk Loadbalancer im Tennant des Kunden weitergeleitet.

Service Architektur

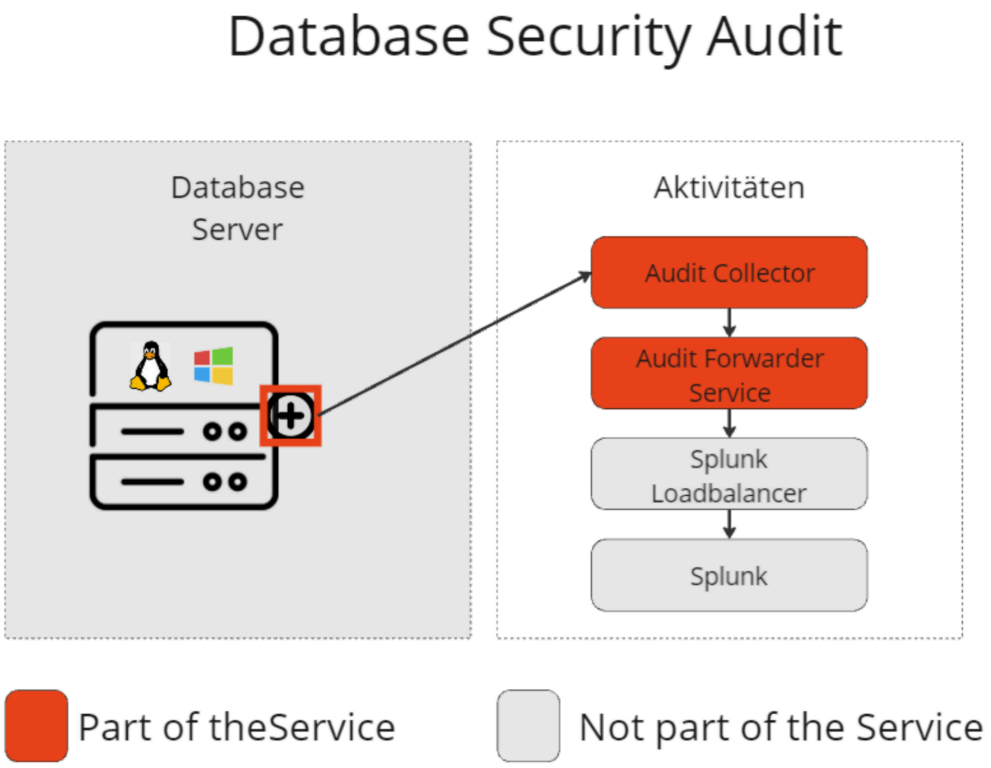


Bild: Service Architektur

Service Umfang

Obligatorisches Database Security Audit

Tabelle: Obligatorisches Database Security Audit

Security Audit	Beschreibung
Audit Logins	- Alle User Succsess/Faild Logins - Logout

Das obligatorische Security Audit wird per Default auf jeder Instanz installiert und kann nicht deaktiviert werden.

Optionales Database Security Audit

Tabelle: Optionales Database Security Audit

Security Audit	Beschreibung
Audit Privileges	- Alle Create/Delete/Grant/Revoke System Privileges - Alle Create/Delete/Grant/Revoke Database Privileges

Audit Systemsettings	- Alle Audit Policies Änderungen - Alle Instance Anpassungen
Audit Activity high Privileged User	- Alle DDL-Aktionen von User mit hohen Rechten inkl. Datenbankadministratoren Das Audit erfolgt Top Level nur auf Meta Daten der Query - Alle DML-Aktionen von User mit hohen Rechten inkl. Datenbankadministratoren Das Audit erfolgt Top Level nur auf Meta Daten der Query

Das optionale Security Audit wird per Default auf jeder Instanz installiert und bei bedarf deaktiviert werden. Dies wird im Audit bei Deaktivierung erfasst und in der Konfiguration des Managed Service in Portal dokumentiert.

IT Grundschutz Database Service

Patch Management

- Die Patches werden alle 4 Wochen in 3 Waves deployed
- Systeme, die nicht automatisch gepatcht werden können, werden monatlich manuell gepatcht. Der Patch-Vorgang und alle relevanten Informationen werden im Confluence dokumentiert.
- Beim Emergency Patching wird eine identifizierte kritische Schwachstelle umgehend gepatcht.

Logging

- Die Systeme werden durch unser Monitoring protokolliert, einschliesslich Event-Logs, Login's und Aufzeichnungen von Administratorenkonten.
- Die Logs werden 90 Tage online gespeichert, Statistiken werden 360 Tage vorgehalten.
- Eine Überwachung stellt sicher, dass die Log's fortlaufend aufgezeichnet werden. Im Fehlerfalle wird automatisch eine Ticket an den Betrieb gesendet.

Malware Schutz

- Der Malware Schutz wird mit dem Schutz über das Operating System sichergestellten.

Container Services

Damit Informatik-Organisationen die dynamischen Anforderungen zur Umsetzung ihres Geschäftsmodells erfüllen können, setzen viele Unternehmen moderne IT-Plattformen und Organisationskonzepte wie DevOps ein. Die folgenden Dienstleistungen unterstützen Kunden dabei, die

Anwendungsentwicklung und den skalierbaren IT-Betrieb optimal auf die Geschäftsdynamik auszurichten.

Mit «Container Services» bietet die ix.Cloud ein umfangreiches Tool-Set, um Micro-Services vollautomatisiert deployen und effizient verwalten zu können. Dabei fokussieren sie sich vollumfänglich auf ihre Anwendungen und Prozesse, während Inventx für sie die Infrastruktur betreibt und stetig weiterentwickelt.

Tabelle: Container Services

Service Name	Service Kurzbeschreibung
IT-Grundschutz	Erläuterung Container Service IT-Grundschutz
Container Registry	Speichern und verwalten Sie ihre Docker-Container-Images sicher in der ix.Cloud
Agile Factory	Bietet eine Kunden individuell integrierbare und auf Openshift Kubernetes basierende DevOps Umgebung
AnyCloudK8s	Ist ein flexibler und agnostischer Container-Plattform-Service
Container Namespace	Erlauben es dem Entwickler, ausgewählte Typen bei der Programmierung miteinander zu gruppieren und mehrfach benötigten Code in Module auszulagern

IT-Grundschutz

In diesem Abschnitt wird der allgemeine IT-Grundschutz für die Container-Services beschrieben. Sollte es bei einem spezifischen Service Abweichungen geben, werden diese im entsprechenden Service-Umfang explizit aufgeführt.

Upgrade und Patching

- **Herstellerabhängige Vorgaben:** Patching und Upgrades erfolgen gemäss den Vorgaben der jeweiligen Hersteller. Die Intervalle richten sich danach, wann neue Versionen oder Patches veröffentlicht werden.
- **Kein Umgang mit Exclusions:** Da es sich um ein PaaS-Umfeld handelt, werden keine individuellen Patches verteilt. Alle Patches und Upgrades erfolgen stets auf der Plattform-Ebene.

- **Emergency Patching:** Bei der Identifikation einer kritischen Schwachstelle wird diese sofort gepatcht oder ein Upgrade durchgeführt, sobald eine entsprechende Lösung vom Hersteller bereitgestellt wird für die Plattform-Ebene.

Logging

- **Systemlogs:** Systemlogs werden in Splunk gespeichert.
- **Aufbewahrungsfrist:** Logs werden für einen Zeitraum von 3 Monaten aufbewahrt.

Container Registry

Die Container Registry ist ein zentraler Ort, an dem Container Images bereitgestellt werden können. Bei der Bereitstellung wird das Image automatisch einem Vulnerability-Scan unterzogen. Damit kann die Ausführung unsicherer Images verhindert werden.

Mit der Integration der Container Registry in bestehenden CI/CD-Strukturen können vollautomatische Pipelines eingerichtet werden.

Service Architektur

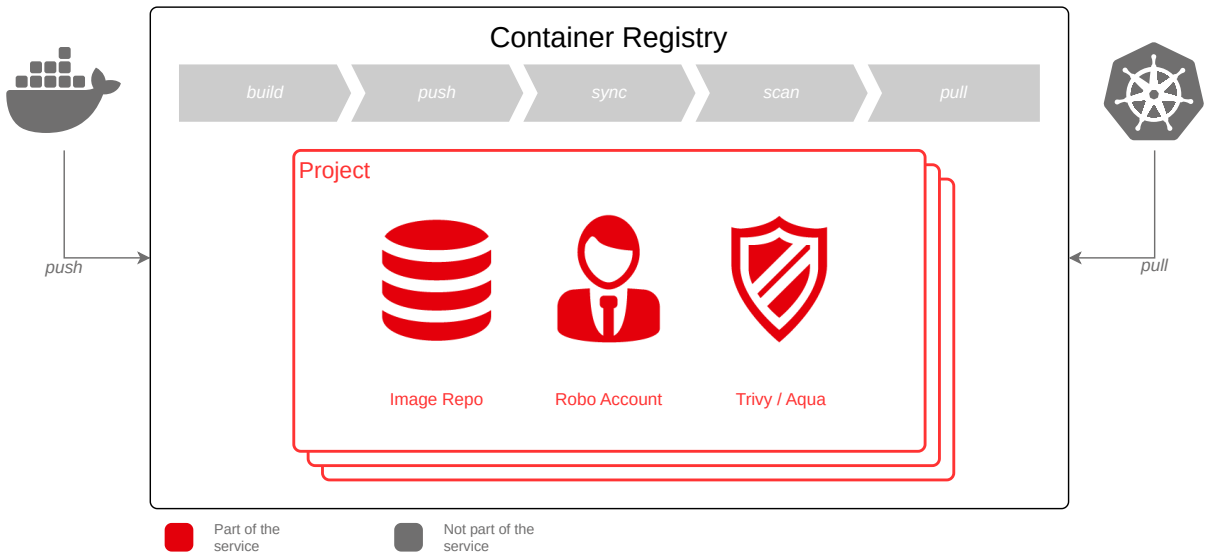


Bild: Service Architektur Container Registry

Service Umfang

Tabelle: Container Registry Service Umfang

Leistungsmerkmale

IT-Grundschutz	■
Quota	■
Vulnerability Scan	■
Robot Account	■
Allow Public Access	■
Access to User Interface	■
CVE allowlist	■

IT-Grundschutz

Patching/Upgrade Interval

Tabelle: Container Registry Patching/Upgrade

Wochen Tag	Uhr Zeit
Einmal pro Quartal, am zweiten Mittwoch vom Monat	12:00-14:00 Uhr

Hardening

- **Externe Überprüfung:** Der Service wird alle 2 Jahre durch eine externe Firma auf Sicherheitslücken und Konformität geprüft.
- **Sicherstellung durch CI/CD:** Der Service wird über einen Pipeline (Continuous Integration/Continuous Deployment) bereitgestellt, wodurch kontinuierlich ein sicheres und gehärtetes Setup gewährleistet wird.

Service Optionen

Die folgenden Optionen stehen im Service "Container Registry" zur Verfügung und können im Self-Service individuell eingestellt werden.

Quota

Die Quota definiert die maximale Speicherkapazität der Repository. Wenn diese erreicht wurde, können keine weiteren Images hochgeladen werden.

Die maximale Speicherkapazität der Repository kann jederzeit im Portal nach oben oder nach unten angepasst werden.

Vulnerability Scan

Der Vulnerability Scan ist standardmässig aktiviert und kann nicht deaktiviert werden. Sämtliche Images werden einmal täglich automatisch durch den Vulnerability Scanner geprüft. Damit wird sichergestellt, dass für jedes Image ein tagesaktueller Vulnerability Report vorhanden ist.

In der folgenden Tabelle werden die verfügbaren Vulnerability Scanner aufgelistet und beschrieben:

Tabelle: Container Registry Vulnerability Scannner

Scanner	Beschreibung
Trivy	Einfaches Scan-Tool für Anwendungen, die nicht geschäftskritisch sind, oder wenn mit weniger komplexen verteilten Architekturen gearbeitet wird.
Aqua Enterprise	Erweitertes Scan-Tool für erhöte Sicherheit. Besonders empfehlenswert bei geschäftskritische und komplexe cloud-native Anwendungen.

:::caution

Der Vulnerability Scanner "Aqua Enterprise" generiert zusätzliche Kosten.

:::

Robot Account

Robot Accounts werden im Allgemeinen für die Workflow-, Bereitstellungs- und Testautomatisierung verwendet.

:::info

Wird im Feld "Expiration time in days" der Wert "-1" eingetragen, hat der Token kein Ablaufdatum.

:::

Allow Public Access

Um anonyme Benutzer auf eine Container Registry mit Lesezugriff zu berechtigen, muss "Allow Public Access" eingeschaltet werden.

Access to User Interface

Für die erweiterte Verwaltung der Container Registry wird der Zugriff auf das User Interface erlaubt. Auch kann über das UI zusätzlich Informationen wie z.B. der Vulnerability Report der einzelnen Images eingesehen werden.

CVE allowlist

Es kann pro Repo/Projekt eine Allow Liste erstellt werden, welches für alle Images in dieser Lokation gilt. Die Gültigkeitsdauer der Liste kann mit einem Datum definiert werden, oder das sie nie Ablauft. Der

Defaultwert ist "Never expires".

Agile Factory

Die Agile Factory ist ein Container-Plattform Service, der aus einer vielzahl an Komponenten besteht, die untereinander zu einer effizienten und branchenoptimierte DevOps Umgebung verbunden werden. Alle Komponenten und die Verbindungen unter diesen werden durch Inventx nach best-practices bereitgestellt und betrieben, obwohl einzelne Komponenten auch durch den Kunde bereitgestellt werden können.

Mit diesem Service erstellen, verwalten und skalieren cloud-native Anwendungen effizient und simple. Inventx verwaltet alle Komponenten und bietet eine Entlastung für den Kunden. Entwickler können sich ganz auf die Geschäftslogik und die Eigenentwicklungen konzentrieren.

Die Agile Factory wird in drei standardisierten Architekturen/Ausführungen (Basic, Top und Premium) auf Basis des Virtual Machine Service angeboten. Die Ausführung Basic ist für nicht-produktive, die Ausführung Top für produktive und die Ausführung Premium für geschäftskritische Anwendungen zu empfehlen.

Die initiale Installation und Konfiguration sowie sämtliche Änderungen danach sind mit einem "Generic Request" oder einem "Service Request" zu beauftragen.

:::info

Dem Service Agile Factory liegt der ix.Cloud standard Service Level zugrunde und die Worker Nodes der jeweiligen Ausführungen **Basic**, **Top** und **Premium** legen den gültigen SLA fest.

Für den Wiederanlauf der Agile Factory muss zusätzlich zum standard Service Level mit einem Uplift von 2 Stunden gerechnet werden.

:::

Service Architektur

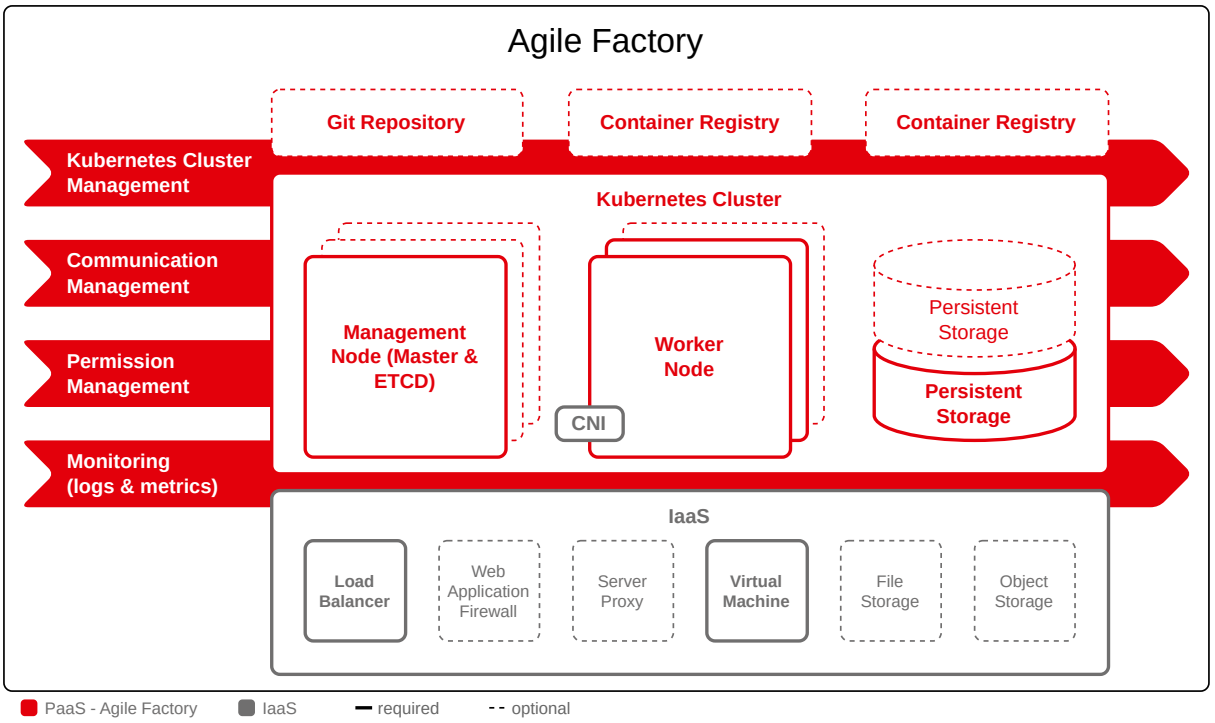


Bild: Agile Factory Service Architektur für Rancher und Openshift

Service Umfang

Tabelle: Agile Factory Service Umfang

Leistungsmerkmal	Basic	Top	Premium
IT-Grundschutz	■	■	■
Initiales Setup	□	□	□
Git Repository	□	□	□
Container Registry	□	□	□
Container Network	■	■	■
Management Node (Master & ETCD)	■	■	■
Worker Node	■	■	■
Persistent Storage	■	■	■
Load Balancer	■	■	■
Web Application Firewall	□	□	□

Server Proxy	□	□	□
Kubernetes Cluster Management	■	■	■
Communication Management	■	■	■
Permission Management	■	■	■
Monitoring (logs & metrics)	■	■	■
Cluster Network Interface	-	-	■

IT-Grundschutz

Patching/Upgrade Interval

Tabelle: Agile Factory Patching/Upgrade Interval

Wochen Tag	Uhrzeit
Am Freitag nach dem zweiten Montag im Monat	02:00-06:00 Uhr

Hardening

- Die Vorgaben wurden im ATSB geprüft und abgenommen
- Diese werden durch die Automatisierung umgesetzt
- Diese wird durch GitOps sichergestellt

Marware-Schutz

Alle Container-Images werden in der Container Registry auf Sicherheitslücken und Schwachstellen gescannt.

Configuration Management

Das Asset Mgmt wird im GitOps sichergestellt

Configuration Management

Das Asset Mgmt wird im GitOps sichergestellt

Service Optionen

Nachfolgend sind die einzelnen Komponenten der Agile Factory im Detail beschrieben. Teils Komponenten sind zwingend notwendig und teils optional.

Initiales Setup

Die initiale Konfiguration der Agile Factory wird im Rahmen eines Projekts umgesetzt und verrechnet. Dabei werden in Zusammenarbeit die kundenindividuellen Konfigurationen spezifiziert und anschliessend implementiert.

Git Repository

Für die Versionierung von Code der Deployments ist in der Agile Factory zwingend ein Git Repository notwendig. Diese kann durch den Kunde oder durch Inventx bereitgestellt werden.

Wenn das Git Repository durch Inventx gestellt wird, dann erhält der Kunde im Inventx eigenen Git einen autorisierten Benutzer, mit dem Projekte erstellt, verwaltet und gelöscht werden können. Wird das Git Repository vom Kunde bereitgestellt, so wird im Initial Setup die Kommunikation zwischen den Komponent aufgebaut und sichergestellt.

Container Registry

Die Agile Factory benutzt für sämtliche Deployments im Kubernetes Cluster eine Container Registry. Diese Komponente kann durch den Kunden oder die Inventx bereitgestellt werden.

Wenn Inventx die Container Registry stellt, dann wird der Service Container Registry eingesetzt. In diesem Fall ist Inventx für einen störungsfreien Betrieb dieser wichtigen Komponente verantwortlich.

Wird die Container Registry vom Kunde bereitgestellt, so wird im Initial Setup die Kommunikation zwischen den beiden Komponenten Kubernetes Cluster und Container Registry sichergestellt. In diesem Fall ist der Kunde gleichermassen mitverantwortlich, dass die Kommunikation zwischen den Komponenten störungsfrei läuft.

Container Network

Für jede Agile Factory benötigt es noch ein Subnetz. Durch die Grösse des Netzes wird definiert, wie viele Worker Nodes dem Cluster maximal hinzugefügt werden kann.

Tabelle: Netzwerkgrösse

Produkt	Optionen
Openshift/Rancher	Die Netzwerkgrösse ist frei wählbar

Management Node (Master & ETCD) für Openshift/Rancher

Der Management Node dient der Verwaltung des Kubernetes Clusters. Über den Management Node kann via CLI, GUI oder API der Kubernetes Cluster sowie darauf installierten Anwendungen verwaltet werden. Er dient als Steuerungsebene des Clusters und verwaltet ständig den Ist-Zustand des Cluster in den definierten Soll-Zustand. Der Management Nodes koordiniert alle Aufgaben einschließlich der Planung und Skalierung von Anwendungen.

Diese Klusterkomponente wird nach Inventx Best Practices entweder auf dedizierten Virtual Machine installiert und konfiguriert. Um eine Fehlertoleranz zu erreichen, wird je nach Serviceausprägung mehr als ein Management Node installiert.

Die initiale Konfiguration eines Management Nodes ist nicht veränderbar und wie folgt definiert:

Tabelle: Agile Factory Management Nodesfür Openshift/Rancher

Leistungsmerkmal	Basic	Top	Premium
Anzahl Server	Rancher: 1, OpenShift: 3	Rancher: 3, OpenShift: 3	Rancher: 3, OpenShift: 3
Service-Level	Rhodium	Rhodium	Rhodium
Hardware-Profile	Rancher: P2/8, OpenShift: P4/32	Rancher: P2/8, OpenShift: P4/32	Rancher: P2/8, OpenShift: P4/32
Storage Klasse	High Performance	High Performance	High Performance
Backup Retention Time	14 Tage	14 Tage	14 Tage

Worker Node

Der Worker Node ist eine Virtual Machine, auf dem die Anwendungen ausgeführt werden und der vom Management Node gesteuert wird.

Anders als beim Management Node können die Hardware-Ressourcen beim Worker Node ausgewählt und angepasst werden. Entweder man fügt weitere Worker Nodes im Kubernetes Cluster hinzu (scale-out) oder man ändert das Hardware-Profile bei den bestehenden Worker Nodes (scale-up).

Die Ressourcen Anpassung der Worker Node kann mit einem "Service Request" beauftragt werden.

Die Initialkonfiguration und die Ausbauschritte pro Serviceausprägung für Openshift/Rancher sind in der folgenden Tabelle ersichtlich:

Tabelle: Agile Factory Worker Nodes

Leistungsmerkmal	Basic	Top	Premium
Anzahl Server 1*	2 (initial) bis 30	3 (initial) bis 30	3 (initial) bis 30
Service Level	Silber	Gold	Rhodium
Hardware-Profile 2*	P4/16 (initial) P8/32	P4/16 (initial) P8/32	P4/16 (initial) P8/32

	P8/64	P8/64	P8/64
Storage Klasse	Standard	Standard	Standard
Backup Retention Time	14 Tage	14 Tage	14 Tage

:::info

1* Je mehr Worker Node der Cluster besitzt, desto mehr Spares (Worker Node) müssen mit einberechnet werden.

- bis 16 Worker Node 1 Spare
- ab 16 Worker Node 2 Spares

2* Weiter Hardware Profile können bei Inventx angefragt werden.

:::

Persistent Storage

Für persistente Daten wird die Agile Factory im Initial Setup mit persistentem Storage (SVM) ausgestattet. Bei Bedarf kann der Kubernetes Cluster mit weiterem persistentem Storage ausgebaut werden.

Typischerweise wird der persistente Storage vom Service File Storage bezogen. Optional kann auch der Service Object Storage als persistenter Storage von extern genutzt werden.

Alle Storage Klassen sind georedundant. Folgende Storage Klassen werden zur Verfügung gestellt und können durch die applikationsspezifische Konfiguration eingesetzt werden.

Snapshots werden beim Erstellen entsprechender Kubernetes Ressourcen von der Applikation ausgelöst. Damit ist es möglich einen konsistenten Snapshot der Applikationsdaten zu erstellen.

Tabelle: Agile Factory Persistent Storage Klassen

Leistungsmerkmal	**Beschreibung**	**Storage Klassen**	**Reclaim Policy**	**Storage Klassen (deprecated)**
Block (Snapshot fähig)	Erstellen von Snapshot ist möglich per kubeApid	block-std	Retain	netapp-block-std-ndr-$CUSTOMER-$ENV
Block Economy	Keine Snapshot Möglichkeiten	block-eco	Retain	netapp-block-eco-ndr-$CUSTOMER-$ENV

File (Snapshot fähig)	Erstellen von Snapshot ist möglich per kubeApi	file-std	Retain	netapp-file-std-ndr-$CUSTOMER-$ENV
File Economy	Keine Snapshot Möglichkeiten	file-eco	Retain	netapp-file-eco-ndr-$CUSTOMER-$ENV

Empfehlungen zur Nutzung der Storage Klassen

Grundsätzlich sind die eco Storage Classes zu bevorzugen.

Tabelle: Agile Factory Empfehlungen persistem Storage

Storage Class	Beschreibung
Block	Stroge Klasse für alle SAN Workloads die eigene Datensicherung benötigen, ausgelöst durch Scheduler
Block Economy	Stroge Klasse für alle SAN Workloads die keine eigene Datensicherung benötigen
File	Stroge Klasse für alle NAS Workloads die eigene Datensicherung benötogen, ausgelöst durch Scheduler
File Economy	Stroge Klasse für alle NAS Workloads die keine eigene Datensicherung benötigen. Diese Storage Class ist im Cluster als default markiert

:::note

Weiter Storage Features

- Beim entfernen von PVCs und PV's mit der Reclaim Policy "Retain", wird das Volume im Backend erst nach 14 Tagen gelöscht. Das wieder bereitstellen des Volums muss per Generic Request bestellt werden
- Das Autoscaling der PVCs die eine File Storage Class nutzen, werden bei einem Schwellwert von 79% automatisch erweitert. Die Erweiterung ist abhängig von der Ausgansgrösse des PVC. Diese Prüfung der Nutzung, wird alle 5 Minuten durchgeführt.

:::

Load Balancer

Um Anwendungen im Cluster resilient aufbauen zu können, ist der Einsatz eines Layer 7 Load Balancer oder einer Web Application Firewall zwingend notwendig.

Web Application Firewall

Um Anwendungen im Cluster resilient aufbauen zu können, ist der Einsatz einer Web Application Firewall oder eines Layer 7 Load Balancer zwingend notwendig.

:::note

Gegenüber einem Load Balancer bietet eine Web Application Firewall zusätzlicher Schütz vor unerwünschten Anfragen auf Anwendungen.

:::

Server Proxy

Damit Anwendungen ins Internet (ausgehender Verkehr) kommunizieren können, ist die Verwendung vom Inventx Server-Proxy zwingend. Siehe dazu unseren Service Server Proxy.

Im Initial Setup wird definiert ob ein private- oder shared Server Proxy genutzt wird im Cluster.

Kubernetes Cluster Management

Die Kubernetes Cluster werden zentral mit einer der Cluster-Management Systeme Openshift/Rancher oder AnyCloudK8s verwaltet. Im Initial Setup wird mit dem Kunde definiert, welches Produkt eingesetzt wird.

Das Kubernetes Cluster Management beinhaltet im wesentlichem das monatliche Patchen sowie das Updaten/Upgraden nach Bedarf der gesamten Plattform.

Communication Management

Inventx stellt sicher, dass Anwendungen innerhalb des Clusters standardmässig nicht miteinander kommunizieren können. Auf Wunsch kann der Kunde die Kommunikation unterhalb der Anwendungen mit einer SSL-Verschlüsselung zulassen. Die SSL-Verschlüsselung wird durch ein self-signed Zertifikat sichergestellt.

Permission Management

Über die Authentication Authorization Infrastructure (AAI) und dem LDAP Operator kann ein individuelles RBAC-Konzept umgesetzt werden. Dazu werden vom Kunde definierten AD-Gruppen und Kubernetes Cluster Rollen miteinander verlinkt.

:::caution

Damit Inventx beim Initial Setup alle Einrichtungen vornehmen kann, muss der Kunde folgende Informationen zur Verfügung stellen:

- gewünschte AD-Gruppen

- ein AD Read Only Benutzer
- Schlüsselmaterial für LDAPS

:::

Monitoring (logs & metrics)

Während der Betriebszeit wird der Container Service von Inventx fortlaufend maschinell überwacht. Allfällige Events werden protokolliert, an die entsprechende Supportorganisation weitergeleitet und während der Servicezeiten bearbeitet.

Für alle Komponenten der Agile Factory welche Inventx verantwortet, werden Logs zentral gesammelt, ausgewertet und beim Erkennen von Problemen entsprechende Massnahmen durch Inventx ergriffen.

:::note

Die Logs werden während 90 Tag aufbewahrt.

:::

AnyCloudK8s

AnyCloudK8s ist ein vielseitiger, agnostischer Container-Plattform-Service, der aus einer Vielzahl von Komponenten besteht. Diese Komponenten werden optimal miteinander verbunden, um eine effiziente und branchenspezifische DevOps-Umgebung bereitzustellen. Inventx stellt dabei alle Komponenten und deren Verbindungen gemäss Best Practices bereit und betreibt diese. Es besteht jedoch auch die Möglichkeit, dass Kunden einzelne Komponenten selbst bereitstellen.

Mit AnyCloudK8s können Unternehmen cloud-native Anwendungen effizient erstellen, verwalten und skalieren – einfach und unkompliziert. Die Plattform bietet maximale Flexibilität, unabhängig davon, welchen Cloud-Anbieter Sie verwenden.

Dank der umfassenden Verwaltung aller Komponenten durch Inventx werden Kunden massgeblich entlastet. Entwickler können sich vollständig auf die Geschäftslogik und Eigenentwicklungen konzentrieren, ohne sich mit der Infrastruktur befassen zu müssen.

Zusätzlich steht AnyCloudK8s im ix.Portal als Selfservice zur Verfuegung – inklusive einfacher Bereitstellung und Verwaltung der Umgebung direkt übers Portal.

Die Bestellung kann etwas Zeit in Anspruch nehmen, da die Netzwerkbereitstellung noch nicht vollständig End-to-End automatisiert ist. Sobald das Netzwerk verfügbar ist, wird der Cluster automatisch bereitgestellt.

:::info

Dem Service AnyCloudK8s liegt der ix.Cloud standard Service Level zugrunde und die Worker Nodes der jeweiligen Ausführungen **Silber** und **Rhodium** legen den gültigen SLA fest.

Für den Wiederanlauf des AnyCloudK8s muss zusätzlich zum standard Service Level mit einem Uplift von 1 Stunden gerechnet werden.

:::

Service Architektur

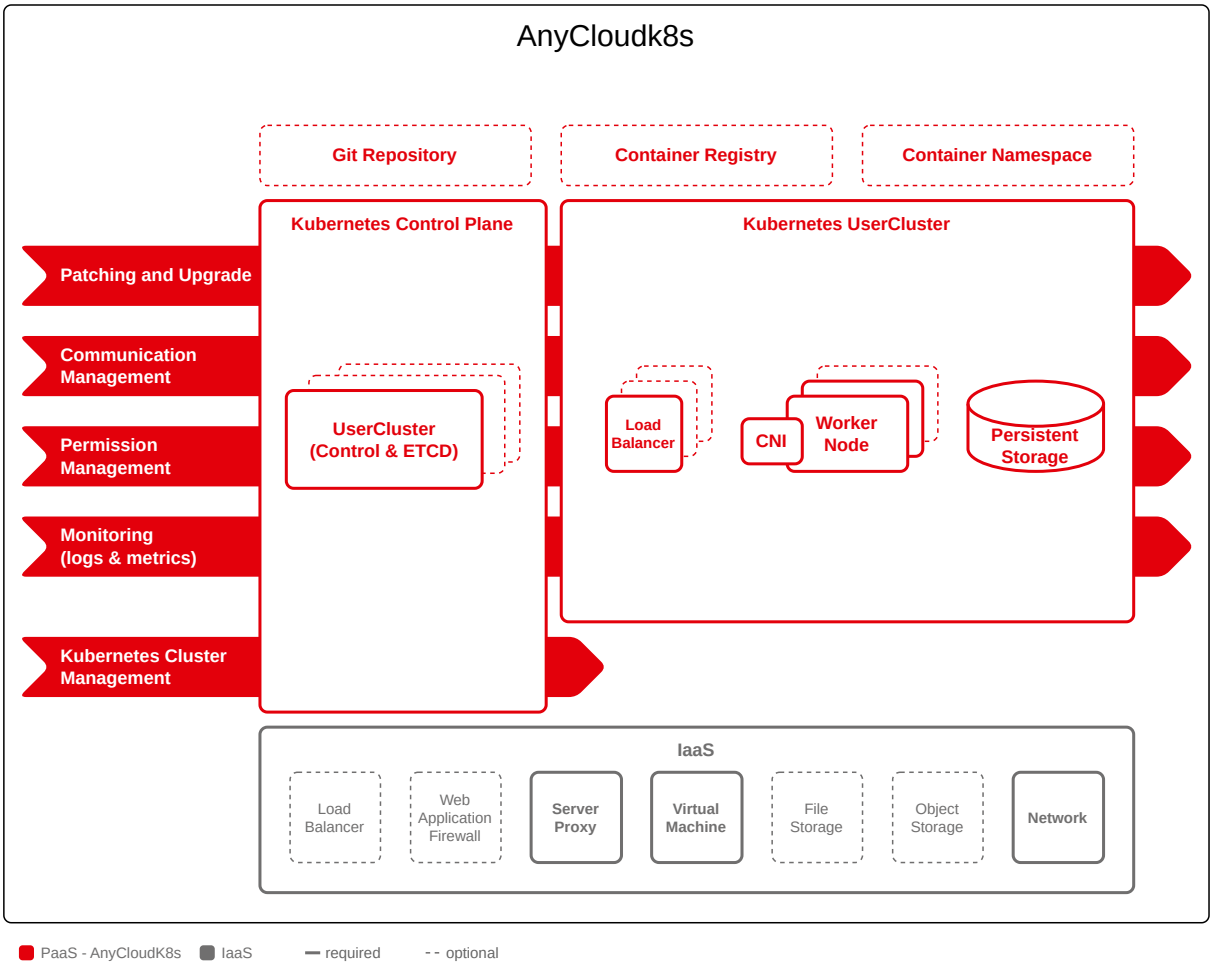


Bild: Service Architektur für AnyCloudK8s

Service Umfang

Tabelle: AnyCloudK8s Service Umfang

Leistungsmerkmal	Basic	Premium
IT Grundschutz	■	■
Initiales Setup	■	■

Git Repository	☐	☐
Container Registry	☐	☐
Container Network	■	■
Cluster Control Plane	■	■
Worker Pool	■	■
Worker Node	■	■
Persistent Storage	■	■
Load Balancer	■	■
Web Application Firewall	☐	☐
Server Proxy	■	■
Kubernetes Cluster Management	■	■
Communication Management	■	■
Permission Management	■	■
Monitoring (logs & metrics)	■	■
Cluster Network Interface	■	■

IT-Grundschutz

Patching/Upgrade Interval

Tabelle: AnyCloudK8s Patching/Upgrade Interval

Wochen Tag	Uhrzeit
Am Freitag nach dem zweiten Montag im Monat	02:00-06:00 Uhr

Hardening

- Die Vorgaben wurden im ATSB geprüft und abgenommen
- Diese werden durch die Automatisierung mit Gitops umgesetzt

Marware-Schutz

Alle Container-Images werden in der Container Registry auf Sicherheitslücken und Schwachstellen gescannt.

Configuration Management

Das Asset Mgmt wird im GitOps und CR's (ix.Cloud Operatoren) sichergestellt

Service Optionen

Nachfolgend sind die einzelnen Komponenten der AnyCloudK8s im Detail beschrieben. Teils Komponenten sind zwingend notwendig und teils optional. Dies ist in der oberen Tabelle AnyCloudK8s Service Umfang ersichtlich.

Initiales Setup

Bei der Bestellung eines neuen Clusters kann die Bereitstellung bis zu 5 Tage dauern. Der Service ist aktuell noch nicht vollständig automatisiert, da das Netzwerk als Managed Service beim zuständigen Team separat beauftragt wird. Sobald das Netzwerk bereitsteht, wird der Cluster anschliessend vollautomatisiert bereitgestellt.

Nach der initialen Bereitstellung sind alle weiteren Service-Funktionen vollautomatisiert verfügbar, z.B. Patchen/Updates sowie das Management der Worker Pools (Erweitern, Modifizieren, Verkleinern).

Git Repository

Für die Versionierung von Code der Deployments ist in der AnyCloudK8s zwingend ein Git Repository notwendig. Diese kann durch den Kunde oder durch Inventx bereitgestellt werden.

Wenn das Git Repository durch Inventx gestellt wird, dann erhält der Kunde im Inventx eigenen Git einen autorisierten Benutzer, mit dem Projekte erstellt, verwaltet und gelöscht werden können. Wird das Git Repository vom Kunde bereitgestellt, so wird im Initial Setup die Kommunikation zwischen den Komponent aufgebaut und sichergestellt.

Container Registry

Die AnyCloudK8s benutzt für sämtliche Deployments im Kubernetes Cluster eine Container Registry. Diese Komponente kann durch den Kunden oder die Inventx bereitgestellt werden.

Wenn Inventx die Container Registry stellt, dann wird der Service Container Registry eingesetzt. In diesem Fall ist Inventx für einen störungsfreien Betrieb dieser wichtigen Komponente verantwortlich.

Wird die Container Registry vom Kunde bereitgestellt, so wird im Initial Setup die Kommunikation zwischen den beiden Komponenten Kubernetes Cluster und Container Registry sichergestellt. In diesem Fall ist der Kunde gleichermassen mitverantwortlich, dass die Kommunikation zwischen den Komponenten störungsfrei läuft.

Container Network

Für die AnyCloudK8s Umgebung benötigt es noch ein Subnetz. Durch die Grösse des Netzes wird definiert, wie viele Worker Nodes dem Cluster maximal hinzugefügt werden kann.

:::note

Bitte beachten, dass der gesamte IP-Range nicht für die Worker Nodes verfügbar ist. In diesem Netzwerk werden zusätzliche Management- und PaaS-Komponenten bereitgestellt, die für die Service-Erbringung essentiell sind. Diese Komponenten benötigen eigene IP-Ressourcen, wodurch der nutzbare Bereich für die Worker Nodes entsprechend eingeschränkt wird.

:::

Die Netzwerkgrösse sind in drei T-shirt size vordefiniert small(/27), middle(/26) und large(/25)

Tabelle: Netzwerkgrösse

T-shirt size	Maximale Worker Node
Small	10
Medium	26
Large	58

Zusätzlich wir eine DHCP-VM deployt, welche die Verwaltung der IP-Adressen im Container-Netzwerk übernimmt. Dieser Service wird automatisch bei der Bereitstellung des Netzwerks für AnyCloudK8s bereitgestellt und vollständig konfiguriert. Dadurch wird sichergestellt, dass alle Komponenten nahtlos miteinander kommunizieren können und die Netzwerkressourcen effizient verwaltet werden

Die **valid-lifetime = lease time** ist fix auf **3600 Sekunden** eingestellt.

Cluster Control Plane

Die Control Plane dient der Verwaltung des Kubernetes Clusters. Über sie kann via der Kubernetes API auf den Cluster sowie darauf installierten Anwendungen verwaltet werden. Sie dient als Steuerungsebene des Clusters und verwaltet ständig den Ist-Zustand des Cluster in den definierten Soll-Zustand. Die Control Plane koordiniert alle Aufgaben einschliesslich der Planung und Skalierung von Anwendungen.

Um eine hohe Fehlertoleranz und Ausfallsicherheit zu gewährleisten, wird die Control Plane auf einem Seed Kubernetes Cluster bereitgestell.

Die benötigten Ressourcen werden dynamisch auf IaaS-Ebene sichergestellt.

Tabelle: Management Nodes AnyCloudK8s

Leistungsmerkmal	Basic	Premium
Seed Cluster	Lokal-Redundanz	Geo-Redundanz
Service-Level	Silber	Rhodium
Storage-Klasse	High Performance	Standard
Backup Retention Time	14 Tage	14 Tage

Woker Pool

Ein Cluster kann aus einem oder mehreren Worker Pools bestehen. Pro Worker Pool definieren Sie einen einheitlichen Worker Node (z.B. CPU/RAM-Profil) und können so unterschiedliche Anforderungen innerhalb desselben Clusters gezielt abdecken.

Wann mehrere Worker Pools sinnvoll sind

Man nutzt mehrere Worker Pools, um unterschiedliche Worker Node – etwa allgemeine Knoten und solche mit viel Arbeitsspeicher – in einem Cluster zu kombinieren und Workloads entsprechend zu verteilen. Mithilfe von Taints und Tolerations sorgt man dafür, dass bestimmte Workloads nur auf dafür vorgesehenen Knoten laufen.

Gezielte Platzierung per Pod-Spezifikation: Steuern Sie die Planung über nodeSelector (oder bei Bedarf Node Affinity), damit Pods auf die passenden Worker Pools bzw. Worker Node eingeplant werden.

Worker Pools erweitert managen

Worker Pools können im Portal nicht nur erstellt und erweitert, sondern auch gezielt angepasst werden. So lassen sich unterschiedliche Worker Node, Hardware-Profile und Scheduling-Anforderungen innerhalb eines Clusters sauber trennen und über den gesamten Lebenszyklus steuern.

ERWEITERTE VERWALTUNG FÜR WORKER-POOL-ANPASSUNGEN

Mit den erweiterten Funktionen können Sie Worker Pools an derzeitige Anforderungen anpassen, ohne das gesamte Cluster neu aufzusetzen:

- Worker Pools erweitert modifizieren Ändern Sie pool-spezifische Einstellungen wie Worker Node/Flavor, Ressourcenprofil, Metadaten sowie Scheduling-Parameter. So richten Sie Workloads auch nachträglich auf passende Node-Profile aus.
- Worker Pools verkleinern (Scale-down) Reduzieren Sie die Anzahl Worker Nodes eines Pools kontrolliert. Dabei werden Nodes geordnet aus dem Pool entfernt, um Kapazität zu senken und Kosten zu optimieren (z.B. nach Lastspitzen oder nach Projektabschluss).
- Taints / Labels / Annotations pro Worker Pool definieren Hinterlegen Sie Regeln und Metadaten direkt am Worker Pool:

- Labels für gezieltes Scheduling (z.B. nodeSelector / Affinity)
- Taints um Pools für spezielle Workloads zu reservieren (z.B. GPU, High-Memory) und nur per Tolerations zuzulassen
- Annotations für zusätzliche Steuerungs- und Integrationsinfos (z.B. Betrieb, Monitoring, Automatisierung)

Worker Node

Der Worker Node ist eine Virtual Machine, auf dem die Anwendungen ausgeführt werden und der vom Management Node gesteuert wird.

Anders als beim Management Node können die Hardware-Ressourcen beim Worker Node ausgewählt und angepasst werden. Entweder man fügt weitere Worker Nodes im Kubernetes Cluster hinzu (scale-out) oder man ändert das Hardware-Profile bei den bestehenden Worker Nodes (scale-up).

Ein Ausbau kann durch den Worker Pool selbständig getätigt werden.

Tabelle: Virtual Machine Hardware-Profile Standard 1*

Standard		**RAM in GB**								
		4	**8**	**16**	**24**	**32**	**64**	**96**	**128**	**256**
Anzahl vCPU	**2**	-	-	-	-	-	-	-	-	-
	4	-	■	■	-	■	■	-	-	-
	6	-	-	-	-	-	-	-	-	-
	8	-	-	■	-	■	■	-	■	-
	12	-	-	-	-	-	-	-	-	-
	16	-	-	-	-	■	■	-	■	■
	24	-	-	-	-	-	-	-	-	-
Systemdisk		FlatCar: 80 GB								

:::info

Der Unterschied zu AgileFactory wird bei AnyCloudK8s zuerst eem Cluster ein Worker Node beigefügt, somit müssen keine zusätzliche Spare Nodes bereitgestellt werde. Der Ausbau ist im Backend automatisiert und kann schneller bereitgestellt werden.

1* Weiter Hardware Profile können bei Inventx angefragt werden.

:::

Persistent Storage

Für persistente Daten wird die AnyCloudK8s im Initial Setup mit persistem Storage (SVM) ausgestatet. Es kann pro Cluster nur ein persister Storage im Subnetz bereitgestellt werden.

Typischerweise wird der persistente Storage vom Service File Storage bezogen. Optional kann auch der Service Object Storage als persistenter Storage von extern genutzt werden.

Bei AnyCloudK8s werden die Storage Klassen gemäss SLA des Cluster automatisch bereitgestellt

Tabelle: AnyCloudK8s persistem Storage

Leistungsmerkmal	Basic	Premium
Cluster	Lokal-Redundanz	Geo-Redundanz
Persistem Storage	Lokal-Redundanz	Geo-Redundanz

Folgende Storage Klassen werden zur Verfügung gestellt und können durch die applikationsspezifische Konfiguration eingesetzt werden.

Tabelle: AnyCloudK8s Persistent Storage Klassen

Leistungsmerkmal	Beschreibung	Storage Klassen	Reclaim Policy
Block (Snapshot fähig)	Erstellen von Snapshot ist möglich per kubeApid	block-std	Retain
Block Economy	Keine Snapshot Möglichkeiten	block-eco	Retain
File (Snapshot fähig)	Erstellen von Snapshot ist möglich per kubeApi	file-std	Retain
File Economy	Keine Snapshot Möglichkeiten	file-eco	Retain

:::info

Snapshots werden beim Erstellen entsprechender Kubernetes Ressourcen von der Applikation ausgelöst. Damit ist es möglich einen konsistenten Snapshot der Applikationsdaten zu erstellen.

:::

Empfehlungen zur Nutzung der Storage Klassen

Grundsätzlich sind die eco Storage Classes zu bevorzugen.

Tabelle: AnyCloudK8s Empfehlungen persistem Storage

Storage Class	Beschreibung
Block	Stroge Klasse für alle SAN Workloads die eigene Datensicherung benötigen, ausgelöst durch Scheduler
Block Economy	Stroge Klasse für alle SAN Workloads die keine eigene Datensicherung benötigen
File	Stroge Klasse für alle NAS Workloads die eigene Datensicherung benötogen, ausgelöst durch Scheduler
File Economy (default)	Stroge Klasse für alle NAS Workloads die keine eigene Datensicherung benötigen. Diese Storage Class ist im Cluster als default markiert

:::note

Weitere Storage Features

- Beim entfernen von PVCs und PV's mit der Reclaim Policy "Retain", wird das Volume im Backend erst nach 14 Tagen gelöscht. Das wieder bereitstellen des Volums muss per Generic Request bestellt werden
- Das Autoscaling der PVCs die eine File Storage Class nutzen, werden bei einem Schwellwert von 79% automatisch erweitert. Die Erweiterung ist abhängig von der Ausgansgrösse des PVC. Diese Prüfung der Nutzung, wird alle 5 Minuten durchgeführt.

:::

Load Balancer

Um Anwendungen im Cluster resilient aufbauen zu können, ist der Einsatz eines Layer 4/7 Load Balancer oder einer Web Application Firewall zwingend notwendig.

Bei der Bereitstellung eines AnyCloudK8s-Clusters wird **kein Load Balancer automatisch** installiert oder konfiguriert. Wenn ein Load Balancer benötigt wird, definiert der Kunde diesen **selbst im Cluster per Manifest** (z.B. als Service vom Typ LoadBalancer, gemäss bereitgestellter *Vorlage*).

```
apiVersion: v1
kind: Service
metadata:
  name: loadbalancer-sample
  annotations:
    lb.ixcloud.ch/enable: ""
```

```
    lb.ixcloud.ch/retain: ""
    lb.ixcloud.ch/fqdn: "only-test.[FQDN]"
    lb.ixcloud.ch/loadBalancingAlgorithm:
"LeastConnections"
    lb.ixcloud.ch/maxThroughput: "10"
    lb.ixcloud.ch/costCenter: "[Cost124]"
spec:
  type: LoadBalancer
  selector:
    app: my-app                              # muss zu den
Pod-Labels passen
  ports:
  - name: http
    port: 80
    targetPort: 8080
    protocol: TCP
```

Sobald der Load Balancer im Cluster definiert ist, sorgt unsere Automatisierung dafür, dass die **Backend-Konfiguration bei Änderungen** (z.B. bei einer Anpassung der IP-Adresse oder Patchen/Upgrade) **automatisch** aktualisiert wird.

:::info

Merkmale

- Automatisierte Anpassungen: Änderungen an Backend-Konfigurationen erfolgen ohne manuellen Eingriff.
- Skalierbarkeit: Pro Cluster können mehrere Load Balancer gleichzeitig verwaltet werden, um komplexere Anforderungen zu unterstützen.

:::

Diese Automatisierung sorgt für eine effiziente und fehlerfreie Verwaltung der Netzwerkkomponenten und erleichtert die Skalierung und Erweiterung der Cluster-Infrastruktur.

Web Application Firewall

Um Anwendungen im Cluster resilient aufbauen zu können, ist der Einsatz einer Web Application Firewall oder eines Layer 7 Load Balancer zwingend notwendig.

:::note

- Gegenüber einem Load Balancer bietet eine Web Application Firewall zusätzlicher Schütz vor unerwünschten Anfragen auf Anwendungen.
- Wenn ein **L7-Load-Balancer** oder eine **WAF** benötigt wird, stellen Sie bitte zuerst einen **L4-Load-Balancer** per Manifest im Cluster bereit. Anschliessend kann dieser über einen **Generic Request** entsprechend zu L7 bzw. WAF umfunktioniert werden.

:::

Server Proxy

Damit Anwendungen innerhalb des AnyCloudK8s-Clusters mit dem Internet kommunizieren können (ausgehender Verkehr), ist die Nutzung des Inventx Server-Proxys zwingend erforderlich. Weitere Details hierzu finden Sie in der Dokumentation unseres Service Server Proxy.

Bei der Bereitstellung eines AnyCloudK8s Cluster wird immer nur der shared Server Proxy genutzt. Diese stellt sicher, dass alle ausgehenden Verbindungen den Sicherheits- und Compliance-Anforderungen von Inventx entsprechen.

Kubernetes Cluster Management

Die Kubernetes-Cluster von AnyCloudK8s werden zentral durch Inventx verwaltet. Ein zentrales Merkmal dieses Ansatzes ist die Entkopplung der Control Plane aus dem Cluster. Dadurch erhält der Besteller Admin-Rechte auf dem Cluster, während Inventx die übergreifende Verwaltung sicherstellt.

Inventx stellt regelmässig unterstützte und aktuelle Patches sowie neue Kubernetes-Versionen zur Verfügung, die vom Kunden bei Bedarf für Upgrades genutzt werden können. Ankündigungen zu neuen Versionen sowie Abkündigungen von bestehenden Versionen erfolgen monatlich über Release-Notes gemäß dem ixCloud-Prozess.

Dieses Management-Modell gewährleistet die Sicherheit, Stabilität und Aktualität der Kubernetes-Umgebung, während der Kunde maximale Flexibilität für die Verwaltung seines Clusters behält.

Communication Management

Inventx stellt sicher, dass Anwendungen innerhalb des Clusters standardmässig nicht miteinander kommunizieren können. Auf Wunsch kann der Kunde die Kommunikation unterhalb der Anwendungen mit einer SSL-Verschlüsselung zulassen. Die SSL-Verschlüsselung wird durch ein self-signed Zertifikat sichergestellt.

Permission Management

Wie im Kubernetes Cluster Management beschrieben, erhält der Besteller Admin-Berechtigungen für den bereitgestellten Cluster. Diese Berechtigungen ermöglichen dem Kunden volle Kontrolle und Flexibilität bei der Verwaltung und Nutzung des Clusters.

Über das Portal kann die entsprechende Kubeconfig unkompliziert heruntergeladen werden. Mit dieser Konfigurationsdatei können Admins direkt über ihre bevorzugten Tools (z. B. kubectl) auf den Cluster zugreifen.

Monitoring (logs & metrics)

Während der Betriebszeit wird der Container Service von Inventx fortlaufend maschinell überwacht. Allfällige Events werden protokolliert, an die entsprechende Supportorganisation weitergeleitet und während der Servicezeiten bearbeitet.

Für alle Komponenten der AnyCloudK8s welche Inventx verantwortet, werden Logs zentral gesammelt, ausgewertet und beim Erkennen von Problemen entsprechende Massnahmen durch Inventx ergriffen.

:::note

Die Logs werden während 90 Tag aufbewahrt

:::

Bei der Bereitstellung eines Clusters wird im Portal automatisch eine Time Series Database unter der gleichen Subscription eingerichtet. Die Metriken des Clusters werden in diese Datasource übertragen.

Die Datasource dient zur Speicherung und Analyse der Metriken, was eine kontinuierliche Überwachung und Optimierung des Clusters ermöglicht.

Diese Integration stellt sicher, dass alle relevanten Metriken zentral gesammelt und bei Bedarf für Monitoring- oder Reporting-Zwecke genutzt werden können.

Cluster Network Interface

Die Cluster können standardmässig mit dem Container Network Interface (CNI) **Canal** oder **Cilium** bereitgestellt werden.

Canal kombiniert die Funktionalitäten von Flannel (für das Netzwerk-Overlay) und Calico (für Netzwerk-Sicherheitsrichtlinien), um ein robustes und flexibles Netzwerk-Setup für Kubernetes-Cluster bereitzustellen.

Cilium basiert auf eBPF und ermöglicht eine performante, skalierbare und sicherheitsorientierte Netzwerkimplementierung. Neben der Pod-zu-Pod-Konnektivität unterstützt Cilium granulare Network Policies sowie erweiterte Observability-Funktionen.

Container Namespace

Der Container Namespace Service vereinfacht die Nutzung der Agile Factory und AnyCloudK8s. Alle benötigten Clusterbase Berechtigungen für Namespace werden in diesem Service bereitgestellt.

Namespaces ist in Kubernetes zentral und ein Key-Element. Namespace ermöglichen es dem Entwickler, sein Projekt modular aufzubauen und bestimmte Aspekte in eine eigene Datei auszulagern. So können sie ihre Applikationen modernisieren und die Komplexität verringern, wodurch der Entwickler sich auf das wesentliche fokussieren kann.

Service Architektur

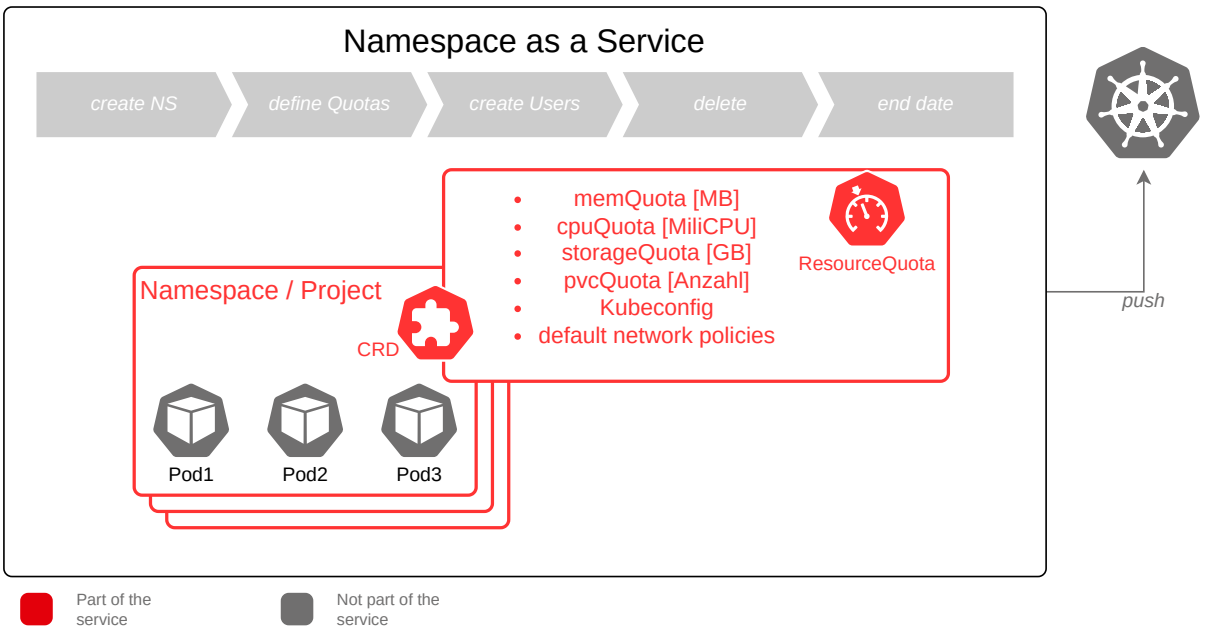


Bild: Namespace Service Architektur

Service Umfang

Tabelle: Namespace Service Umfang

Leistungsmerkmal	Rancher	OpenShift	AnyCloudK8s
Initiales Setup	□	□	□
Target Destination	■	■	■
Network Policy	■	■	■
Quotas	■	■	■
KubeConfig	■	■	■
Annotations/Labels	■	■	■

:::info Um sicherzustellen, dass systemkritische Namespaces geschützt bleiben, haben wir einen Blacklist-Filter eingeführt. Dieser stellt sicher, dass bestimmte vom Cluster genutzte Namespaces nicht

bestellt werden können. Die folgenden Namespaces sind davon betroffen:

openshift openshift- ; kube- ; trident ; argocd ; cert-manager ; patch-operator ; patch-automation ; conjur ; k8s-operators ; ix-ocpbackup-system ; ix-aai ; alertmanager-zabbix-webhook ; collectorforopenshift ; cerberus ; kyverno ; aqua :::

Service Optionen

Nachfolgend sind die einzelnen Komponenten des Container Namespace im Detail beschrieben.

Inital Setup

Die Basis für den Einsatz eines Container Names Space bildet eine bestehende Agile Factory oder AnyCloudK8s. Die Subscription welche bei der Bestellung genutzt wird, muss vorab aufgeschaltet werden auf dem Target Destination.

Für die Freigabe der verfügbaren Target Destinationen sowie sämtliche spätere Änderungen sind mit einem "Generic Request" zu beauftragen

Target Destination

Es kann pro Subscription definiert werden, welche Target Destinationen verwendet werden können. So kann spezifisch definiert werden welche User auf welcher Agile Factory oder AnyCloudK8s einen Container Namespace respektiv eine Applikation deployen darf.

Network Policy

Beim Erstellen eines Namespace auf der Target Destination, werden vordefinierte Network Policy gesetzt. Diese müssen bei einem Deploying der Applikation gemäss Anforderungen der Applikation angepasst werden.

Auflistung der von Inventx gesetzten Netzwerk Policy's

- Allow Namespace
- Allow DNS
- Default denyAll

Quotas

Beim Erstellen eines Namespaces müssen die Quotas definiert werden. Dadurch wird die Voraussetzung geschaffen, dass Applikationen resilient auf dem entsprechenden Cluster betrieben werden können. Mittels Quotas wird sichergestellt, dass eine Applikation nicht alle Cluster-Ressourcen ausschöpfen und andere Applikationen negativ beinträchtigen kann.

Folgende Quotas müssen bei er Erstellung angegeben werden:

Tabelle: Container Namespace Quotas

Leistungsmerkmal	Beschreibung
Memory	Memory Quota in MB auf dem Namespace
CPU	CPU Quota in Millicpu auf dem Namespace
Storage	Storage in GB auf dem Namespace
PVC	Maximale Anzahl PVC's im Namespace

Diese Quotas haben alle einen minimal Wert definiert, die Definitionen sind in der untern Tabelle ersichtlich:

:::note

Es gibt Applikationen welche mit den ResourceQuotas oder Networkpolicy vom Namespace nicht umgehen können. Diese können beim bestellen des Namespace deaktivieren werden

:::

Tabelle: Container Namespace Quotas mindes Wert

Quota	Mindestwert
Memory	> 256MB
CPU	> 200m
Storage	>= 1
PVC	>0

Der maximale Wert ist nicht limitiert, somit liegt es im Ermessen des Kunden, diesen zu definieren gemäss den vorhanden Ressourcen auf der Agile Factory oder AnyCloudK8s.

:::note

Die Memory Quota muss gedacht ausgewählt werden, da es die Applikationen zum Abstürzen bringen kann, wenn dieser zu knapp gewählt wird

:::

KubeConfig

Jeder Container Namespace hat einen Service Account. Dieser Account kann mit unterschiedlicher Berechtigung bestellt werden. Entweder als Admin Service Account oder als Viewer. Zusätzlich zum Service Account, wird auch ein Token erstellt, welches nach der Ablaufzeit des definierten "Time to Live" abläuft. Die Definition, ob die Berechtigung Admin oder Viewer sein soll, kann nur bei der Erstellung des Container Namespace eingestellt werden.

Das KubeConfig kann angezeigt und kopiert werden. Sollte die KubeConfig abgelaufen sein (erreichen der Time to Live) kann es erneuert werden. So ist sichergestellt, dass die Berechtigung auf den Namespace nicht immer die gleichen Credentials hat.

:::note

Der Container Namespace kann nur auf dem Target Cluster gelöscht werden, wenn er mit Admin Rechte bestellt wurde

:::

Annotations/Labels

Das Feature ermöglicht das Setzen von Labels und Annotations beim Erstellen und Verwalten von Namespaces, was die Automatisierung und Transparenz im Cluster fördert.

Labels ermöglichen eine klare und strukturierte Kategorisierung von Namespaces, z. B. nach Teamzugehörigkeit, Umgebung oder Applikationstyp. Annotations bieten die Möglichkeit, zusätzliche Metadaten wie Beschreibungen, Verantwortlichkeiten oder betriebsrelevante Informationen zu hinterlegen.

:::caution

Der Key eines Labels oder einer Annotation kann nach dem Erstellen nicht mehr geändert werden. Der zugehörige Value hingegen lässt sich jederzeit anpassen.

:::

Splunk Index

Die Splunk Index Erstellung ist ein zentraler Ort für die Verwaltung von Splunk-Indizes, um eine effiziente und strukturierte Verwaltung zu gewährleisten. Der Service bietet die Möglichkeit, einen Splunk Index zu erstellen, der verschiedene Service-Optionen unterstützt. Es können sowohl technische als auch organisatorische Informationen nach der Erstellung der Indizes abgerufen werden.

Verfügbare Service-Optionen

Tabelle: Splunk Indexe Service-Optionen

Service-Option	Service-Optionsbeschreibung
Type	Splunk Index oder Splunk Summary
Stage	Produktion oder Testumgebung
Online Retention	Aufbewahrungszeit in Tagen. Definiert, wie lange die Logs in dem Index verbleiben.
Description	Beschreibung des Index oder Summary. In der Regel sollte "Index" ausgewählt werden. Der Zweck von "Summary" ist es, Daten aus bereits bestehenden Indices zu filtern, zu aggregieren und zu speichern.

Verfügbare Meta-Informationen

Tabelle: Splunk Indexe Meta-Informationen

Meta-Information	Meta-Informationsbeschreibung
Subscription	Die ix.Cloud Subscription, in der der Index oder Summary erstellt wurde
Organizational Unit	Die Organisationseinheit, der der Index oder Summary zugeordnet ist
Cost Center	Das Cost Center für die Verrechnung
Owner	Die verantwortliche Person oder das Team
Tags	Schlagwörter oder Labels zur Kategorisierung
Custom Properties	Zusätzliche benutzerdefinierte Eigenschaften

---

Enterprise Streaming Service

Enterprise Streaming Service – vollständig verwaltete Event Streaming Plattform der ix.Cloud für die Echtzeit-Verarbeitung von Events, Transaktionen und Zustandsänderungen.

:::info Status: Alpha Der Enterprise Streaming Service ist ein Community Service der ix.Cloud. :::

Er stellt eine vollständig verwaltete Event Streaming Plattform bereit, die von mehreren Kunden gemeinsam genutzt wird (Shared Service). Die Mandantentrennung wird durch die Plattform auf Topic-

Ebene sichergestellt.

Der Service wird in den Rechenzentren der Inventx betrieben. Der Service erfüllt die regulatorischen Anforderungen an Datenhaltung, Mandantenisolation und Auditierbarkeit.

Die folgenden Leistungen werden durch Inventx erbracht und sind im Service enthalten.

Leistungsumfang Inventx

Managed Streaming Cluster

Inventx betreibt und überwacht die gesamte Streaming-Infrastruktur. Dazu gehören Broker-Management, Cluster-Skalierung, Rolling Upgrades, Patching und Kapazitätsplanung. Der Kunde nutzt die Plattform, ohne sich um den Betrieb kümmern zu müssen.

Schema Registry

Inventx stellt eine zentrale Schema Registry bereit. Diese ermöglicht es Producern und Consumern, Schemas zentral zu verwalten und die Kompatibilität zwischen Anwendungen sicherzustellen.

Unterstützte Schema-Typen:

- Avro
- Protobuf
- JSON Schema

Zugriffskontrolle & Mandantentrennung

Jedes Topic des Kunden beginnt mit dem Kundenkürzel, welches im System der Inventx festgelegt ist. Innerhalb dieses Prefixes können weitere Topic-Gruppen erstellt werden, um die Zugriffskontrolle granularer zu gestalten. Berechtigungen werden pro User und Topic-Prefix vergeben.

Unterstützte Authentifizierungsmethoden:

- SASL/SCRAM
- mTLS
- OAuth

Die Erfassung und Verwaltung von Clients erfolgt durch Inventx. Der Kunde erhält Reports, mit denen er die Berechtigungen innerhalb seiner Topics einsehen und überprüfen kann.

Topic Management

Nach der Vergabe eines Topic-Prefixes und der zugehörigen Berechtigungen können innerhalb dieses Bereichs Topics erstellt und konfiguriert werden:

- Direkt über die Kafka Admin API (sofern entsprechende Berechtigungen vorliegen)
- Über den Inventx Self-Service (geplant)

Konfigurierbare Topic-Einstellungen:

Einstellung	Standard	Maximum
Retention Time	7 Tage	30 Tage
Partition Count	12	96

Fest vorgegebene Einstellungen:

Einstellung	Wert
Replication Factor	3

Monitoring & Alerting

Inventx überwacht Cluster Health, Throughput und Partitionsverteilung in Echtzeit. Proaktives Alerting erfolgt bei Anomalien und SLA-relevanten Schwellenwerten.

Security

Tabelle: Security

Art	Beschreibung
Encryption in Transit	Bei mTLS-Authentifizierung immer garantiert. Bei OAuth oder SASL/SCRAM muss die Verbindung über TLS aufgebaut werden.
Encryption at Rest	Sichergestellt über die Standard-Disk-Encryption der ix.Cloud.
Application-Level Encryption	Wird nicht durch den Service abgedeckt. Liegt in der Verantwortung der jeweiligen Applikation.

Topic Monitoring & Logs

Monitoring- und Log-Informationen für die eigenen Topics und Clients des Kunden werden über Reports bereitgestellt.

Interne Cluster- und Betriebslogs (z.B. Broker-/System-Logs) werden nicht bereitgestellt. Log-Forwarding in kundeneigene Systeme wird nicht unterstützt.

Aufbewahrung	Dauer

Online	90 Tage
Offline	2 Jahre

Verantwortung Kunde

Die folgenden Punkte liegen in der Verantwortung des Kunden.

Anbindung von Applikationen

Der Kunde ist verantwortlich für die Entwicklung, Konfiguration und den Betrieb seiner Producer- und Consumer-Applikationen. Dabei gelten folgende Rahmenbedingungen:

- Maximale Message-Grösse: 1 MB
- Topics müssen den zugewiesenen Topic-Prefix verwenden (der Applikationsname kann nicht frei gewählt werden)
- Connectors, die auf Shared-Ressourcen innerhalb des Clusters zugreifen (z.B. MirrorMaker 2), können nicht eingesetzt werden
- Die Kafka-Version wird durch den Enterprise Streaming Service vorgegeben
- Der Replication Factor ist fix und kann nicht beeinflusst werden

Netzwerkkonnektivität

Der Kunde stellt sicher, dass die Netzwerkkonnektivität zwischen seinen Consumer-/Producer-Applikationen und der Streaming-Plattform besteht (in Zusammenarbeit mit Inventx Network Services).

Schema-Registrierung

Schemas sind vor der Produktion in der Schema Registry zu registrieren.

Monitoring-Nutzung

Der Kunde nutzt die bereitgestellten Monitoring-Reports aktiv für die Überwachung seiner Topics und Kapazitäten.

Service Level Parameter (SLP)

Die Service Level Parameter orientieren sich am Leistungsübergabepunkt (LÜP) Plattform (PaaS) in der Stufe Platin.

Zeichenlegende

Folgendes Regelwerk gilt zu den Zeichen pro Spalte resp. Zeile in einer Tabelle:

- Die mit "■" gekennzeichnete Positionen sind im Basispreis gemäss separater Preisliste enthalten.
- Die mit "□" gekennzeichnete Positionen sind nicht im Basispreis enthalten, können aber optional dazu bestellt werden. Die Verrechnung erfolgt gemäss separater Preisliste.
- Die mit "-" gekennzeichneten Positionen sind nicht verfügbar.