xelon

Datenfalle Kubernetes?

Das müssen Schweizer Unternehmen über Datensicherheit mit Kubernetes wissen

Whitepaper

xelon

Inhalts-verzeichnis

Einleitung

Kubernetes hat sich in der IT-Welt als Standard für den Betrieb containerisierter Anwendungen etabliert. Auch in der Schweiz setzen immer mehr Unternehmen auf die Open-Source-Plattform. Doch besonders in regulierten Branchen wie Finanzdienstleistungen, Gesundheitswesen oder öffentlicher Verwaltung kommen vermehrt Bedenken rund um Datenhoheit, Informationssicherheit und die Einhaltung von Compliance-Vorgaben auf.

Wer mit besonders schützenswerten oder sensiblen Informationen arbeitet, sollte sicherstellen, dass die Daten in der Schweiz verarbeitet und gespeichert werden, um rechtliche Risiken durch ausländische Gesetze wie den US CLOUD Act zu vermeiden.

Schweizer Unternehmen, die auf Kubernetes setzen, stehen heute vor der Herausforderung, technologische Innovation und einfache Skalierbarkeit mit Datensicherheit zu verbinden. Der Standort der Infrastruktur ist nicht nur eine technische Entscheidung, sondern zunehmend auch ein strategischer Faktor für Vertrauen, Sicherheit und Compliance.

Hier findet ihr Einblicke in das Thema Datensicherheit mit Kubernetes und eine Schritt-für-Schritt-Anleitung, wie ihr innert weniger Minuten Kubernetes-Cluster in einer Schweizer IT-Infrastruktur aufsetzen könnt.

Was ist Kubernetes (K8s)?

Die Trend-Technologie Kubernetes automatisiert die Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen. Damit eignet sich K8s – wie Kubernetes auch genannt wird – ideal für den Betrieb von Microservices und Cloud-nativen Anwendungen.

Fun Fact #1

Die Abkürzung K8s kommt daher, dass zwischen dem 'K' und 's' von Kubernetes acht Buchstaben sind.

Das sind die wichtigsten Funktionen von Kubernetes:

1 Container-Orchestrierung

Kubernetes steuert und verwaltet Container, die in Umgebungen wie Docker ausgeführt werden. Das Open-Source-System hilft dabei, mehrere Container auf verschiedenen Hosts zu koordinieren.

2 Automatische Skalierung

K8s kann je nach Last automatisch die Anzahl der laufenden Container skalieren, um den Anforderungen gerecht zu werden.

4

3 Selbstheilung

Wenn ein Container abstürzt, startet Kubernetes ihn neu oder ersetzt ihn, um die Verfügbarkeit der Anwendung zu gewährleisten.

4 Lastverteilung

Kubernetes verteilt automatisch den Netzwerkverkehr auf mehrere Container, um eine optimale Leistung und Verfügbarkeit sicherzustellen.

5 Bereitstellung und Rollbacks

Mit Kubernetes sind schrittweise Updates von Anwendungen und bei Bedarf einfache Rollbacks möglich.

Fun Fact #2

Der Name Kubernetes stammt aus dem Griechischen und bedeutet «Steuermann», was die Rolle von Kubernetes als Koordinator und Verwalter von Container-Anwendungen widerspiegelt.

Kubernetes und Datensicherheit: Was passiert mit Unternehmens-daten?

Der Aufbau einer stabilen, hochverfügbaren Control Plane erfordert nicht nur fundiertes Know-how in Container-Orchestrierung, sondern bedeutet oftmals auch erheblichen Aufwand für Wartung, Sicherheitsupdates und Skalierung. Mit dem Xelon Kubernetes Service (XKS) erhalten Schweizer Unternehmen nun allerdings eine vollständig verwaltete Kubernetes-Lösung. Dabei behalten sie die **volle Kontrolle über das User-Erlebnis**, denn der XKS lässt sich unter dem eigenen Markennamen weiterverkaufen und in bestehende Service-Angebote integrieren.

Beim Aufsetzen oder Ausbau von Kubernetes gilt es, technische, rechtliche und organisatorische Aspekte zu berücksichtigen. Besonders wichtig ist dabei der **Standort der IT-Infrastruktur,** auf der Kubernetes betrieben wird. Mit dem XKS bleiben alle Daten jederzeit in der Schweiz. Sämtliche Kundendaten und Anwendungen laufen in ISO-zertifizierten Rechenzentren in der Schweiz und unterstehen vollumfänglich dem Schweizer Recht. **Dies schliesst Zugriffsmöglichkeiten durch ausländische Gesetze wie den US Cloud Act aus.** Der 2018 in den USA verabschiedete CLOUD Act verpflichtet US-Unternehmen, auch dann Daten an US-Behörden herauszugeben, wenn diese Daten ausserhalb der Vereinigten Staaten gespeichert sind. Selbst wenn ein US-amerikanischer Cloud-Provider seine Rechenzentren in Europa betreibt, kann er also zur Herausgabe dieser Daten gezwungen werden.

Gerade für Unternehmen in regulierten Branchen wie Finanzen, Gesundheitswesen oder öffentlicher Verwaltung ist der **Datenstandort Schweiz** ein immer wichtigeres Argument. Xelon bietet eine Infrastruktur auf Enterprise-Niveau mit ISO-27001-Zertifizierung, privatem Netzwerkzugang, Firewalls sowie Integration in bestehende Identitätssysteme. Jeder Kubernetes-Cluster ist isoliert in einem dedizierten Netzwerksegment untergebracht, was die Sicherheit auf das Niveau einer On-Premise-Lösung hebt.

Hier könnt ihr mehr über den Xelon Kubernetes Service erfahren.

Für Schweizer Unternehmen mit lokalem User-Kreis ist die regionale Datenverarbeitung ein Performancevorteil: **Minimale Latenzzeiten und hohe Übertragungsraten** machen den Xelon Kubernetes Service zur idealen Lösung für Echtzeitanwendungen, kritische Lieferkettenlösungen oder interne Geschäftsanwendungen.

Sicherheitsmassnahmen wie Zugriffskontrollen, Verschlüsselung und Netzwerksegmentierung schützen sensible Informationen. Auch eine zum Unternehmen passende Storage-Lösung, ein durchdachtes Backup- und Business-Continuity-Konzept sowie Monitoring- und Alerting-Systeme sind entscheidend für Stabilität und Transparenz.

Technisch bietet der XKS vollständigen **Zugriff auf die Kubernetes-API.** Die Plattform lässt sich über eine REST-Schnittstelle in bestehende Systeme integrieren. So erhalten IT-Teams die Möglichkeit, Deployments zu automatisieren oder den XKS nahtlos in ihre bestehenden Tools und Prozesse wie etwa CI/CD-Pipelines oder Kundenportale einzubinden.

Xelon bietet im Vergleich zu internationalen Hyperscalern zudem tendenziell **tiefere Egress-Kosten sowie eine transparentere Preisstruktur**. Während bei grossen Tech-Konzernen die Abrechnung für Bandbreite und Speicher oft komplex und schwer planbar ist, setzt Xelon insbesondere beim ausgehenden Datenverkehr und Speicherressourcen auf einfach nachvollziehbare Preise. Das minimiert das Risiko von unerwarteten Zusatzkosten, ermöglicht eine verlässliche Budgetplanung und sorgt dafür, dass Skalierung nicht mit finanziellen Überraschungen einhergeht. Die klare Preisstruktur vereinfacht zudem die internen Finanzprozesse.

Hier könnt ihr die Kosten für euer Kubernetes-Projekt mit dem XKS berechnen lassen.

Tutorial: Kubernetes-Cluster erstellen

Mit unserem benutzerfreundlichen Erstellungsassistenten könnt ihr innerhalb weniger Minuten einen funktionsfähigen Cluster aufbauen, der sowohl für Test- als auch für Produktivumgebungen geeignet ist.

Nachfolgend zeigen wir euch Schritt für Schritt, wie ihr bei uns einen Kubernetes Cluster erstellen und welche Optionen und Einstellungen dabei zur Verfügung stehen.

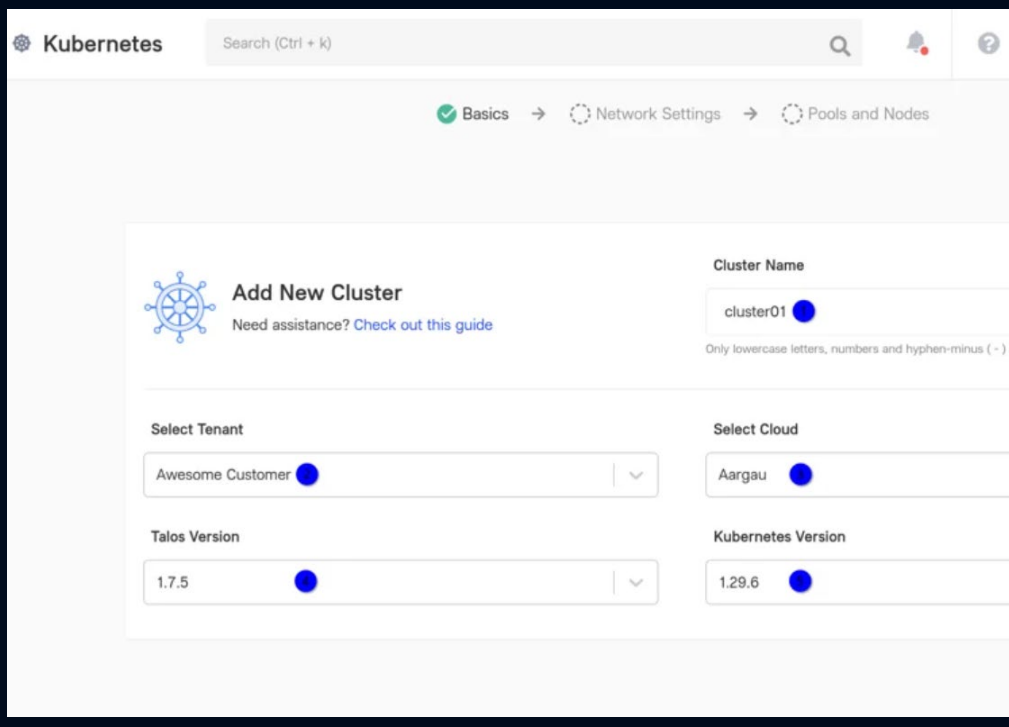
Ausgangslage: Zunächst benötigt ihr einen Account bei der Cloud-Management-Plattform Xelon HQ. Wenn ihr noch keinen Account habt, könnt ihr euch an unser Sales-Team wenden, das euch einen Account kreieren und das Onboarding vereinfachen kann. Sobald ihr einen Account habt und eingeloggt seid, könnt ihr diesen Anweisungen folgen und innerhalb weniger Minute euren ersten Kubernetes Cluster einrichten.

1.

Navigiert in der seitlichen Übersichtsleiste zu Kubernetes und klickt auf «Create Cluster». Der Erstellungsassistent ist in drei Abschnitte unterteilt, die unten aufgelistet sind.

2.

Anschliessend öffnet sich der Erstellungsassistent, der alle notwendigen Informationen abfragt.



a) Cluster Name:

Dieser Name ist ein Anzeigename, der die Wiedererkennung des Clusters erleichtert.

b) Select Tenant:

Mit dieser Option könnt ihr einen Cluster für eure Kundinnen und Kunden bereitstellen.

c) Select Cloud:

Standardmässig laufen alle Nodes eines Kubernetes Clusters in einer dedizierten Cloud, ihr könnt jedoch auswählen, welche Cloud verwendet werden soll.

d) Talos Version:

Talos ist das Betriebssystem, das wir für den Betrieb unseres Dienstes verwenden, wählt hier die gewünschte Version aus.

e) Kubernetes-Version:

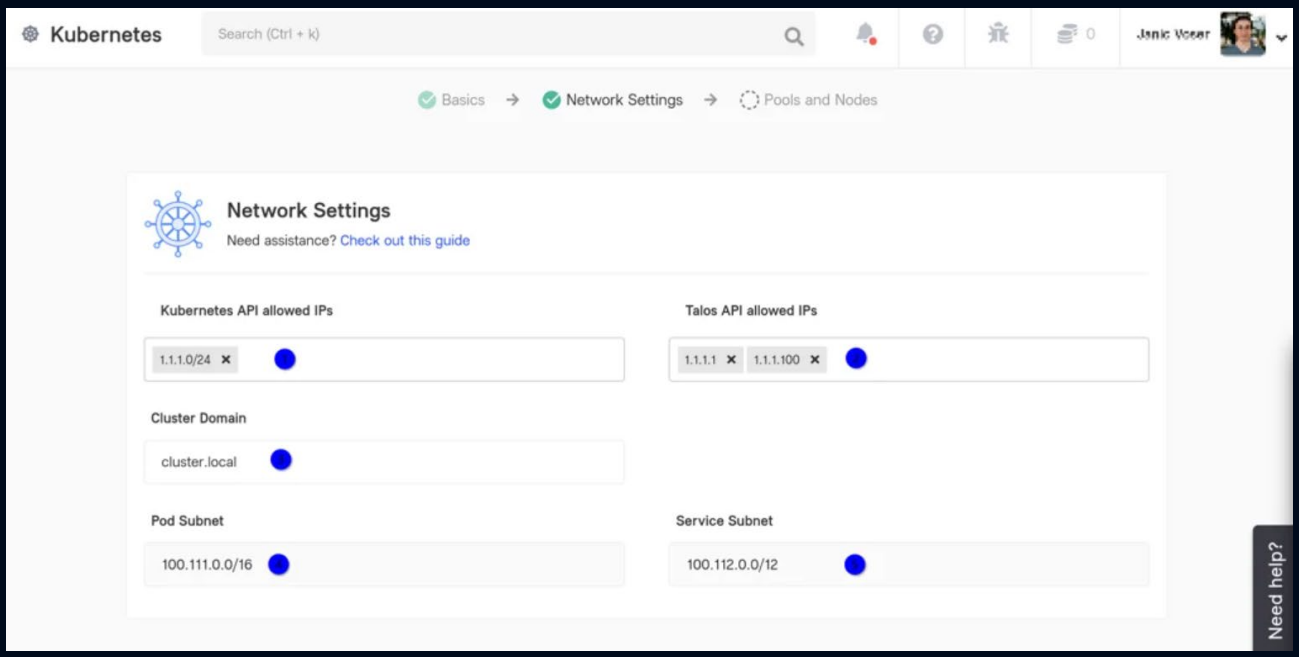
Details zu den aktuellen Kubernetes-Versionen finden sich auf der offiziellen Website. Grundsätzlich sind neuere Versionen besser.

Achtung

Kubernetes verwendet das Semantic-Versioning-Format, aber auch Minor Patches enthalten inkompatible API-Anpassungen.

Network Settings

Die Cluster-Netzwerkeinstellungen regeln den Zugriff auf den Cluster sowie die IP-Verteilung und DNS-Einstellungen im Cluster.



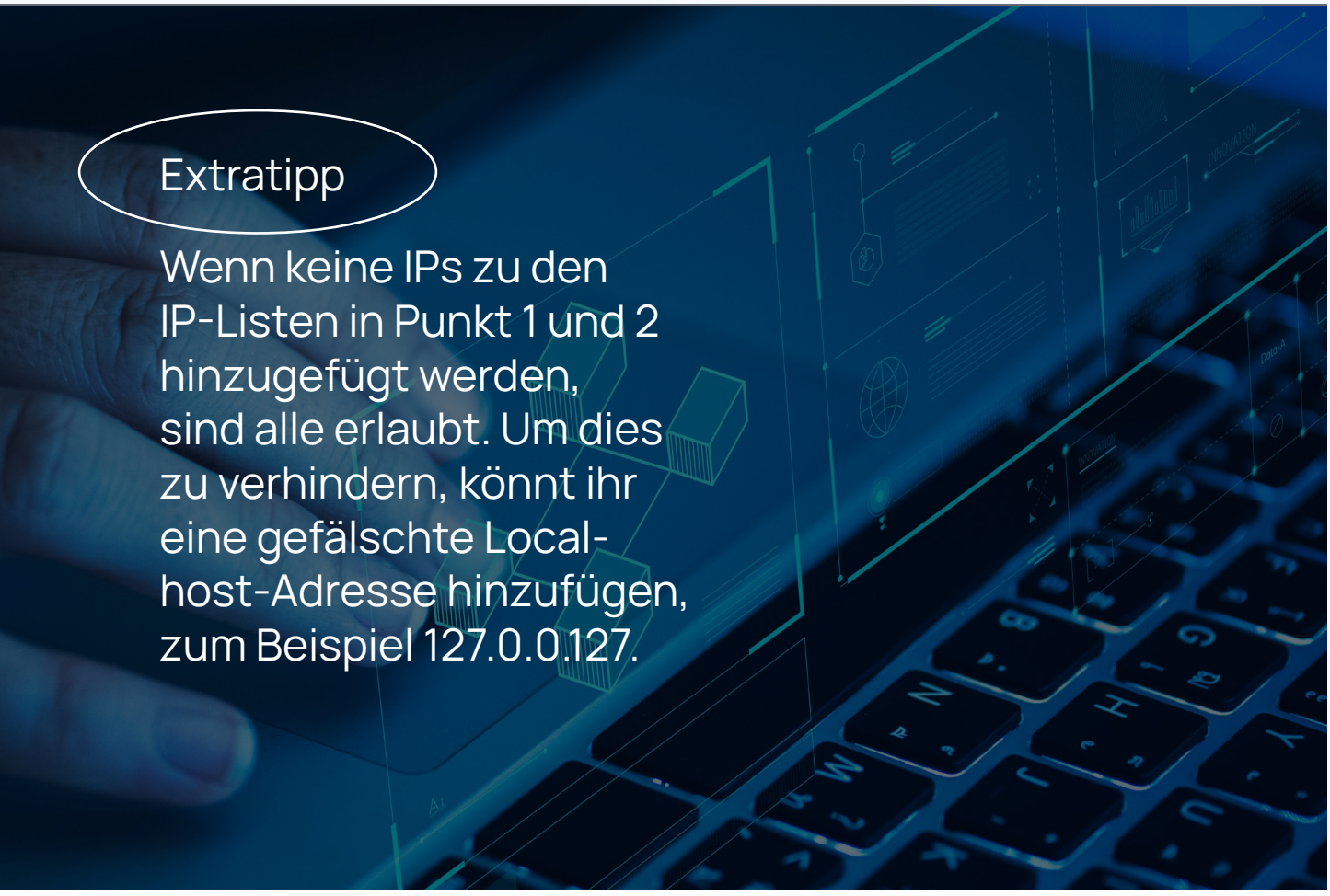
Kubernetes API allowed IPs: Diese Liste von IP-Adressen und Netzwerken erlaubt den externen Zugriff auf die KubeAPI, diese Regel wird von den Load Balancern durchgesetzt. Die KubeAPI wird zur Konfiguration und Verwaltung des Workloads auf dem Kubernetes-Cluster verwendet.

Talos API allowed IPs: Diese Liste von IP-Adressen und Netzwerken erlaubt den externen Zugriff auf die TalosAPI, diese Regel wird von Load Balancern durchgesetzt. Die TalosAPI wird verwendet, um die Konfiguration des Betriebssystems der Nodes zu manipulieren.

Cluster Domain: Kubernetes verwendet intern DNS-Auflösung, um auf Services und Container zu verweisen, alle Services und Container haben einen eigenen «fully Qualified Domain Name», der auf die Cluster Domain endet.

Pod Subnet: Wir verwenden hierfür standardmässig ein Netzwerk aus dem CGNAT-Bereich, welches im Internet nicht geroutet wird. Erfahrt mehr darüber im RFC 6598.

Service Subnet: Aktuell ist dieses noch nicht manipulierbar, wir verwenden ein Netzwerk aus dem CGNAT-Bereich, das nicht über das Internet geroutet wird. Mehr dazu in RFC 6598.

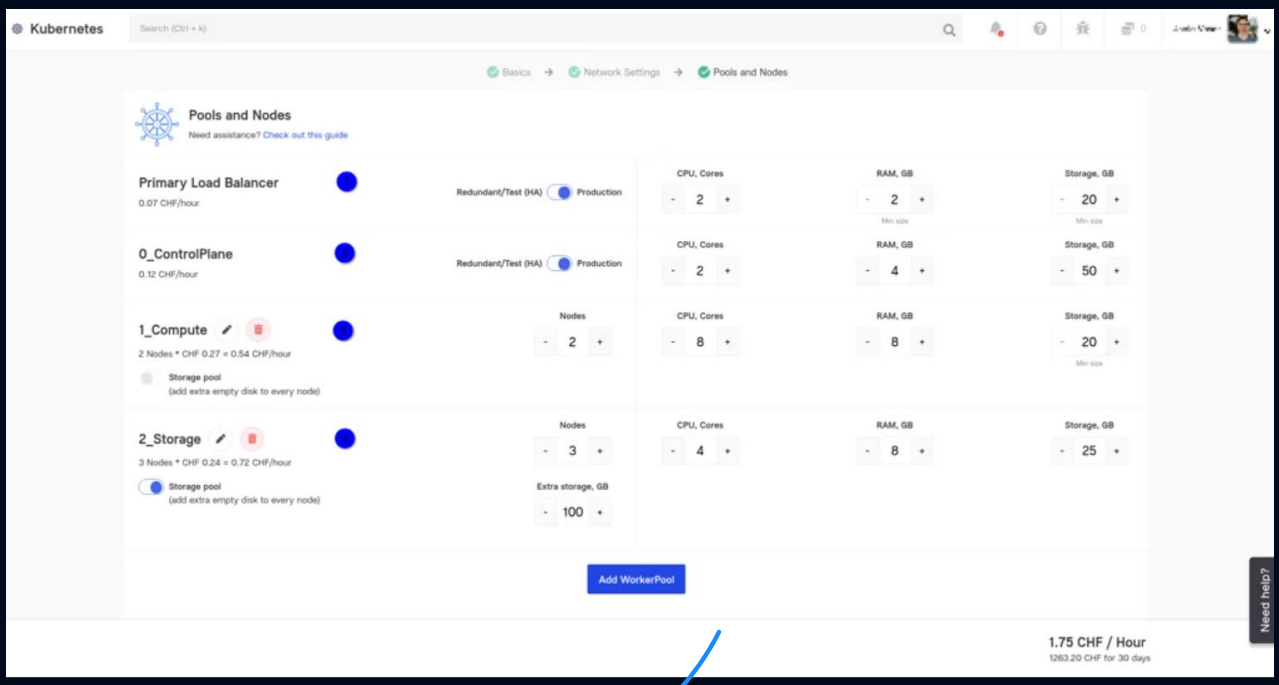


Extratipp

Wenn keine IPs zu den IP-Listen in Punkt 1 und 2 hinzugefügt werden, sind alle erlaubt. Um dies zu verhindern, könnt ihr eine gefälschte Local-host-Adresse hinzufügen, zum Beispiel 127.0.0.127.

Pools und Nodes

Pools sind eine logische Abstraktion, um eine vordefinierte Grösse für die virtuellen Maschinen zu haben. Nodes hingegen sind die virtuellen Maschinen selbst. Generell kann man selbst entscheiden, wie viele Ressourcen man den virtuellen Maschinen zur Verfügung stellen möchte.



1. Primary Load Balancer

Das Primary Load Balancer Cluster wird verwendet, um Kubernetes-Services vom Typ “Load Balancer”, den Standard Ingress Controller sowie die KubeAPI und TalosAPI zu veröffentlichen. Ausserdem wird er als Gateway für die Kubernetes Nodes selbst verwendet. Der Produktivmodus skaliert die Anzahl der Load Balancer Nodes von einer auf zwei Nodes, was die Fehlertoleranz durch Failover-Mechanismen erhöht.

2. 0_ControlPlane

Die Zahl am Anfang des Poolnamens ist die Pool-Index-Nummer. Dieser Pool ist der ControlPlane-Pool, der das Gehirn

(ETCD) von Kubernetes hostet. Der Produktivmodus skaliert die Anzahl der ControlPlane-Knoten von einer Node auf drei Knoten, dies erhöht die Fehlertoleranz und ermöglicht das Management des Kubernetes Clusters / KubeAPI auch während ein ControlPlane-Knoten nicht verfügbar ist.

3. 1_Worker

Dieser Pool ist der erste Worker Pool, je nach Struktur und Funktion des Clusters werden ein oder mehrere Worker Pools erstellt, in diesem Beispiel wird zwischen Compute Nodes und Storage Nodes unterschieden. Die Anzahl der Worker Nodes ist frei und jederzeit skalierbar, es wird jedoch empfohlen, mindestens zwei Worker Nodes zu haben, um Workload Failover zu ermöglichen.

4. 2_Storage

Dieser Pool ist der zweite Worker Pool, den wir über den Button «Add WorkerPool» hinzufügen können. Das Besondere hier ist, dass wir die Option «Storage Pool» aktiviert haben, was es uns ermöglicht, für jede Node in diesem Pool eine weitere Festplatte hinzuzufügen, die wir als lokalen Speicher verwenden können. Achtung: Diese Festplatten sind an die Nodes gebunden und werden gelöscht, sobald der entsprechende Node gelöscht wird.

Wenn alles wie gewünscht selektiert ist, kann man mittels «Deploy Cluster» am unteren Rand des Bildschirms das Cluster erstellen, nach Drücken dieses Knopfes wird das Deployment direkt gestartet und man sieht noch eine kleine Übersicht.

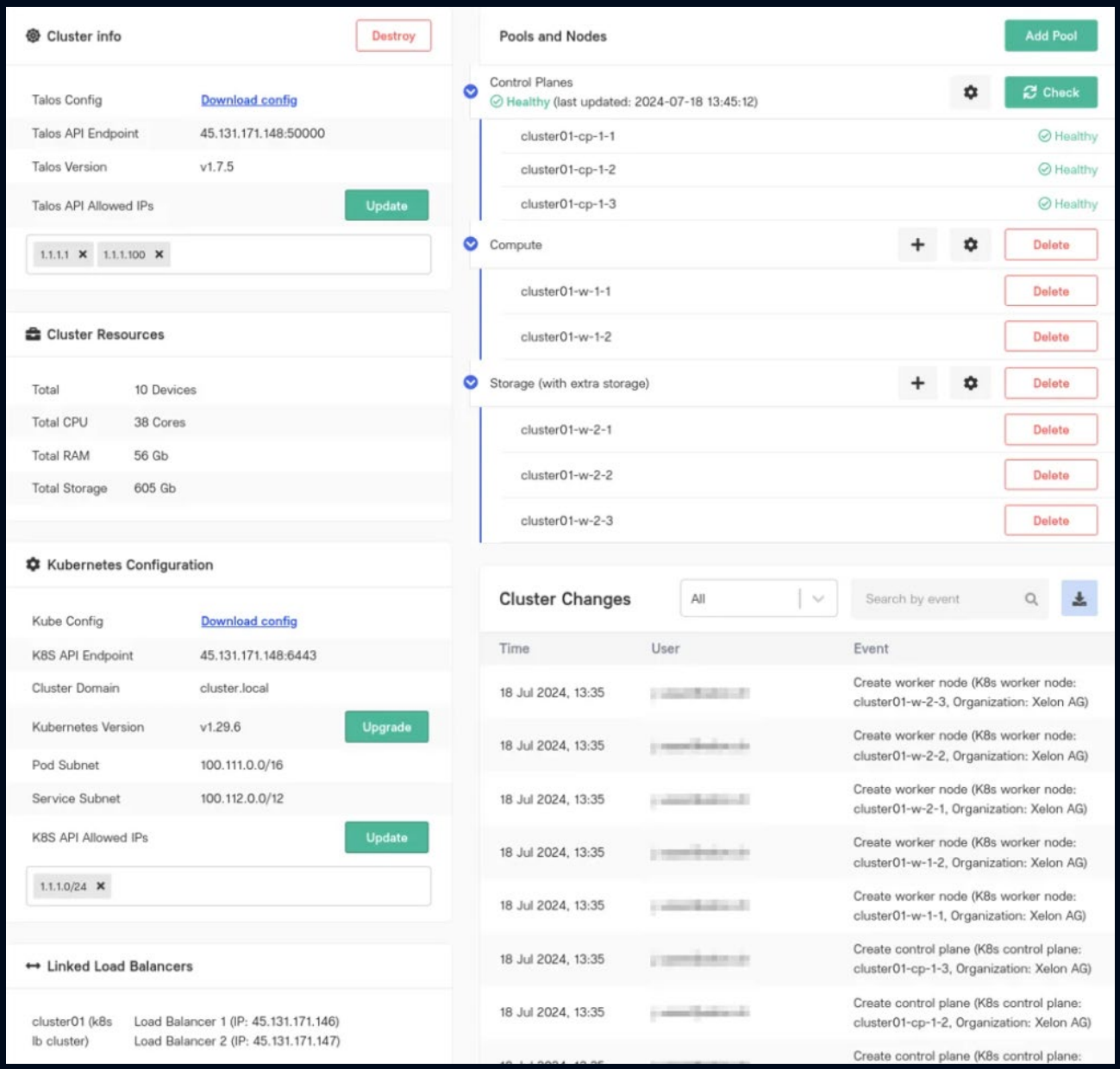
Das Erstellen eines Clusters dauert zwischen drei und zehn Minuten, je nach zugewiesenen Ressourcen.

Erfahrt mehr über die Kubernetes-Komponenten in der offiziellen Dokumentation.

Cluster Dashboard

Navigiert via Navigationsleiste zu Kubernetes und selektiert euer gewünschtes Cluster.

Zunächst wird der Cluster Health Status als «unhealthy» angezeigt, mit der Funktion «Check» kann dieser überprüft werden und einige Sekunden später wird der Status angepasst.



Cluster Info

«Cluster Info» zeigt die wichtigsten Informationen über den Cluster an. Ausserdem könnt ihr hier die Talos-Konfigurationsdatei herunterladen, mit der ihr eure Nodes steuern und manipulieren können. Aus Sicherheitsgründen bieten wir euch auch die Möglichkeit, die Liste der erlaubten IPs über «Talos API Allowed IPs» zu manipulieren.

Wie bereits bei der Erstellung erwähnt, sind alle IPs zulässig, sofern ihr keine dedizierte IP angeben.

Cluster Resources

Der Bereich «Cluster Ressourcen» bietet eine Übersicht, wie viele Ressourcen für alle Geräte zusammen verwendet werden. Hier werden nicht nur die Kubernetes Nodes angezeigt, sondern auch die Load Balancer.

Kubernetes Configuration

«Kubernetes Configuration» zeigt euch die Grundeinstellungen eures Kubernetes Clusters, hier habt ihr wiederum die Möglichkeit, die «K8S API Allowed IPs» anzupassen, sowie die Kubernetes-Version zu aktualisieren. Des Weiteren findet ihr hier auch die Kube Config, welche ihr direkt herunterladen können. um mit Kubectl oder anderen Tools darauf zuzugreifen.

Linked Load Balancers

«Linked Load Balancers» zeigt die verbundenen Load Balancer an, die für jeden Load Balancer angezeigte IP ist nicht die für das Kubernetes Load Balancing verwendete IP, sondern die primäre IP-Adresse des Load Balancers.

Pools und Nodes

Die Sektion «Pools und Nodes» ist der spannendste Teil, mittels “+” Knopf kann ein Arbeiter-Pool um einen Node erweitert werden, dies nennt man auch horizontales Skalieren. Skalieren bedeutet aber nicht nur das Erweitern eines Clusters, sondern auch das Verkleinern eines Clusters, dies ist ebenfalls mittels des «Delete»-Knopfes möglich.

Bitte beachtet, dass es zwei Arten von «Delete»-Knöpfen gibt. Einer befindet sich auf der Pool-Ebene, dieser löscht den gesamten Pool. Die zweite befindet sich auf der Node-Ebene und löscht einen bestimmten Node.

Cluster Changes

Die Sektion «Cluster Changes» ist eine Historie der Aktionen, die auf dem aktuellen Cluster durchgeführt wurden. Diese Logs können auch exportiert werden.

Extratipp

Ihr könnt mehrere Worker-Pools erstellen. Dabei handelt es sich um eine logische Deklaration von Ressourcen, die zur Erstellung neuer Knoten verwendet werden. Um die Skalierung der verfügbaren Ressourcen noch effizienter zu gestalten, erlauben wir auch die vertikale Skalierung der Pools, klickt ihr dazu auf das Zeichen ⚙️ des entsprechenden Pools.

Das Erweitern der Ressourcen erfordert einen Neustart der Node. Fährt die Node über die API sanft herunter. Dabei ist wichtig, dass ihr genügend Ressourcen auf den anderen Nodes habt, um einen Node neu zu starten. Das Ressourcen-Upgrade der Nodes erfolgt seriell.

Vielen Dank für euer Interesse am Kubernetes-Tutorial!

Hättet ihr gewusst, dass es möglich ist, innert Minuten Kubernetes-Cluster in einer skalierbaren Schweizer IT-Infrastruktur mit transparenter Preisstruktur aufzusetzen? Wir hoffen, dieses Tutorial bietet Inspiration, wie sich Kubernetes-Projekte mit hohen Datenschutz- und Compliance-Anforderungen einfacher umsetzen lassen.

Unsere Kubernetes- und IT-Infrastruktur-Experten bieten euch in **einem unverbindlichen Beratungsgespräch** gerne weitere Einblicke in den Xelon Kubernetes Service (XKS) und im **Xelon-Blog** findet ihr mehr Schritt-für-Schritt-Anleitungen und Inhalte zur Trend-Technologie Kubernetes.

Bei anderen Fragen zu IT-Projekten könnt ihr euch gerne **bei mir melden** oder euch **auf LinkedIn mit mir vernetzen.**

Ueli Schwegler
Director Cloud Infrastructure
Unit bei Xelon

Letzte Überabeitung: Juli 2025