pluscloud open – erster Sovereign Cloud Stack für GAIA-X

Die Europa-Cloud kommt

Martin Gerhard Loschwitz

PlusServer positioniert sich mit pluscloud open als einer der ersten GAIA-X-Hoster. Was bietet das Produkt und taugt es, europäische Datensouveränität Wirklichkeit werden zu lassen?

Vor etwa anderthalb Jahren hat sich Europa unter der Führung Frankreichs und Deutschlands das Thema Datensouveränität auf die Fahnen geschrieben. Unabhängig oder zumindest unabhängiger als bisher möchte man von den Hyperscalern werden, die unter der Fuchtel der US-Regierung stehen, also AWS, Azure oder Google. „Data Privacy made in Europe" lautet die Devise: Europäische Daten sollen, wenn ihre Eigentümer es nicht wünschen, den europäischen Rechtsraum erst gar nicht verlassen müssen, weil es hierzulande sinnvolle, zuverlässige Hosting-Angebote gibt. Wie so oft in der hohen Politik war GAIA-X am Anfang allerdings nicht viel mehr als ein Konglomerat aus verschiedenen Absichtserklärungen.

Mittlerweile ist klarer, wohin die Reise geht: GAIA-X soll vorrangig Schnittstellen definieren und Prinzipien festlegen, die den Traum von der europäischen Datensouveränität Wirklichkeit werden lassen. Wer aber Schnittstellen betreiben möchte, braucht dafür Infrastruktur. Hier springt das Projekt Sovereign Cloud Stack (SCS) in die Bresche: Unter Leitung von Kurt Garloff entsteht eine OpenStack-basierte Plattformdefinition, die hiesige interoperable Cloud-Umgebungen ermöglicht [1]. Als erstes Unternehmen aus Deutschland tritt PlusServer mit einer SCS-Implementierung mit OpenStack als Unterbau an. *iX* konnte dem Produkt auf den Zahn fühlen und herausfinden, welche Funktionen es bietet, was gut funktioniert und wo es noch hakt. Indirekt kommt auch die SCS-Idee auf den Prüfstand: Kann es so was werden mit der Europa-Cloud?

Zwar wirbt auch Branchenriese IONOS mit der GAIA-X-Cloud, die basiert aber nicht auf dem SCS, sondern man hat einfach die eigene Plattform für „GAIA-X-kompatibel" erklärt. Das ist nicht per se falsch, weil es innerhalb von GAIA-X (noch) keine Übereinkunft darüber gibt, welche technischen Standards für eine GAIA-X-Kompatibilität gelten. Allerdings hat der Autor zum IONOS-Stack ad hoc beispielsweise keine Software gefunden, mit der man ihn nachbauen könnte. Es gibt für die APIs zwar Dokumentation, aber das bedeutet nicht, dass die APIs unter einer offenen Lizenz stehen. Und genau das ist ja eigentlich der Kerngedanke des Sovereign Cloud Stack.

Viel vor der Brust

Fünf Aspekte des PlusServer-Angebots nimmt dieser Artikel genauer unter die Lupe. Zunächst geht es natürlich um die Frage, ob es als Plattform für GAIA-X-bezogene Dienste fungieren kann. Was ist das technische Fundament und wie passt das Paket damit zu den GAIA-X-Zielen? Der zweite Aspekt wechselt von der Theorie in die Praxis und untersucht die Plattform auf ihre Basisfunktionen hin. Kriterium drei beschäftigt sich mit dem Thema Compliance: Welchen rechtlichen Regeln ist die Lösung unterworfen und welche technischen Möglichkeiten gibt es, gängige Compliance-Regeln in Unternehmen im PlusServer-SCS zu nutzen? Aspekt vier beschäftigt sich mit der Sicherheit: Welche Funktionen bietet die Plattform und wie gut arbeiten diese? Den Abschluss bildet der Themenkomplex der Zusatzfunktionen – denn die SCS-Definition umfasst nicht nur die Plattform per se, sondern auch Zusatzaspekte wie PaaS- oder SaaS-Angebote.

GAIA-X und Projekte wie der SCS zielen nicht – wie einige Kritiker behaupten – auf die Schaffung eines europäischen Amazon-Klons. Angesichts der Entwicklungsgeschwindigkeit von AWS wäre das auch albern, denn nicht einmal die große Konkurrenz in Form von Microsoft oder Google vermag mit den Amazon Web Services in Sachen Entwicklungsgeschwindigkeit Schritt zu halten.

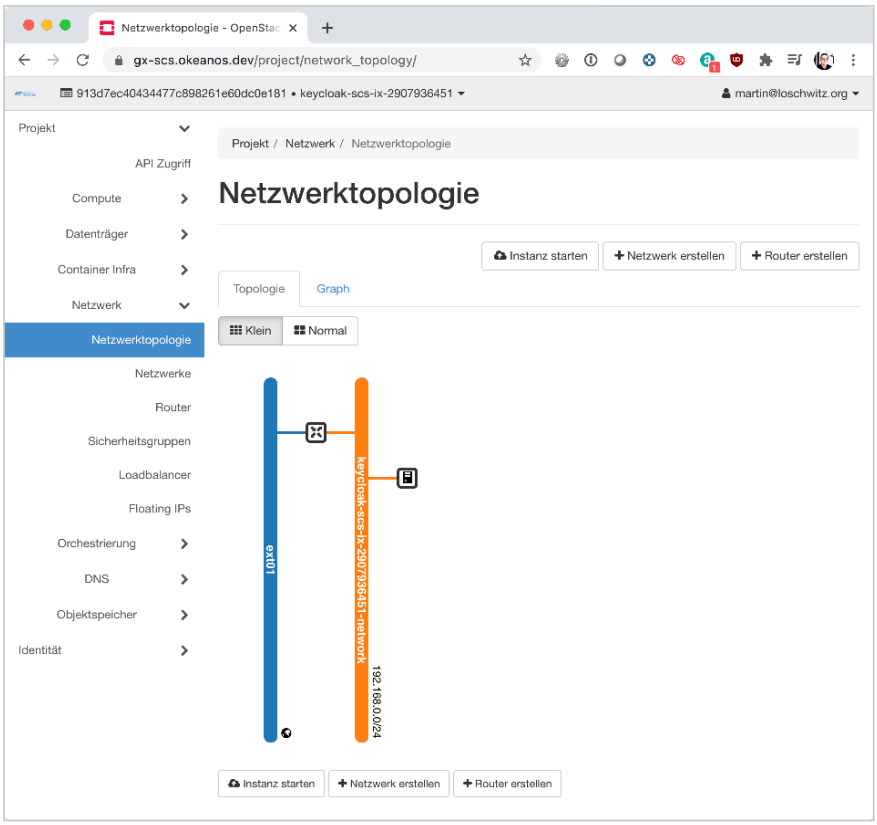
Die Idee hinter GAIA-X und folglich auch hinter SCS ist eine andere. Im Fokus steht die Schaffung robuster offener Standards, die Unternehmen auf eigener Infrastruktur implementieren können. Weil die Standards offen sind, wird es im Kon-

text von GAIA-X auch möglich sein, Workloads zwischen Anbietern zu migrieren. So schön die Tausenden Features von AWS und Co. auch sein mögen – für die alltägliche Arbeit reicht den meisten Unternehmen ein kleines Subset, das jeder gängige Cloud-Anbieter im Portfolio hat. Und genau diese Kunden spricht der Sovereign Cloud Stack primär an – auch in seiner Ausprägung bei PlusServer.

OpenStack soll den Weg zum Erfolg ebnen

Der Kölner Hoster geht mit seiner Umsetzung des Sovereign Cloud Stacks gerade erst auf Kundenfang. Das Produkt ist brandneu – und wer mit OpenStack bereits zu tun hatte, weiß: Es ist bemerkenswert, dass PlusServer hier in wenigen Monaten eine Cloud auf die Beine gestellt hat, die man sich als Public Cloud auch zu vermarkten traut. Ein Kernaspekt einer Public Cloud ist schließlich die Option, diese bei Bedarf in die Breite zu skalieren. Die technischen Grundlagen dafür, etwa auf der Storage- und Netzwerkebene, sind allerdings komplex. Von OpenStack selbst ganz zu schweigen: Die Lösung besteht mittlerweile aus so vielen Komponenten, dass selbst erfahrene OpenStack-Admins manchmal den Überblick verlieren.

Die Verantwortlichen bei PlusServer vertrauen ihrem Produkt aber ganz offenbar so weit, dass man sich jetzt damit aus der Deckung traut. Wobei der Sovereign Cloud Stack hier Schützenhilfe leistet: Teil des Pakets ist die Installation einer OpenStack-Cloud auf Basis des Open Source Infrastructure & Service Managers (kurz OSISM) der Stuttgarter Firma Betacloud. Firmen, die sich dem SCS voll verschreiben, sind also von den üblichen Herstellern wie Red Hat und Canonical in Sachen Cloud unabhängig.



pluscloud open macht es auch Anwendern mit wenig OpenStack-Erfahrung leicht, sich zurechtzufinden – die nötigen Elemente für eine neue VM legt der Anbieter ab Werk an (Abb. 1).

Schon durch die Wahl von OpenStack als technischer Basis ihres SCS hat pluscloud open implizit die Grundlagen dafür geschaffen, die Anforderungen von GAIA-X zu erfüllen. Denn GAIA-X definiert als eine elementare Anforderung offene Schnittstellen, die jedermann nutzen kann. OpenStack, der technische Unterbau von SCS, steht vollständig unter einer freien Lizenz – sowohl der Code selbst als auch die jeweiligen API-Definitionen – und hat im FLOSS-Markt praktisch keine Konkurrenz mehr, die ähnlich gut skaliert und in großen Umgebungen auch nur annähernd gut erprobt ist.

Das geht im Alltag mit vielen Vorteilen einher. Weil PlusServers SCS-APIs öffentlich zugänglich sind, lassen sich sämtliche für OpenStack geschriebenen Werkzeuge auch mit pluscloud open nutzen. Ferner ist es auch kein Problem, Workloads von der SCS-Cloud eines Anbieters auf die Plattform eines anderen Anbieters zu migrieren. Testen ließ sich das in Ermangelung einer zweiten SCS-Cloud nicht, aber dass die Migration von Aufgaben von einer OpenStack-Wolke hin zu einer anderen funktioniert, ist erprobt und auch gut dokumentiert. Dadurch lassen sich natürlich auch unkompliziert hybride Workloads realisieren. In Summe dürfte es für SCS-Anbieter schwierig werden, Kunden technisch an die eigene Plattform zu binden.

Was lässt sich schon nutzen?

Zwar hat OpenStack einen definierten Funktionsumfang, doch längst nicht jeder Anbieter implementiert alle Features, die OpenStack theoretisch beherrscht. PlusServer schöpft bei seiner Plattform aber aus dem Vollen. Wer beim Anbieter eine Teststellung erfragt, bekommt einen Link

X-TRACT

- GAIA-X manifestiert sich nicht mehr länger nur in politischen Absichtserklärungen, sondern auch in konkreter Technik – etwa dem Projekt Sovereign Cloud Stack (SCS), das eine einheitliche Plattformdefinition für Cloud-Anwendungen auf Basis von OpenStack entwickelt.
- PlusServer schickt mit pluscloud open als erster Anbieter einen SCS-basierten Cloud-Stack mit OpenStack-Unterbau ins GAIA-X-Rennen um die Kunden. Er soll technische Grundlage für GAIA-X-bezogene Workloads sein und hostet seine Inhalte ausschließlich im Einflussbereich europäischer Gesetze.
- Technisch nimmt sich der SCS einiges vor: Zwar muss er die großen Hyperscaler wie AWS, Azure oder GCP nicht im Detail nachbauen – der Betrieb einer stabilen, zuverlässigen Cloud-Plattform ist aber selbst bei grundlegenden Features eine Herausforderung.

zu einer Website, auf der man für den eigenen Account einmalig ein Passwort setzt. Danach klappt der Log-in im Webinterface des PlusServer-SCS-Stacks.

PlusServer macht es OpenStack-unerfahrenen Anwendern leicht, sich zurechtzufinden. Ein klassisches OpenStack bietet neuen Nutzern üblicherweise keine vorkonfigurierten Ressourcen. Ein virtuelles Netzwerk, einen virtuellen Router sowie passende Firewallregeln, die SSH-Zugriff auf eigene VMs erlauben, muss man sich zunächst einrichten. PlusServer nimmt Nutzern den größten Teil dieser Arbeit ab (Abbildung 1). Ein virtuelles Netz ist ebenso vorkonfiguriert wie die nötigen Firewallregeln für ICMP und SSH. Nur seinen SSH-Schlüssel lädt der Nutzer noch selbst hoch, wenn er nicht auf die Funktion der Plattform zurückgreifen möchte, ad hoc einen solchen zu generieren. Danach kann es mit der ersten eigenen virtuellen Instanz bereits losgehen (Abbildung 2).

Bei den Betriebssystem-Images bietet PlusServer sämtliche gängigen Linux-Distributionen wie Debian, openSUSE, CentOS oder Ubuntu. Es fehlen hingegen die Enterprise-Distributionen SLES und RHEL, die Nutzer auf Wunsch aber selbst in pluscloud open hochladen können. Hinzu gesellen sich ein paar Funktionen, die man nicht in jeder OpenStack-Cloud findet. Zum Lieferumfang gehört beispielsweise DNS as a Service. Damit legt der Admin Domains fest, um seine virtuellen Maschinen automatisch mit Hostnamen und DNS-Einträgen zu versorgen.

Der Zugriff auf die Umgebung erfolgt wahlweise über die grafische Oberfläche oder über die APIs der OpenStack-Umgebung. Die benötigten Credentials lassen sich direkt im GUI über einen Klick auf den eigenen Benutzernamen oben rechts und „OpenStack RC Datei“ herunterladen. Dank seiner offenen Schnittstellen lassen sich Ressourcen in pluscloud open also auch durch externe Werkzeuge anlegen, zum Beispiel Terraform. Obendrein stellt der Anbieter OpenStack Heat bereit, OpenStacks eigenes Orchestrierungswerkzeug, das seinerseits im Hintergrund die APIs der verschiedenen Dienste abklappert und dort auf Zuruf des Nutzers Ressourcen anlegt.

Was noch fehlt

Einige Dinge fallen bei pluscloud open negativ auf, die meist dem noch jungen Alter geschuldet sein dürften. Der Kölner Hoster betreibt ja daneben auch eine Plattform ohne GAIA-X-Ambitionen und bietet darin Funktionen wie diverse Storage-Optionen oder Backup as a Service an. Die fehlen im SCS-Stack bislang. Hier gibt es nur eine Default-Klasse für virtuellen Blockspeicher, die im Test auch nicht sonderlich flink reagierte – SSDs kommen hier also vermutlich nicht zum Einsatz.

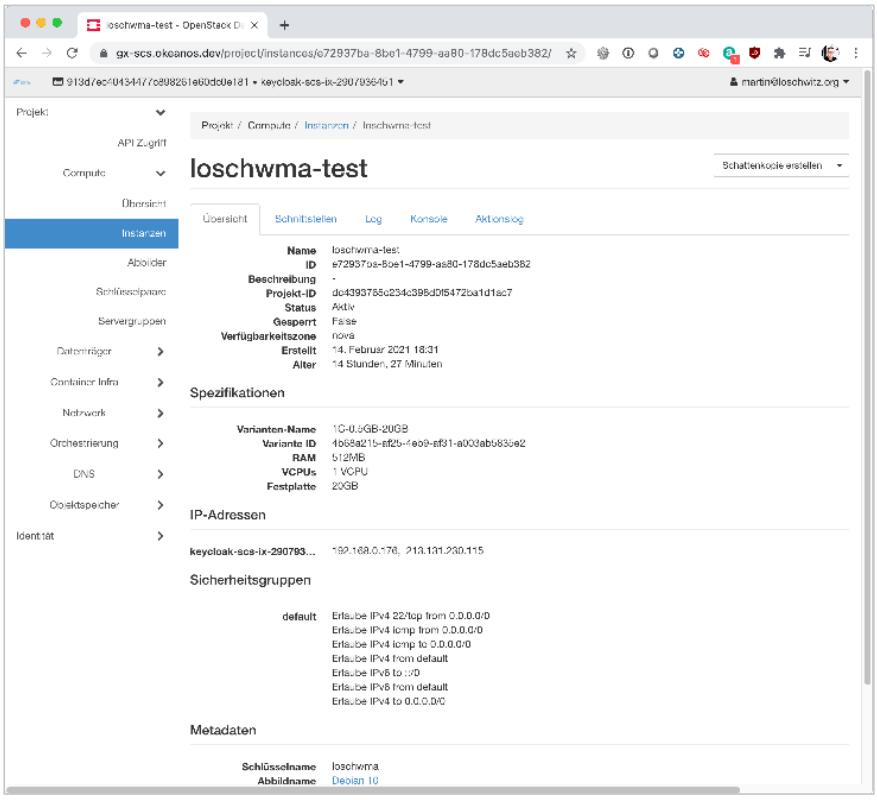
Um Backups muss sich der Cloud-Kunde ebenso selbst kümmern wie etwa um gemanagte Datenbanken. Allerdings kann man PlusServer dafür kaum die Schuld in die Schuhe schieben, denn sowohl Database as a Service als auch Backup as a Service existieren auch für OpenStack selbst nicht zufriedenstellend. Es wird spannend sein, zu beobachten, ob der Sovereign Cloud Stack hier künftig selbst Entwicklungsarbeit leistet oder andere Unternehmen zu entsprechenden Investitionen bewegt. Schnelleren Speicher könnte PlusServer jedoch implementieren – und wird das hoffentlich auch bald tun.

Das leidige Thema Compliance

Die wenigsten Administratoren beschäftigen sich gern mit dem Thema Compliance, denn es ist komplex und führt, wenn falsch behandelt, zu handfesten rechtlichen Konsequenzen. Plattformen wie pluscloud open treffen deshalb auch auf die Erwartungshaltung, dem Admin einen Teil seiner Compliance-Arbeit abzunehmen. Das könnte konkret etwa bedeuten, dass sich die Benutzerverwaltung unkompliziert an vorhandene Verzeichnisdienste eines Unternehmens anbinden lässt – Amazon macht es bei AWS vor. Die in pluscloud open genutzten Komponenten können das zwar grundsätzlich, doch liegen die diesbezüglichen Funktionen derzeit brach. Nutzer der Cloud erhalten eine Kombination aus Benutzername und Passwort, legen damit im Rahmen der eigenen Quotas Ressourcen an – mehr geht nicht.

Benutzer- wie Projektname in pluscloud open legen nahe, dass der Authentifizierungsdienst Keystone im Hintergrund an eine Instanz von Red Hats Keycloak angeschlossen ist. Das deutet darauf hin, dass der Anbieter Federation und Single Sign-on (SSO) später anbieten wird. Anders wären hybride Set-ups allerdings aus Compliance-Sicht auch kaum zu warten – Federation wäre hier kein „nice to have“, sondern ist im weiteren Verlauf eigentlich zwingende Notwendigkeit.

In der von *iX* getesteten Version lassen sich neue Benutzer jedenfalls nur direkt vom Anbieter hinzufügen. Auch ließ sich kein einem RBAC-Prinzip nachempfundenes Rechteschema etablieren – obwohl der Anbieter das in seiner Produktbeschreibung als Funktion der Plattform anpreist. Jeder Nutzer, der auf ein Projekt in plus-



Innerhalb weniger Sekunden nach dem ersten Log-in ist in pluscloud open eine virtuelle Instanz geboren – SSL-Schlüssel hinterlegen, VM starten, fertig (Abb. 2).

cloud open zugreifen darf, hat vollen Zugriff auf die darin vorhandenen Ressourcen. Zur Verteidigung des Anbieters sei allerdings auch erwähnt, dass OpenStack selbst die Implementierung eines Rollenmodells äußerst kompliziert gestaltet. Unmöglich ist es nicht, ein solches zu implementieren, doch rechnet man bei einer jungen OpenStack-Cloud mit dieser Funktion eigentlich sowieso nicht. Das Nachrüsten ist allerdings ein Punkt im Hausaufgabenheft des Anbieters. Vielleicht ist hier auch SCS selbst gefragt, ein entsprechendes Rechteschema zu beschreiben und als Standard zu definieren. Denn ein Rollenschema ergibt eigentlich nur Sinn, wenn es allgemein gültig und für verschiedene Instanzen des SCS-Stacks valide ist – sonst wären Migrationen und hybride Set-ups schwierig bis unmöglich aufzusetzen.

Wie hältst du's mit der Sicherheit?

Neben der Compliance ist die Sicherheit ein zentraler Aspekt bei der Verwendung von Cloud-Diensten. pluscloud open liefert dem Anwender hier zunächst Hausmannskost aus dem Hause OpenStack: Virtuelle Instanzen lassen sich über Security Groups schützen. Die übersetzt der OpenStack-Compute-Dienst Nova auf den einzelnen Compute-Knoten in Regeln für iptables und nftables. Weil die Regeln aus der VM heraus nicht zu verändern sind, gefährdet eine sorgsam abgeschottete VM also auch nicht automatisch das gesamte OpenStack-Projekt, wenn sich Fremde unberechtigt Zugang zu ihr verschaffen.

Weil sie im Hintergrund zu Paketfilterregeln führen, sind Security Groups in ihrer Anwendung sehr flexibel. Sie ermöglichen es, Filter anhand von Protokollen, Ziel- sowie Quelladressen und vielen weiteren Faktoren zu definieren. Im SCS-Stack von pluscloud greifen ihnen zusätzliche Sicherheitsfunktionen unter die Arme. Wie üblich bietet auch pluscloud open wie beschrieben die Funktion, SSH-Schlüssel ad hoc zu generieren oder den öffentlichen Teil eines SSH-Keys zu importieren. Alle gängigen Cloud-Abbilder haben für den Standardbenutzer kein Passwort mehr definiert, sodass ein Log-in ausschließlich per SSH-Schlüssel erfolgen kann.

Als weiteren Beitrag zur Sicherheit bietet pluscloud open OpenStacks Loadbalancer-as-a-Service-Funktion an. Die war im Test zwar kaputt und ließ sich wegen vermeintlich fehlender Berechtigungen nicht nutzen. Fakt ist jedoch: OpenStack Octavia – so heißt die Komponente, die sich um LBaaS im Hintergrund kümmert – entbindet den Administrator davon, eine eigene VM als Loadbalancer zu betreiben.

Netzwerkkompromisse

Dem steht fast schon entgegen, dass pluscloud open auch das OPNsense-Image enthält und Nutzern den Betrieb einer eigenen Firewall ermöglicht. OPNsense ist eine auf HardenedBSD aufsetzende Firewall-Appliance, die sich im SCS-Stack von PlusServer anstelle der Security Groups und letztlich auch anstelle eines virtuellen Routers nutzen lässt. Grundsätzlich funktioniert OPNsense gut, doch ist es nicht ganz trivial, solche Appliances sinnvoll in OpenStack einzubinden. Denn der virtuelle Router, der in OpenStack die Verbindung zwischen einem privaten Cloud-Netz und dem Internet herstellt, tut das stets per

NAT und Port-Forwarding. Weil OPNsense aber ebenfalls NAT nutzt, hängen VMs, die via OPNsense in OpenStack aus dem Internet erreichbar sind, stets hinter doppeltem NAT. Zu umgehen ist das Ganze letztlich nur mit einer Firewall-Appliance, die auf der Netzwerkebene direkt mit dem OpenStack-Dienst Neutron redet, der sich um die virtuellen OpenStack-Netze kümmert.

Dass eine solche Appliance im SCS-Stack von PlusServer zum Einsatz kommt, war nur aus Sicht „von außen" nicht sicher auszuschließen, ist aber zumindest sehr unwahrscheinlich. OpenStack selbst beherrscht Service Chaining für NFV-Anwendungen dieser Art mittlerweile; gut möglich, dass PlusServer in Zukunft also mit entsprechenden Funktionen noch nachlegt.

Zusatzfeatures: Gemanagte Container, Kubernetes und Co.

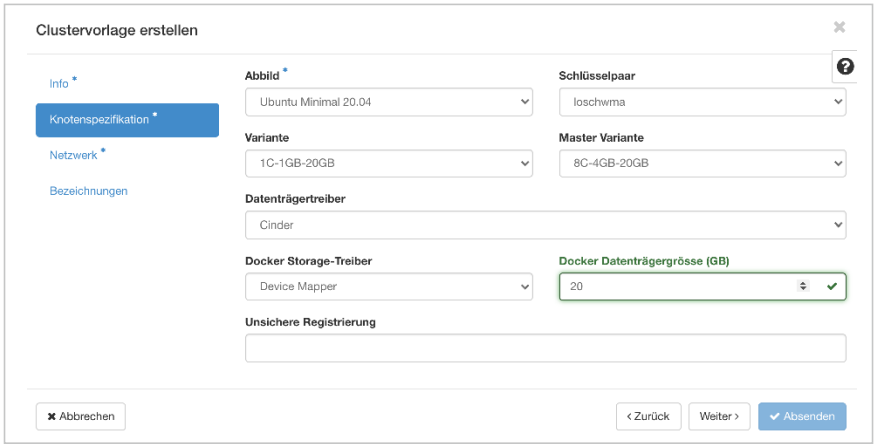
Im letzten Teil schaut dieser Test über den Tellerrand von OpenStack im Kontext des SCS-Stacks hinaus und betrachtet Funktionen, die pluscloud open neben klassischem IaaS noch anbietet. Dieser Faktor gerät bei vielen Betrachtungen rund um den SCS gern aus dem Blick – trotzdem: SCS deckt explizit nicht nur den IaaS-Teil des Stacks ab, sondern will auch für jene Komponenten Standards definieren, die oberhalb davon liegen. Natürlich geht es dabei regelmäßig um den Containerorchestrierer Kubernetes und die Werkzeuge, die man für einen sinnvollen Betrieb braucht. In pluscloud open erkennt man hiervon bisher aber wenig. Zum Lieferumfang der Plattform gehört zwar OpenStack Magnum zum Management von Containerorchestrierern. Die dafür benötigten Templates müssen Benutzer allerdings selbst erstellen. Und das wiederum setzt Vorwissen voraus – ohne dieses ist es unwahrscheinlich, dass Anwender mit dem, was sie in pluscloud open vorfinden, zu einem funktionierenden Kubernetes-Cluster kommen (Abbildung 3).

Das ist einerseits schade, weil sich für PlusServer hier eine Gelegenheit ergeben hätte, gleich zum Produktstart zu beeindrucken. Auf der anderen Seite dürfte aber genau hier auch der Hase im Pfeffer liegen. Zwar wirkt pluscloud open nirgendwo unfertig, und bis auf den LBaaS ließ sich die Umgebung wie vom Anbieter angekündigt nutzen. Man merkt dem Produkt dennoch an, dass es gerade erst den Kinderschuhen entwächst und mancherorts noch ein bisschen Politur fehlt. Fakt ist aber auch: Wer sich nicht davor scheut, selbst Hand anzulegen, startet den vom SCS propagierten oberen Teil des Stacks samt Kubernetes und Co. auf pluscloud open so, wie der Standard es vorsieht.

So erklärt sich letztlich übrigens, dass außer der Containerkomponente in pluscloud open derzeit nur eine einzige Integration mit einer anderen externen Lösung gegeben ist – nämlich jene mit Ceph. Einerseits dient Ceph als Backend-Speicher für Volumes, andererseits bietet die Plattform auch einen Objektspeicher, der in weiten Teilen das S3-Protokoll emuliert und über entsprechende Clients zu betanken ist.

Kosten

Die im Rahmen dieses Artikels getestete Version von pluscloud open war von PlusServer selbst noch nicht für den produktiven Betrieb freigegeben. Das sollte sich laut Aussage des Anbieters zwischenzeitlich zwar geändert haben – eine Auskunft über die Preise, die PlusServer für den Betrieb von Diensten in der GAIA-X-Cloud verlangen will, war aber dennoch nicht zu bekommen. Die Abrechnung nach tatsächlichem Verbrauch statt anhand pauschaler Preise ist laut Anbieter jedenfalls vorgesehen – ohne diese wäre ein Cloud-Angebot auch kaum attraktiv für die Kunden.



Zwar bietet pluscloud open die OpenStack-Komponente Magnum an, mit der sich Orchestrierer für Container wie Kubernetes oder Docker Swarm steuern lassen, intuitiv ist das aber nicht (Abb. 3).

Fazit: Die Richtung stimmt

GAIA-X muss weg vom grünen Tisch und raus in die echte Welt. Der Bedarf an echtem europäischen Datenschutz und echter europäischer Datensouveränität ist gewaltig. Allein die Anzahl der Produkte, die diese Faktoren kombinieren und realisieren, ist derzeit verschwindend gering. pluscloud open auf Basis des Sovereign Cloud Stack zeigt, dass die Europa-Wolke ohne Datenabfluss kein Traum bleiben muss, sondern Realität werden kann. Angesichts des sehr jungen Alters der Umgebung bietet sie eine beachtliche Funktionalität, befeuert von der freien Cloud-Lösung OpenStack.

Mit Ausnahme des Loadbalancer-Problems zeigte sich das Produkt im Vorserientest bereits von seiner besten Seite. Liefert der Anbieter in den kommenden Monaten noch an der einen oder anderen Stelle Convenience-Funktionen nach, etwa in Sachen Compliance oder Sicherheit, hat pluscloud open echte Chancen, sich früh am Markt zu etablieren. Ein Selbstläufer wird das aber nicht, und die Konkurrenz scharrt bereits mit den Hufen: Auch die Deutsche Telekom etwa betreibt in Form der Open Telekom Cloud ja eine Plattform ausschließlich auf europäischem Boden. Die entspricht zwar noch nicht komplett den Bestimmungen des SCS, dürfte sich aber rasch in eine sehr ähnliche Richtung entwickeln. Auf den frühen Lorbeeren sollte PlusServer sich also besser nicht ausruhen. (avr@ix.de)

Quellen

[1] Kurt Garloff; Wolkenverbund; Mit Sovereign Cloud Stack zu mehr digitaler Souveränität; *iX* 12/2020, S. 48

[2] Infos zu pluscloud open und zum Sovereign Cloud Stack: ix.de/z911

Martin Gerhard Loschwitz

ist Cloud Platform Architect bei Drei Austria und beackert dort Themen wie OpenStack, Kubernetes und Ceph.