Die Evolution der Virtualisierung

Effizienz und Sicherheit sind die ewigen Themen der IT-Branche. Was mit virtuellen Servern begann hebt die Container-Technologie auf einen neuen Level. In sogenannten Containern laufen die Server-Programme wie in einer eigenen virtuellen Maschine – bei massiv geringerem Ressourcenbedarf und klarer Abgrenzung zu anderen Services.

Mit dem Siegeszug der Virtualisierung wurde es kosteneffizient möglich unterschiedliche Funktionen auf eigene Server zu platzieren. Diese Aufteilung der Funktionen auf mehrere Server hat auch für die Verfügbarkeit und Sicherheit grosse Vorteile. Komplexe Systeme werden zudem einfacher, wenn einzelne Komponenten möglichst isoliert eine einzige Aufgabe erledigen. Andererseits ist es nicht immer kosteneffizient für jeden kleinen Service eine eigene virtuelle Maschine zu unterhalten. Deshalb werden oft mehrere Funktionen in einem Server integriert, wodurch das System komplizierter und der Unterhalt teurer wird.

Die sogenannte Container-Technologie adressiert genau diese Schwäche heutiger Systeme. Sie ist eine Weiterentwicklung der IT-Virtualisierung mit dem Ziel, ungenutzte System-Ressourcen in virtuellen Maschinen nicht brach liegen zu lassen, sondern zu nutzen. So entfällt beim Einsatz der Container-Technologie der Overhead einer vollständigen virtuellen Maschine mit eigenem Kernel, da nur ein Bruchteil der Ressourcen einer vollständigen virtuellen Maschine benötigt wird. Ein Container kann aufgrund des geringeren Ressourcenverbrauchs ausserdem viel schneller gestartet werden. Auch kann ein Anwendungs-Container Bit-identisch auf verschiedene Systeme dupliziert werden, was die Bereitstellungszeit erheblich vermindert. Für den IT-Betrieb bedeutet dies eine Effizienzsteigerung.

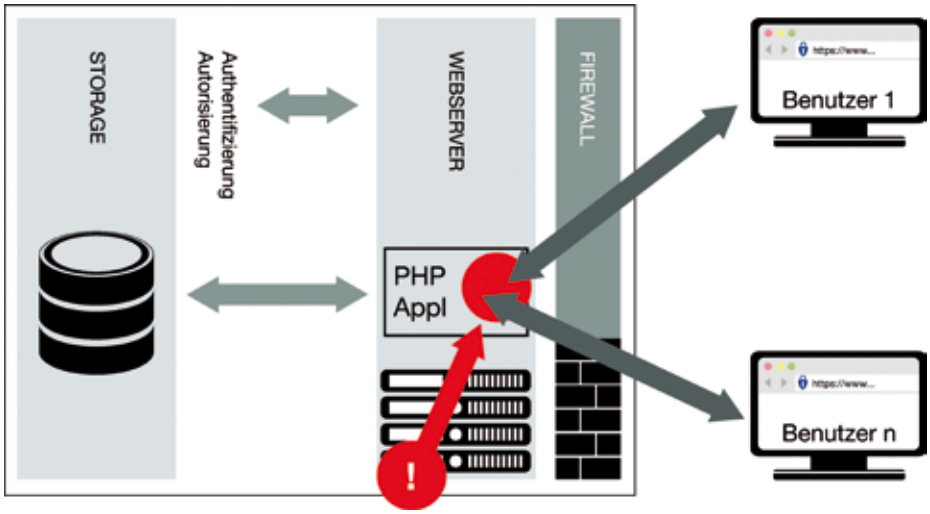
Jedem Service seinen Container

Docker Container heissen die massgeschneiderten «Virtualisierungsboxen» z.B. bei der Open-Source-Software Docker. Die Docker Container laufen in einem Docker Host und der Administrator bestimmt, wie die Container mit anderen Containern und der Aussenwelt kommunizieren können. In einem solchen Container laufen die Server-Programme wie in einer eigenen virtuellen Maschine. Sie sehen nur die wenigen eigenen Benutzer, Prozesse, die eigenen Netzwerkverbindungen und die eigenen Speicherinhalte. Aus Sicht des Systems Engineering ist diese Situation ideal, weil sie die Trennung von Schnittstelle, System und Umgebung wie im Design gefordert umsetzt. Auch aus der Perspektive von Software-Entwicklern und Betreibern sind Container eine gute Sache, weil Container vom Host unabhängig sind und somit die Anwendung

DER AUTOR

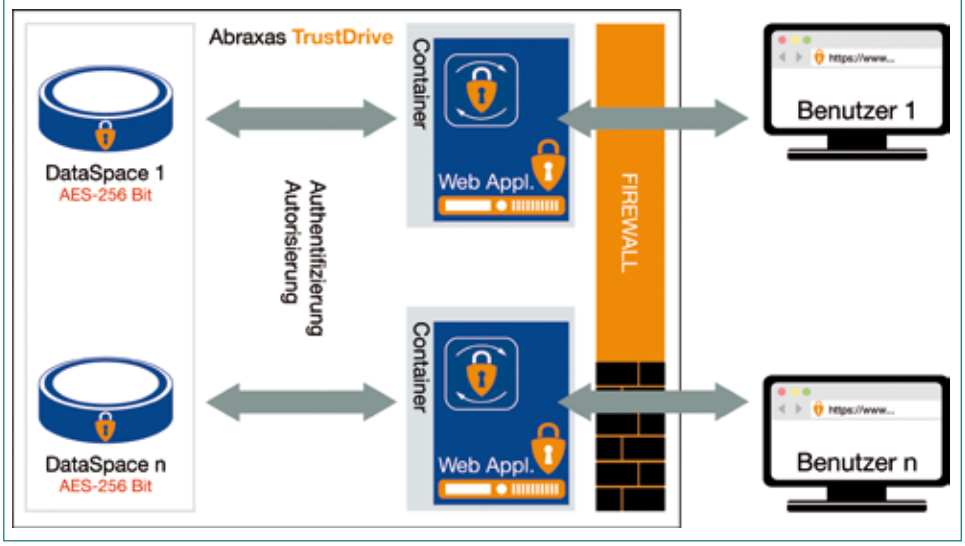
Dr. Peter Englmaier studierte Physik und Astronomie in Heidelberg und doktorierte anschliessend in Basel in Astrophysik. Bei Abraxas verantwortet er als System Engineer unter anderem die Entwicklung der Speicherlösung TrustDrive.

HERKÖMMLICHE WEBAPPLIKATION



Ineffizient und anfällig: Bei herkömmlichen Webapplikationen Teilen sich mehrere User dieselben Ressourcen.

TRUSTDRIVE MIT CONTAINER-TECHNOLOGIE



Alles ist sauber getrennt: Webapplikation mit Container-Technologie

während der Entwicklung, in Tests, beim Staging und beim Deployment in weitgehend identischer Umgebung läuft. Sicherheitstechnisch sind Container mit virtuellen Servern vergleichbar. Richtig eingesetzt erhöhen die Container die Sicherheit. Und nicht zuletzt profitiert auch der Auftraggeber von sinkenden Kosten, wenn sich genügend Container einen Host teilen.

Docker Container machen den TustDrive-Webclient sicher

Die Sicherheitsanforderungen sind für Webapplikationen besonders hoch. In herkömmlichen Systemen nutzen alle Anwenderinnen und Anwender über das Internet die gleiche Instanz einer Applikation. Aufgrund der gemeinsamen Nutzung besteht also das Risiko, dass Hacker mit erbeuteten Zugangsdaten eines einzigen Nutzers möglicherweise auch auf die Daten anderer Anwenderinnen und Anwender zugreifen können. Mittels des Einsatzes von Containern lässt sich dieses Risiko ausschliessen, denn jeder Benutzer erhält für seine Session einen eigenen Container mit einer eigenen Instanz der Webapplikation. Damit ist sichergestellt, dass ein Prozess immer nur Zugriff auf die Daten des angemeldeten Benutzers erhält. Es gilt der Grundsatz: Je besser die Isolierung der Benutzer von einander, desto sicherer die Lösung.

Abraxas nutzt die Effizienz und Sicherheitsversprechen von Containern beim Betrieb ihres TrustDrive Webclients. TrustDrive ist ein Online-Speicher und ein Kollaborations-Tool, um Geschäftsdaten datenschutzkonform und auf höchstem Sicherheitsniveau zu transportieren, zu bearbeiten und zu teilen. Der Vorteil: Im Gegensatz zu herkömmlichen Webapplikationen, bei denen die Applikation selber unter einem einzigen Systembenutzer läuft und so Angreifer auf die Daten aller Anwender und auf die gesamte Serverkonfiguration zugreifen könnten, können beim Container Einsatz die Benutzer und ihre Daten klar und damit sicher voneinander getrennt werden.

Die inhaltliche Verantwortung für den Artikel liegt bei der Abraxas AG.

VORTEILE DER CONTAINER-TECHNOLOGIE IM ÜBERBLICK

Docker Container bietet viele Vorteile um die gewünschte Funktionalität und Sicherheit ohne höhere Kosten zu erreichen:

Kernel: Im Host läuft bereits ein Linux Kernel, der Container hat keine eigene Hardware und bekommt somit nur eigene Ressourcen im Kernel zugeteilt. Der Kernel ist mit Docker quasi Mandantenfähig geworden. Da der Kernel nur einmal geladen wird, spart ein Container gegenüber einer Virtueller Maschine wertvollen RAM.

Betriebssystem: Docker stellt sowohl Betriebssysteme als auch fertige Applikationen in verschiedenen Versionen zur Verfügung. Der Container wählt lediglich die gewünschte Version aus. Container erlauben so eine effizienteres Systems Engineering und erhöhen die Flexibilität bei der Unterstützung unterschiedlicher Softwareprodukte.

Speicherplatz: Die im Container laufenden Programme sehen eine eigene Kopie der Dateien im Betriebssystem und können diese auch verändern. Somit unterscheidet sich das System aus Anwendersicht nicht von einem normalen Betriebssystem. Allerdings belegen unveränderte Dateien keinen zusätzlichen Disk Space, egal wie viele Container das gleiche „Betriebssystem“ verwenden.

Unabhängigkeit: Da die Container so günstig sind, wird es möglich, jede Komponente in einen eigenen Container zu legen und den gegenseitigen Zugriff nur über die definierte Schnittstelle zu erlauben. Dadurch wird die Sicherheit vor unerwünschten Zugriffen und die Stabilität erhöht. Zudem können Legacy Komponenten mit spezifischen Abhängigkeiten leichter integriert werden.

Zeit: Neue virtuelle Server lassen sich in 15 Minuten bereitstellen. Neue Container sind hingegen innert Sekunden einsatzbereit.