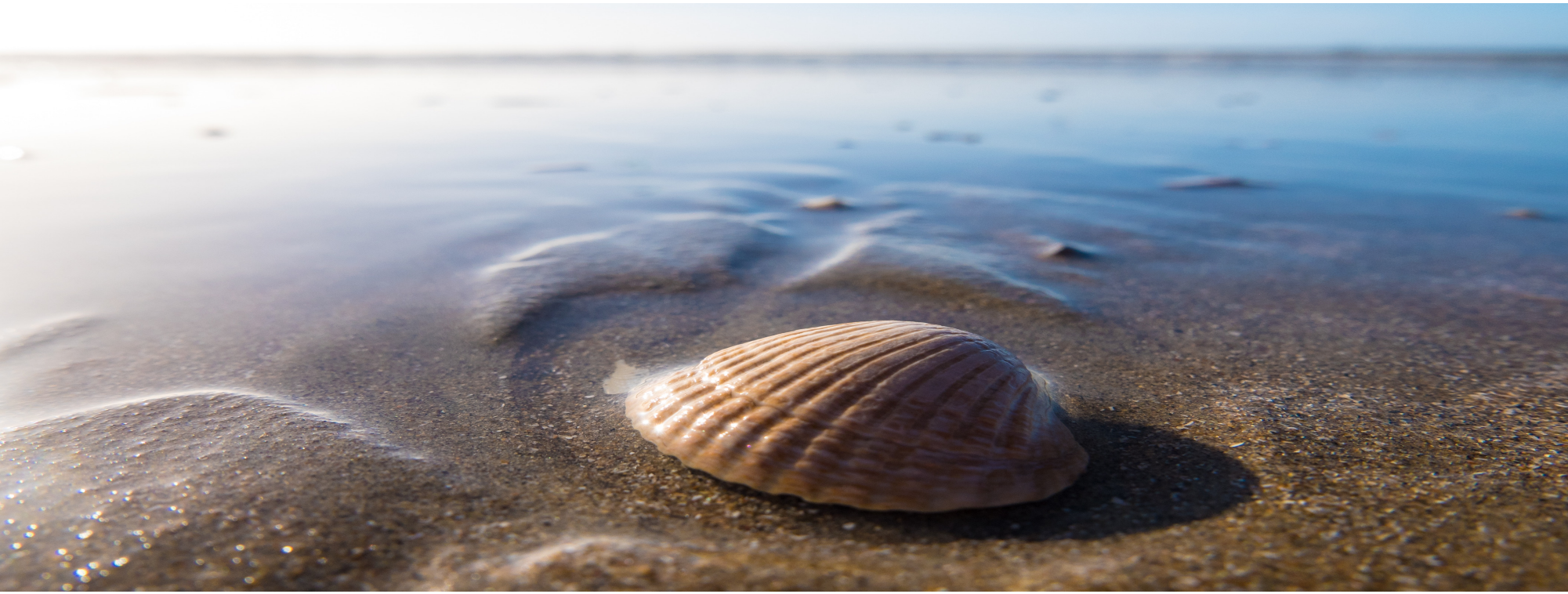
TRALIOS
Linux Server Management

Intern: SSH im Webspace-Paket

Wie können wir im Shared-Hosting eine eingeschränkte Shell anbieten?



Thomas Witzenrath ▪ 03.08.2017

Remote Shell

TRALIOS
Linux Server Management

- Benutzer wollen per SSH auf ihren Webspace zugreifen
- Dies gibt ihnen viele neue Möglichkeiten Dinge zu tun
- Nicht alle diese Dinge sollten in einem Webspace-Paket möglich sein

Was soll ein Benutzer dürfen?

TRALIOS
Linux Server Management

- Eigene Dateien verwalten (cp, mv, rm, ..)
- Archive entpacken (tar, unzip, ..)
- (SQL-)Skripte ausführen (mysql, Installationsskript für CMS, ..)
- Dateien hoch-/runterladen (scp, sftp)
- Dateien von anderen Servern holen (wget, curl, ..)

Was soll ein Benutzer nicht können?

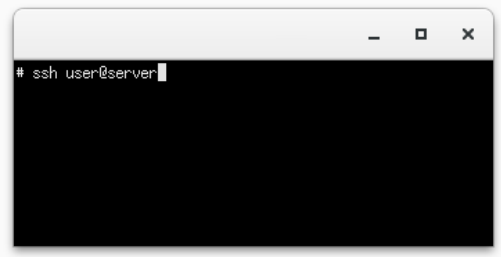
TRALIOS
Linux Server Management

- Nicht auf Daten anderer zugreifen(!)
- Keine lang laufende Prozesse (Daemons) starten
- Keine Ports weiterleiten oder öffnen
- Kein uneingeschränkter Netzwerkzugriff
- Ressourcenlimits

SSH

TRALIOS
Linux Server Management

- per Default keine Einschränkungen
- Dateirechte vom System, aber wie verhindern wir, dass Benutzer diese falsch setzen
- Portweiterleitung lässt sich unterbinden
- Öffnen von (high-)Ports möglich
- ..



Für Managed-Server-Kunden kein Problem, im Shared-Hosting aber nicht machbar

SSH ins chroot

TRALIOS
Linux Server Management

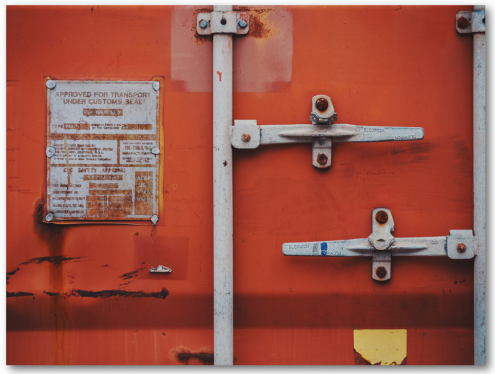
- verschiedene Varianten (rssh, chroot-jail, ..)
- Bauen der chroot-Umgebung relativ umständlich
- Öffnen von Ports weiter möglich
- keine Laufzeitbeschränkung für Prozesse

Wir hatten rssh schon benutzt, aber wieder abgeschafft, da es zu unkomfortabel war

SSH to Docker

TRALIOS
Linux Server Management

- statt einem chroot sperren wir den Benutzer in einen Docker Container
- Home-Verzeichnis als Volume eingebunden
- Ein Container pro Benutzer
- komfortabel für uns: Container sind leicht zu erstellen
- kontrollierbar: Docker bietet viele Möglichkeiten zur Ressourcenbeschränkung



Klingt doch eigentlich gut..

Was muss man da noch bedenken?

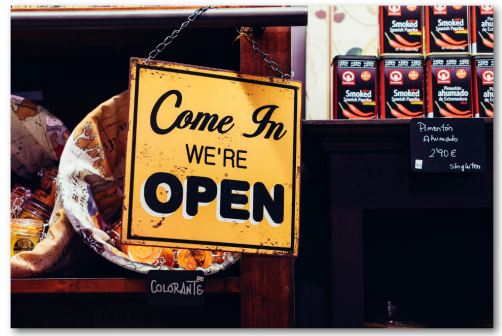
TRALIOS
Linux Server Management

- Wie bekommen wir den Benutzer da rein?
- Wann können wir alte Container entfernen?
- scp/sftp und direkte Kommandos
- Wie kann man Resourcenverbrauch einschränken?

Wie bekommen wir den Benutzer da rein?

TRALIOS
Linux Server Management

- Wir wollen ein Image für alle
- aber nur einen Benutzer pro Container
- Login nur per SSH-Key, der an ein Wrapper-Kommando gebunden wird
- beim Starten des Containers die Informationen zum Benutzer (UserID, Gruppen) ”einpacken” und im Container nutzen



Was muss man da noch bedenken?

TRALIOS
Linux Server Management

- Wie bekommen wir den Benutzer da rein? ✓
- Wann können wir alte Container entfernen?
- scp/sftp und direkte Kommandos
- Wie kann man Resourcenverbrauch einschränken?

Wann können wir alte Container entfernen?

TRALIOS
Linux Server Management

- Ein Container soll on-demand gestartet werden
- nicht benutzte Container sollen wieder weg
- Container beim Logout entfernen?
- Besser: Container nach Zeitspanne entfernen
- Noch besser: Zeitspanne bei Aktivität dynamisch verlängern

Was muss man da noch bedenken?

TRALIOS
Linux Server Management

- Wie bekommen wir den Benutzer da rein? ✓
- Wann können wir alte Container entfernen? ✓
- scp/sftp und direkte Kommandos
- Wie kann man Resourcenverbrauch einschränken?

scp/sftp und so..

TRALIOS
Linux Server Management

- scp ist einfach, startet nur das scp-Binary. Worked out of the box!
- sftp benutzt das sftp-Subsystem laut sshd-Config. Der Pfad unterscheidet sich je nach Distribution!
- sonstige Kommandos: auf das Home-Verzeichnis achten (cd ~; $cmd)

Was muss man da noch bedenken?

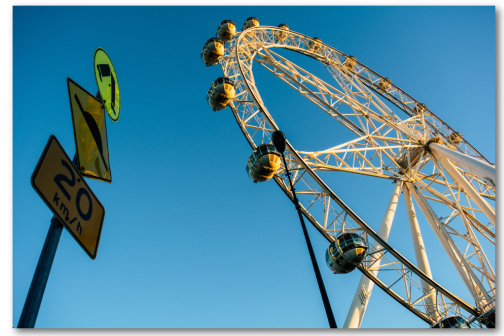
TRALIOS
Linux Server Management

- Wie bekommen wir den Benutzer da rein? ✓
- Wann können wir alte Container entfernen? ✓
- scp/sftp und direkte Kommandos ✓
- Wie kann man Resourcenverbrauch einschränken?

Resourcenverbrauch einschränken

TRALIOS
Linux Server Management

- direkt über Docker: CPU-Shares
- über cgroups: CPU, Memory, etc
- iptables: Netzwerkzugriff einschränken



Dieser Teil steht noch auf der TODO-Liste, sollte sich aber leicht umsetzen lassen

Was muss man da noch bedenken?

TRALIOS
Linux Server Management

- Wie bekommen wir den Benutzer da rein? ✓
- Kann das Weg oder brauchen wir das noch? Wann können wir einen Container entfernen? ✓
- scp/sftp und direkte Kommandos ✓
- Wie kann man Resourcenverbrauch einschränken? ...

Nächste Schritte

TRALIOS
Linux Server Management

- Resourcenbeschränkungen einbauen
- Code-Review
- eigene Tests
- Fremd-Tests (Betatest)
- Roll-out