

Technisches

Die Implementierung von Jails ist nicht auf das Userland begrenzt. So gibt es an zahlreichen sicherheitsrelevanten Stellen im Kernel Abfragen ob ein Prozess auf dem Hostsystem ausgeführt wird oder aber gejailed ist.

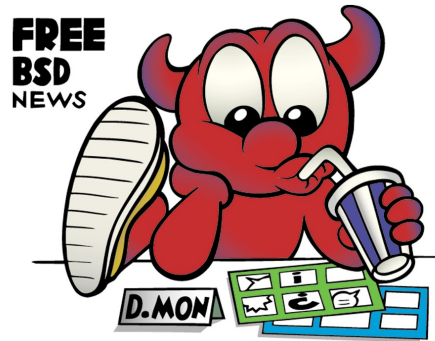
Eine Jail braucht in etwa 140MB auf Speicherplatz auf der Festplatte, je nachdem was in einer Jail installiert wird steigt auch der Speicherbedarf einer Jail. Es geht aber auch andersherum. So können viele Dateien aus einer Jail gelöscht werden bis nur noch der eigentliche Dienst in dieser bestehen bleibt.

Aus Sicht der Administration wird eine Jail wie jedes andere System behandelt. So kann man sich beispielsweise via SSH in diese einloggen und hat hiernach keinen Zugriff auf das Hostsystem. Aus Sicht des Hostsystem ist eine Jail ein Verzeichnis mit einer kompletten minimalen FreeBSD Installation auf welches Sie vom Hostsystem Zugriff haben.

Um mit der Jail zu arbeiten muss man sich aber nicht immer in die selbst einloggen, so kann man mit „jexec“ Dienste und Programme von Hostsystem aus in einer Jail starten und stoppen oder sich auch nur die Prozessliste in der Jail anzeigen lassen oder welche User eingeloggt sind.

Über das Hostsystem ist jeder Jailprozess in der Prozessliste mit einem „J“ gekennzeichnet. So ist für den Betreiber einer Jail, auch ohne login in die Jail, sofort ersichtliche welche Dienste auf dem Server ausgeführt werden.

Eine Jail unterliegt auch gewissen Restriktionen, die man, zum Teil, über das Hostsystem und den Kernel Variablen, sogenannten sysctl, verändern kann. So sind keine raw sockets (wie ping und traceroute) erlaubt, können aber über das Hostsystem, ebenso wie das Setzen des Hostnames, explizit für bestimmte, oder alle, Jails erlaubt werden. Eine der grössten Einschränkungen einer Jail ist aber, das eine Jail immer nur eine IP-Adresse zugewiesen werden kann. Dabei ist auch darauf zu achten dieser die Netzmaske /32 zuzuweisen.



FreeBSD

Jails

Weitere Informationen

Wir hoffen Ihnen mit dieser kurzen Übersicht eine verständliche Vorstellung der FreeBSD Jails gegeben zu haben.

Eine ausführliche Anleitung finden Sie unter:

<http://www.grunix.de/doku/howto/jails/index.html>

Die Manpage zu den Jails ist sehr gut geschrieben:

[man jail](man:jail)

Wenn Sie sich mehr für die Securityfeatures von FreeBSD interessieren, so erhalten Sie einen Überblick in den folgenden Flyern:

[Firewall](#) und [Sicherheit](#)

Allgemeine Informationen rund um FreeBSD erhalten Sie im FreeBSD handbook:

http://www.FreeBSD.org/doc/de_DE.ISO8859-1/books/handbook/index.html



Was sind Jails?

Kurz gesagt kann man Jails mit „chroot auf Steroiden“ umschreiben. Eine Jail geht aber deutlich weiter als eine chroot-Umgebung. So ist eine Jail ein komplettes eigenständiges FreeBSD-System, mit eigener IP-Adresse, innerhalb eines FreeBSD Systems, wobei diverse Restriktionen auf einen Prozess und dessen Kindprozesse gesetzt werden. Prozesse in einer Jail können somit nicht auf Prozesse des Hostsystem zugreifen.

Dabei wird keine Hardware emuliert (wie bei vmware) oder ein eigener Kernel (wie bei XEN) genutzt, eine Jail teilt sich die Ressourcen mit dem Hostsystem. ohne das das Hostsystem von Veränderungen, die innerhalb einer Jail stattfinden, betroffen ist. Aus diesem Grund ist der Jail Mechanismus anderen virtuellen Realisierungen in Sachen wie Performance überlegen (insbesondere, wenn mehrere virtuelle Instanzen genutzt werden sollen).

Die FreeBSD Jails gehören zum Basissystem und erhöhen die Sicherheit signifikant. Neben einem kompletten System kann aber auch nur ein Prozess, ein Dienst, in eine Jail eingesperrt werden. Eine Jail ist ein System für sich, sprich, es kann dort die gleiche Software installiert werden wie auf einer normalen FreeBSD Installation.

Serverdienste in Jails

Gerade Serverdienste wie DNS, HTTP, SMTP/POP3/IMAP, FTP und viele weitere, waren in der Vergangenheit oftmals die Schwachstelle im System, welche ein Hacker für einen erfolgreichen Angriff ausnutzte. Auch wenn man immer up-to-date bleibt und eine Firewall nutzt, so kann man die Risiken immer nur minimieren.

Um diese auf ein Minimum schrumpfen lassen bietet es sich an diese Serverdienste in eine Jail zu sperren. Sei es jeden Serverdienst in eine einzelne oder alle Dienste in eine Jail, Ihr Hostsystem wird im Falle eines Einbruchs über eine Schwachstelle eines Serverdienstes nicht beeinträchtigt werden.

Sicherheit durch Jails

Wenn ein Eindringling etwas verändert, wie können Sie dann sicher sein, das er nicht noch mehr Schaden angerichtet hat, oder gar eine backdoor installiert hat? Ihr System an sich ist sicher? Was ist aber mit den angegebenen Diensten? Sind Sie sicher das hier nicht ein Bug

vorhanden ist den ein Angreifer ausnutzen könnte um auf Ihr System einzudringen? Was ist mit der downtime Ihres Servers bis sie diesen wieder bereinigt oder gar neu aufgesetzt haben? Zeit ist Geld und mit einer Jail können Sie sich Mühe aber vor allem Geld ersparen. Wurde Ihr Webserver, welcher selbstverständlich in einer Jail läuft, kompromittiert, so suchen Sie nicht lange nach veränderten Dateien.

Sie stoppen die Jail, kopieren Ihre Backup-Jail an die Stelle der alten, und starten diese wieder. Dies wird nicht mehr als 1 Minute in Anspruch nehmen und Ihre Internetpräsenz ist wieder auf dem alten Stand. Danach können Sie offline die kompromittierte Jail untersuchen und den Fehler ausfindig machen.

Sie sehen, neben der richtigen Wahl des Betriebssystems, der Nutzung einer Firewall, eines IDS und weiteren Sicherheitsfeatures, sollten Sie auf die Möglichkeiten einer Jail nicht verzichten.

Ihr Server als Fort Knox

Sicher ist aber auch, das nichts wirklich sicher ist, auch wenn Hersteller diverser Firewalllösungen oftmals anderes versprechen. Firewalls sorgen für die erste Barriere, das System an sich für die zweite, wenn Sie Jails nutzen errichten Sie ein dritte Mauer und mit den FreeBSD security flags steht hinter dieser Mauer noch ein Tresor der keine Tür hat. Der Einbruch in ein System ist schon schlimm genug, durch die Nutzung einer Jail nehmen Sie schon viel von dem Schrecken, ärgerliche wird es wenn der Eindringling Daten verändert, Daten löscht und seine Spuren aus den diversen Logfiles löscht. Er braucht dazu administrative Rechte, als root Zugriff, und diesen bekommt er nicht? Was aber wenn doch? Er kann machen was er will, oder doch nicht?

Nein, das kann er nicht, denn durch die Nutzung von security flags können Sie Ihre Verzeichnisse und Dateien so bearbeiten, das nicht einmal mehr root diese zu verändern vermag. Wollen Sie auf diese Möglichkeit der Absicherung verzichten? Wohlkaum. Aber damit nicht genug, mit dem securelevel, welche man erhöhen kann, während des laufendes Betriebs aber nicht herabsetzen, kann auch verhindert werden, daß ein Eindringling die Firewallregeln modifiziert, Kernelmodule lädt oder entlädt oder Disks zum schreiben öffnet. Mehr zu security flags und securelevel erfahren Sie im entsprechenden Dokument.

Eine Jail kann mehr

Sicher dient eine Jail in erster Linie dazu das System sicherer zu machen, die weiteren Vorteile liegen aber auf der Hand.

- So können mehrere virtuelle Server, mit unterschiedlichen Diensten, auf einem Server betrieben werden. So lässt sich eine Demilitarisierte Zone (DMZ) nur mit Jails auf einem Server aufbauen.
- Serverdienste sind meist sehr umfangreich und werden daher meist nicht von einem Administrator betreut. Entweder es haben mehrere User root-Rechte, oder Sie müssen mit Dingen wie „sudo“ experimentieren. Lagern Sie alle Dienste in eine Jail aus, so kann jeder Administrator seine Jail und seinen Dienst pflegen ohne das andere darauf Zugriff haben.
- Sie brauchen eine Testumgebung für Ihren Entwickler? Warum extra einen Server einrichten, ganz zu schweigen was die Kosten der Hardware angeht. Richten Sie Ihrem Entwickler eine Jail ein und er kann, ohne das Hostsystem zu beeinträchtigen, in dieser Schalten und Walten.
- Bei Schulungen müssen nicht alle Teilnehmer auf dem gleichen Server arbeiten, sie können diesen jeweils eine Jail einrichten in der Sie die gestellten Aufgaben erarbeiten können. Wenn die Schulung beendet ist muss nicht der komplette Server neu aufgesetzt werden, es reicht aus einfach neue Jails an die Stelle der alten zu kopieren, das System der Jails ist wieder sauber.
- Will man seinen Kunden root-shells anbieten, kann man dies auf einem Server und vielen Jails für viele Kunden abwickeln. Die Anschaffung neuer Hardware entfällt, die Einrichtung ist eine Angelegenheit von Minuten (oder wird automatisiert).
- Sie sehen, neben dem mehr an Sicherheit bieten Jails die Möglichkeit Dienste und virtuelle Server besser aufzuteilen, was die Übersicht verbessert, und vorallem können Sie Ihnen auch helfen Geld für den auf neuer Hardware zu ersparen.