サーバ公開勘所 -自分はこうしてます編-



- 誰もが気にするセキュリティー周り
- 特にOSやミドルウェアの話を共有したい!

→ こんなこと考えてます

- 3W1Hを明確に
- 最新版を追いかける
- 登場人物と役割を決める
- ソフトを知ってさらに固める



3W1Hを明確に

誰が いつ 何処 から どう 使うか

- サーバの最小構成が決まる
- 「やってはいけない事」がハッキリする

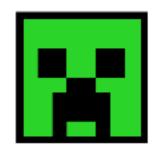


● 我が家の要望は・・・

- 誰 who
 - 自分と他友人2人くらい
- 何処 / いつ where/when
 - 。いつでも、日本国内のどこからでも
- どう使う how
 - 作ったサイトの実験場が欲しい!
 - ファイルの共有場所あったら便利だよね!
 - 専用wikiとかどうですか!
 - ∘ Minecraftしたい!



★ そんな我が家のサーバ構成



Minecrafut







PHP - FPM





freeBSD.

サーバの構成が決まったらインストールしていく

➡最新版を追いかける

最初はOSについて

- 特別な理由がない限り、 できるだけ最新のものがよいです。
- パッチもどんどん出るので インストール直後は最新化する。

● 我が家のOSはバージョン何?

BSDは uname -a で確認。

[gh123or456@kuma_da_kuma ~]\$ uname -a FreeBSD kuma_da_kuma 9.3-RELEASE-p30 f usr/obj/usr/src/sys/GENERIC amd64

サポートが終了したリリース

これまでのサリースのサリース日、分類、保守終了日 (End Of Life (FOL)) の完全が情報は、FreeBSD セキュリティ情報 の サポートが終了。 <u>レたサリース</u> にまとめられています。

- 11.0 (2016年 10月) アナウンス: リリースノート: インストールガイド: ハードウェアノート: Readme: Linata (正説表): チェックリム
- 10.2 (2015 年 8 月) アナウンス: リリースノート: インストールガイド: ハードウェアノート: Readme: Linata (正調表)
- 10.1 (2014年 11月) <u>アナウンス</u>: <u>リリースノート</u>: <u>インストールガイド</u>: <u>ハードウェアノート</u>: <u>Readme</u>: <u>Errata (正誤表)</u>
- 10.0 (2014年1月) <u>アナウンス: リリースノート: インストールガイド: ハードウェアノート</u>: <u>Readme</u>: <u>Errata (正器表)</u>.
- 9.3 (2014年 7月) <u>アナウンス: リリースフート: インストールガイド</u>: <u>ハードウェアフート RLADML</u>: <u>Lrrata (正誤表)</u>.
- 9.2 (2013 中 9 月) アプウンス: リリースノート: インストールガイド: ハードウェアノート README: Ectata (正説表)
- **9.1** (2012 年 12 月) <u>アナウンス</u>: <u>リリースノート</u>: <u>インストールガイド</u>: <u>ハードウェアノート *README*: *Errata* (止誤表)</u>

●OS最新化とパッチ充て

基本的に公式サイトに載っている通りにやる

- OSのメジャーアップデート freebsd-update -r 11.1-RELEASE upgrade
- セキュリティパッチの適用 freebsd-update install

```
[gh123or456@kuma_da_kuma ~]$ freebsd-version
11.1-RELEASE-p7
[gh123or456@kuma_da_kuma ~]$ <mark>|</mark>
```

コマンドごと変わった

ルソフトのインストール

パッケージ管理ソフトに頼る

- 管理ツールのDB更新 pkg update -f
- ソフトをインストールする pkg install nginx

ここで構成管理ツール(Ansibleとか)を使うのもあり

一古いソフトの更新

- 管理ツールから最新版があるか確認できる pkg version -l '<'
- まとめて更新 pkg upgrade

手動でソースからインストールしていたりすると 管理ツールの監視から外れるので 難易度が跳ね上がる。上級者向け。

一登場人物と役割を決める

各ユーザの使い方を明確にすること

- 管理者、作業者、システムユーザ、など 各ユーザのできることは明確にする。
- sudoを使ってコマンド単位で委任するのが定石-> ありがちなのは、すべてのコマンドをsudoできる影の管理者

一登場人物と役割を決める

不要なユーザはnologinにしてしまうか削除する。

- ありがちなのは、 「guest」「test」「admin」「tomcat」など?
- 参考
 不要なデフォルト・ユーザー・アカウントの除去 (IBMの記事)

メジャーなソフトのメジャーな対応

ソフトによってはセキュリティを高められる 機能があるので活用していく。

- sshd
 - ∘ ポート変更
 - rootログインの拒否
 - 鍵認証
 - ∘ パスワードログインの拒否

- nginx
 - ∘ 応答に余計な情報を載せないようにする server_tokens off などなど
 - ファイルの公開決定
 - 。 SSL対応
 - etc etc etc.....

できることが多すぎるので、外部の評価ツールに 頼るのがよいかと思う

メジャーな脆弱性対応

話題になりそうなものは適宜対応する 自分が当てにするのは以下

- 脆弱性の特設サイト
- IPA先生のアナウンス
- OSの公式サイト(セキュリティパッチ)
- ソフトのサイト
- VPSを借りてるサイトのアナウンス(さくら)
- CVE/JNV

我が家はこんな状況でした

脆弱性	状況
POODLE	SSL3.0は無効にした
ShellShock	bashは更新済み
Heartbleed	OpenSSL更新済み
GHOST	我が家はBSD 危険性低め
Dirty COW	我が家はBSD
KRACKs	VPSなのでついてない
BlueBorne	VPSなのでついてない
MELTDOWN	アップデートして祈る
SPECTRE	アップデートして祈る

通信の制限

ファイアウォールによるポート、プロトコル制限

- iptable
- pf

ウェブサーバなら受信拒否

- IP やMacアドレスではじく
- クライアント認証

定期的なログ確認

外部とやり取りするソフトはアクセスログを 残せることが多いので定期的に確認する。

- sshdなど-> auth.log
- nginx -> access.log
- pf -> pflog

access.log

```
[20/Mar/2018:21:05:09 +0900] "Get /art/intex.php H TP/1.0" 404 10 "-" "Mozi Te/5.0"
67,108,249,199
                "Mozi It/b.0"
67, 106, 246, 196
                [207Man/2018:21:05:09 (0:001] "R = 7-PA/index.php L (P/1.01 404 18
67, 06,246,196
                [20]/Mai/2018:21:06: 0 #0900] GFT /onany/index.php FTTP/ .01 /04
67. 08.248.198.
                [20/Mar/2013;21:05; | 1 +0900] | GET /charty2/ index.php HTTY1.01 404.
                    Mar/2013:21:05: | +1910] GET /mysql/incex.php hTT7/ .17
                [207ktar/2013:21:05:11 +0900] "Ge /adm t/index.php F 1 91.
                [20/Mar/2018:21:05:12 (0000] "GL /ob/ hdow.php (H F/1.01 404 16)
67,106,249,199
                   67, 106, 246, 196
67, 106, 246, 196
                [20]/Mai /2018:21:05:13 (0:00] "B = /oks/cheNyAcrin/ index.phc = L P/1.0" 404-16 [
                [20]/Mai/2018:21:05: 3 (0900] "GTT Zachim/zma/inde-uphp HTTF/ .0" 404 16 " "
[20]/Mai/2018:21:05: 3 +0900] GET Zachim/PMA/index.php HTTF/ .0" 404 16 -1
67. 06.246.196
67, 06,249,199
                [20]/Har/2013:21:05: / +0900] GET /adm //mysql/index.php HTT7/ .07 404
                [20/kkm/2013:21:05:14 +0800] "GET /admin/mysql2/index.php -TTP/1.0" 404 16
                [20/Mair/2018:21:05:15 +0000] "Ge //admin/ahproyachin/indok.aha -1 P/1.0" 404 15
67,103,248,198
                67,106,249,199
                [90/Mai/90Be21:0be16 (0.00] "Bit /Arthrit/Chprisserin//index.php II 1-/1.07 404 18
67, 106, 246, 196
67. 06.246.196
                [2078bar/2018:21:05: 6 (0900] GTT /my-ql admin/index.pnp HTTF/ .07 404 6
67, 06,246,196
                [20/Mar/2013:21:05: 7 +0900] GFT /chcapmin/ rdex.php HTTV1.01 404 IB 11-
67. OS. 248. ISS H
```

auth.log

```
input userauth request: inval d user deploy [preauth]
imput usensuth request: inval d user user [preauth]
input userauth request: inval diuser user [preauth]
imput usensuth request: inval d user miner [preauth]
input userauth_request: inval d user test [preauth]
imput userauth request: inval d user ethos [preauth]
input userauth request: inval d user ethos [preauth]
imput usensuth request: inval d user miner [preauth]
input userauth request: inval d user ethos [preauth]
imput usenauth request: inval d user ethos [preauth]
input_userauth_request: inval d user ansible [preauth]
imput userauth request: inval d user rig [preauth]
input userauth request: inval d user rig [preauth]
imput usensuth request: inval d user test [preauth]
input_userauth_request: inval d user user [preauth]
imput usensuth request: inval d user support [preauth]
input_userauth_request: inval d user ?lomSplp [preauth]
imput userauth request: inval d user ftbuser [preauth]
input userauth request: inval d user ubuntu [preauth]
imput_userauth_request: inval d user torcat [preauth]
```

auth.log

```
input ascreath requests invalled ascriredia (presach)
input userauth request: inval d user radio [preauth]
input ascreath regassit invalid ascriredio [presath]
input_userauth_request: inval d user bot1 [preauth]
input ascreath regassits invalid ascribett [preadth]
input_userauth_request: inval d user bot1 [preauth]
input ascreath regassits invalid ascriuser [preadth]
input userauth request: inval d user bot1 [preauth]
input ascreath request: inval diascridebley [preauth]
input userauth request: inval diuser deploy [preauth]
input ascreath reguests invalid ascridebley [preauth]
input userauth request: inval d user deploy [preauth]
input ascreath requests invalid ascridebley [preauth]
input userauth request: inval d user deploy [preauth]
input ascreath requests invalid ascriminecraft [preaath]
input userauth request: inval diuser hive [preauth]
imput ascreath request: inval diascriminecraft [preaath]
input userauth request: inval diuser mineuraft (preauth)
input ascreath requests invalid ascrininceraft [preaath]
input userauth request: inval diuser minecraft [preauth]
input ascreath reguests invalid ascrininceraft [presach]
```

★まとめ

- 結局コツコツ当たり前の事をやるしかない
- 気づける仕組みを知っておくことが大切

最後に

Q.今の時代、サーバ持つ意味あるんですかね・・・? A.ないです。 ないけど魅力はあるので、是非。