SysAdm: FreeBSD Administration Made Easy

Ken Moore
Senior TrueOS Developer

March 5th, 2017
SCALE 15x
Pasadena, CA

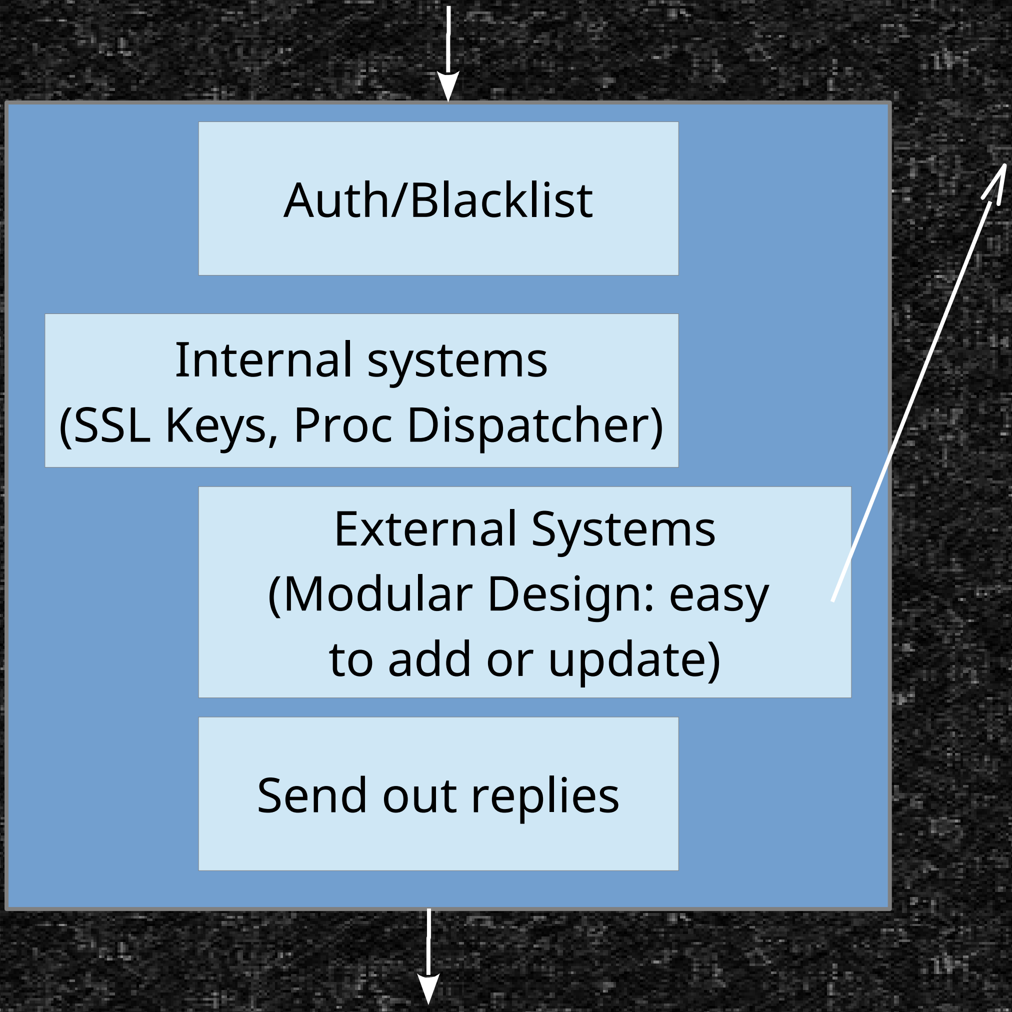
Introduction

- New tool created by the TrueOS developers for administrating FreeBSD systems.
- Comes in three parts
  - SysAdm Server (FreeBSD only)
  - SysAdm Client (Cross-platform)
  - SysAdm Bridge (still in development)

SysAdm Server

- The server is the brains of the project and is the “middleware” component used to facilitate the interactions between the user and the system.
- The binary can be run in two modes: a tcp/REST server or a websocket/JSON server. Both modes can run at the same time on different sockets for multiple access methods.
- The server has no internal database. All information received from the server about the system and all changes to the system are performed directly on the system itself. This allows it to complement traditional SSH access/management of the system rather than work against it.

SysAdm Server



Auth/Blacklist
Internal systems (SSL Keys, Proc Dispatcher)
External Systems (Modular Design: easy to add or update)
Send out replies

Some Current “classes”:

- User Manager (pw)
- Service Manager (service)
- Firewall Manager (ipfw)
- iocage Jails (iocage)
- iohyve VM's (iohyve)
- Data Backup (lpreserver)
- Update Manager (pc-updatemanager)
- Package Manager (pkg)

Full List available at:
http://api.sysadm.us

SysAdm Server: Security

- Latest TLS transport encryption (https or wss)
- Authentication via username/password **OR** external SSL public/private key pair
- Strict connection timeouts and blacklisting
- Privilege separation between full/limited access to subsystems (wheel/operator groups)
- Ability to disable user/pass authentication system and require pre-shared SSL key access.

SysAdm Server: Websocket vs REST

Websocket

- Long-lived connection
- Pure JSON input/output
- Authenticate once with timeout or disconnection from inactivity.
- Spontaneous "events" can be obtained from the system for notifications or status updates

REST

- Single-request connection
- Mixture of REST w/ JSON
- Authenticate with user/pass only, on every request

SysAdm Server: Websocket vs REST

Websocket

- API Example Call:

```
{
  “namespace” : “rpc”,
  “name”:”query”,
  “id”:”UniqueID”,
  “args”:{}
}
```

REST

- API Example Call:

```
GET rpc/query <version>
Authorization:<base64>
{<JSON args>}
```

SysAdm Client

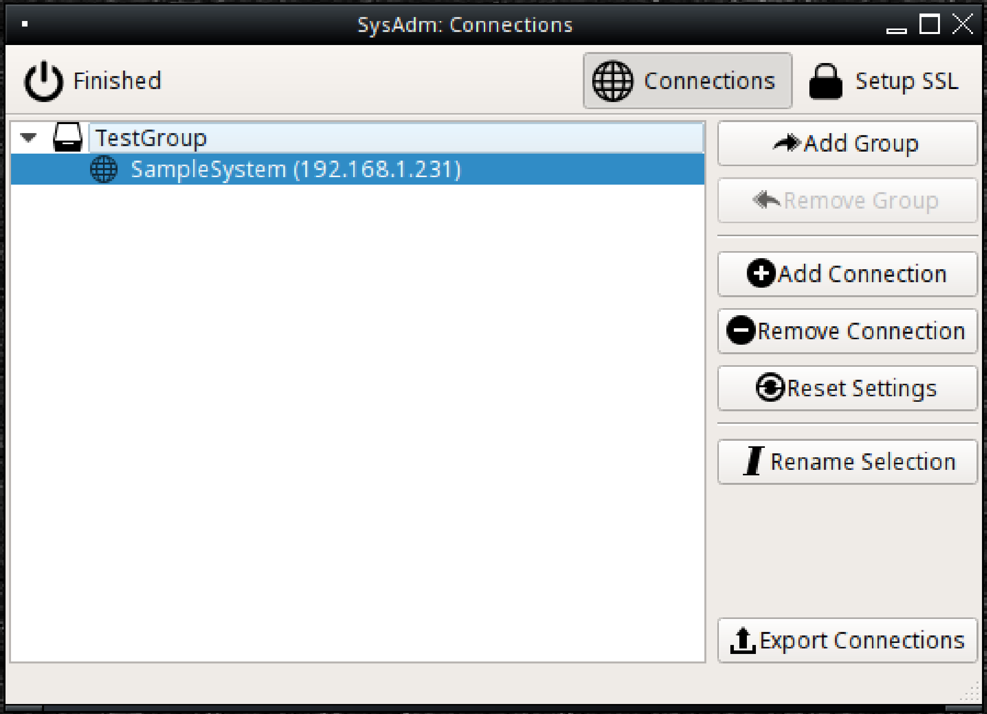
- Graphical client written purely in Qt5
- Fully cross-platform (FreeBSD, Windows, and OSX builds are automated right now)
- Multi-System Management:
  - Setup connections to multiple SysAdm servers/systems
  - Keep informed with regular system health checks
  - Arrange logical “groups” of systems for ease of use in large deployments (Group management operations coming soon!)
  - Localhost connections do not require internet access (TrueOS)

SysAdm Client: Security

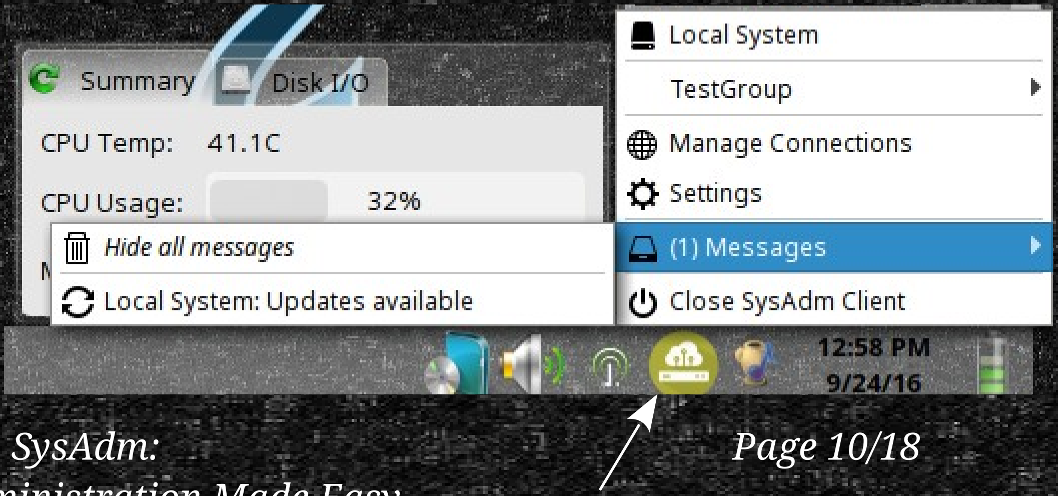
- Generates unique SSL public/private keys for the client
- Uses secure websockets to talk to the servers (user/password required for first-time connection – SSL certs automatically registered and used after that).
- All client SSL certificates and keys are locked on the client system within an encrypted file. User-defined password required to unlock that file and initiate server connections.
- Export/Import your client settings across various client and operating systems while still fully-encrypted.

SysAdm Client: Examples

- Connection Manager
  - Used to create client SSL keys and setup connections to servers.

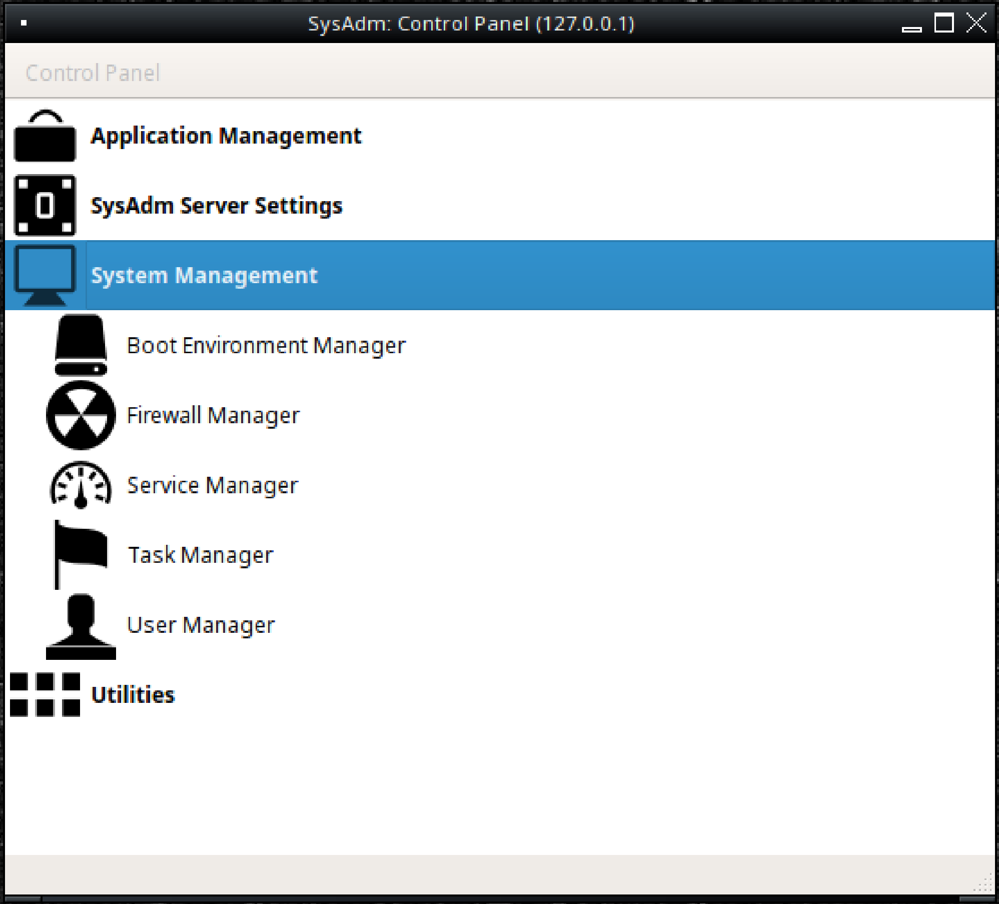


- Tray Interface
  - See messages and system information at a glance.



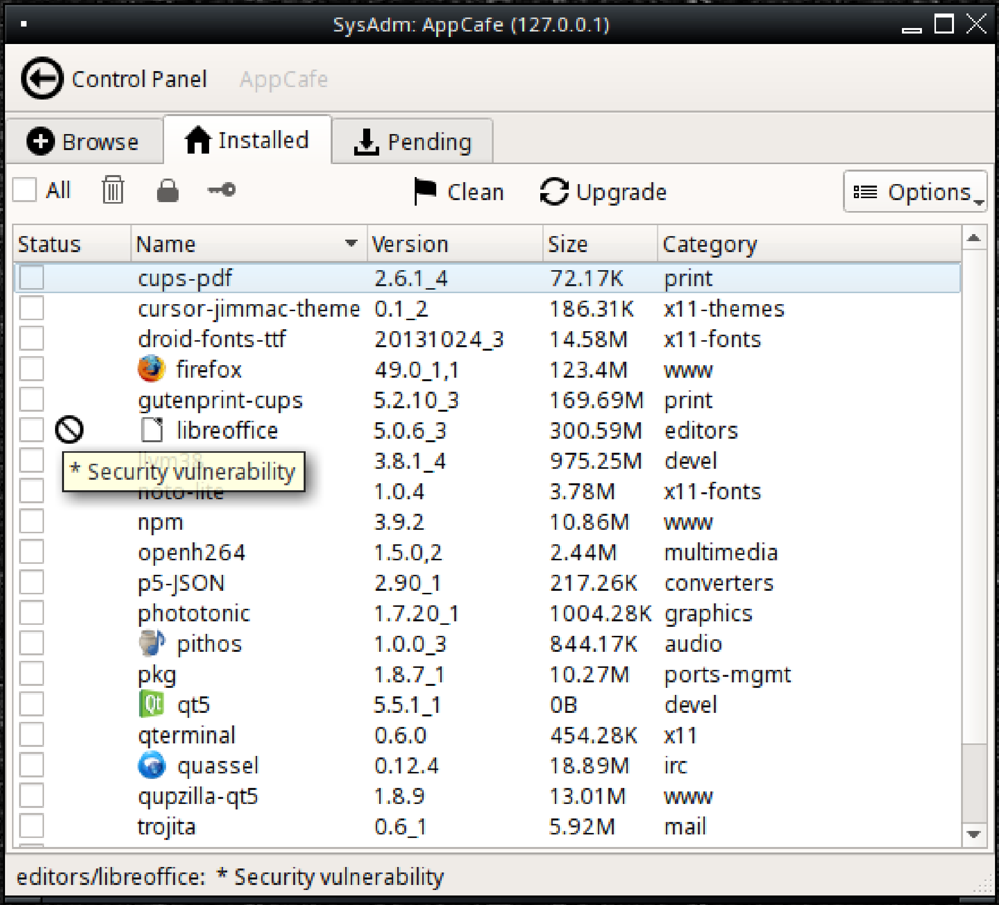
SysAdm Client: Examples

- Control Panel (main page)
  - This lists all the various systems that the user has access to on the system.
  - Many options (especially in the "utilities" category) will not appear unless the relevant utility is installed on the server.



SysAdm Client: Examples

- Package Manager (AppCafe)
  - Graphical interface to the *pkg* utility and database on the server.
  - It allows the user to browse and search for packages, perform updates, [un]install packages, and check for security issues with the installed packages.



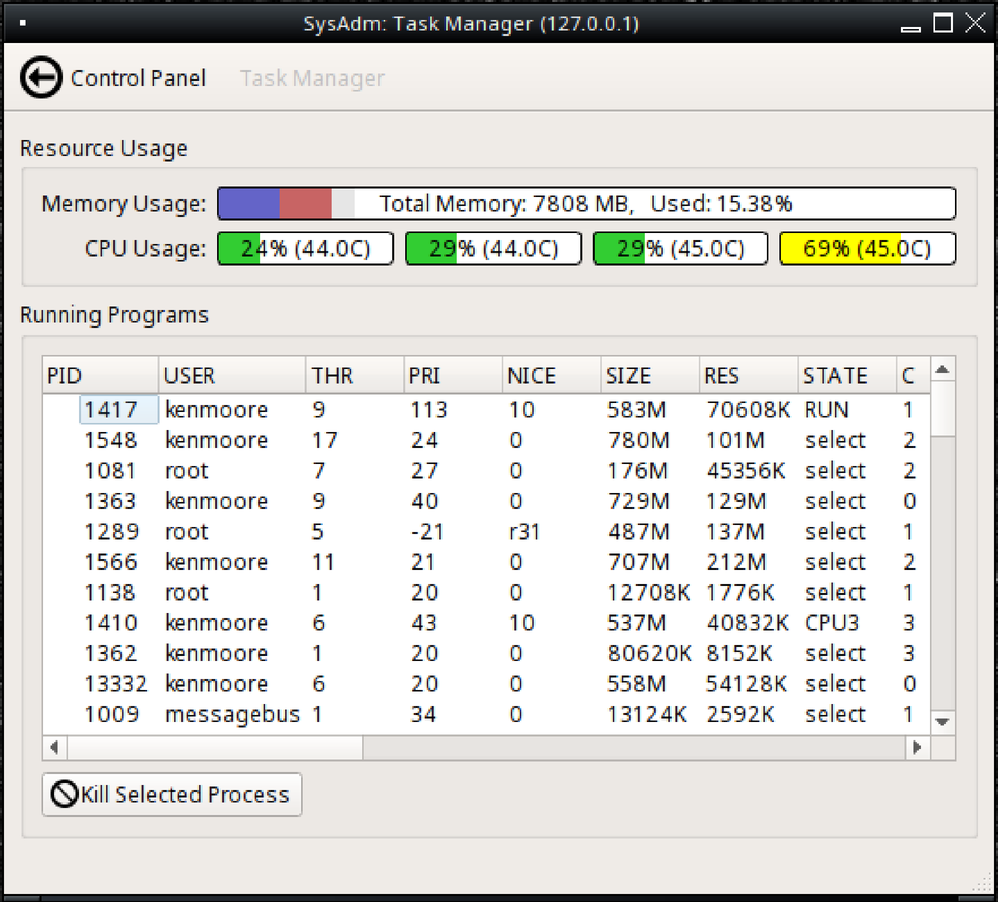
Status	Name	Version	Size	Category
	cups-pdf	2.6.1_4	72.17K	print
	cursor-jimmac-theme	0.1_2	186.31K	x11-themes
	droid-fonts-ttf	20131024_3	14.58M	x11-fonts
	firefox	49.0_1,1	123.4M	www
	gutenprint-cups	5.2.10_3	169.69M	print
⃠	libreoffice	5.0.6_3	300.59M	editors
	llvm38	3.8.1_4	975.25M	devel
	noto-lite	1.0.4	3.78M	x11-fonts
	npm	3.9.2	10.86M	www
	openh264	1.5.0,2	2.44M	multimedia
	p5-JSON	2.90_1	217.26K	converters
	phototonic	1.7.20_1	1004.28K	graphics
	pithos	1.0.0_3	844.17K	audio
	pkg	1.8.7_1	10.27M	ports-mgmt
	qt5	5.5.1_1	0B	devel
	qterminal	0.6.0	454.28K	x11
	quassel	0.12.4	18.89M	irc
	qupzilla-qt5	1.8.9	13.01M	www
	trojita	0.6_1	5.92M	mail

* Security vulnerability

editors/libreoffice: * Security vulnerability

SysAdm Client: Examples

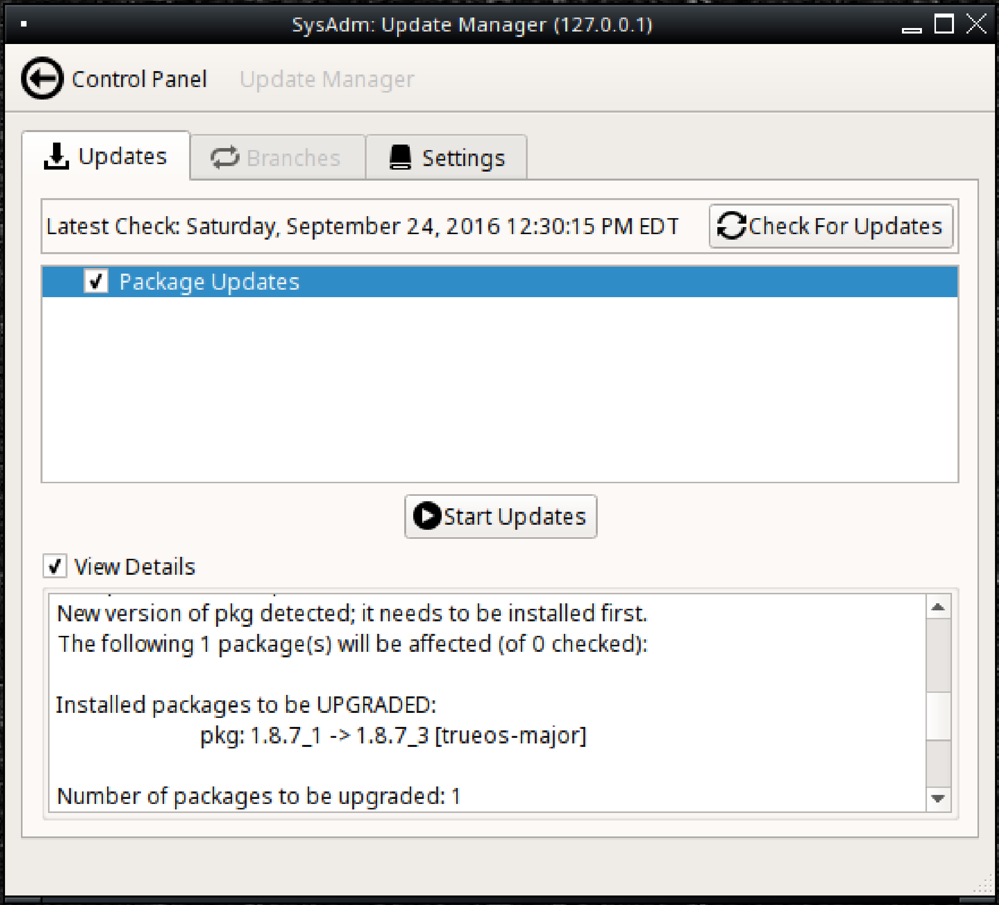
- Task Manager
  - Basically a visual version of *top* on FreeBSD (without running *top*)
  - View CPU usage and temperature per-core, overall memory usage, and individual process statistics (with the ability to kill processes as needed)



PID	USER	THR	PRI	NICE	SIZE	RES	STATE	C
1417	kenmoore	9	113	10	583M	70608K	RUN	1
1548	kenmoore	17	24	0	780M	101M	select	2
1081	root	7	27	0	176M	45356K	select	2
1363	kenmoore	9	40	0	729M	129M	select	0
1289	root	5	-21	r31	487M	137M	select	1
1566	kenmoore	11	21	0	707M	212M	select	2
1138	root	1	20	0	12708K	1776K	select	1
1410	kenmoore	6	43	10	537M	40832K	CPU3	3
1362	kenmoore	1	20	0	80620K	8152K	select	3
13332	kenmoore	6	20	0	558M	54128K	select	0
1009	messagebus	1	34	0	13124K	2592K	select	1

SysAdm Client: Examples

- Update Manager (pc-updatemanager)
  - Check, view, and manage updates on a TrueOS system.
  - Uses ZFS w/ boot environments for safely performing changes without touching the live system.



Latest Check: Saturday, September 24, 2016 12:30:15 PM EDT

```
New version of pkg detected; it needs to be installed first.
The following 1 package(s) will be affected (of 0 checked):

Installed packages to be UPGRADED:
        pkg: 1.8.7_1 -> 1.8.7_3 [trueos-major]

Number of packages to be upgraded: 1
```

SysAdm Bridge (experimental)

- What about servers with dynamic addressing?
- What about servers behind a corporate firewall?
- The SysAdm bridge is an additional type of server designed to be run on a small, statically-assigned, publicly available system (such as a small VM in the cloud). Both servers and clients may be configured to “announce” themselves on a bridge, and make connections from there.

SysAdm Bridge: Security

- The bridge is designed as a completely **untrusted** relay. Servers and clients use a completely separate SSL certificate when talking to a bridge to ensure the “real” one is never used for connecting to an unknown system.
- After connecting to a bridge, the server/client submit the MD5 of their real SSL certificate and the bridge responds with the ID and location of the systems who listed that MD5 within their compatible certificate list.

Conclusions

- SysAdm is a new framework designed to assist in the administration of any number of FreeBSD/TrueOS systems.
- It does not replace years of “muscle memory” from system administrators who use SSH/terminal access for everything. Rather it is designed to come alongside and provide an alternate/easier way to perform many of those routine tasks.
- SysAdm is already used for all TrueOS systems (both desktops and servers) and is constantly being improved with new API classes and corresponding client pages.

Questions?

- Links for additional information

  https://api.sysadm.us (SysAdm API Reference)

  https://www.trueos.org (TrueOS Website)