WHITE PAPER

TrueNAS® 13.0 Security

TrueNAS is an enterprise-grade storage system that delivers unified block, file, and object storage to many organizations across many industries. TrueCommand is an associated single pane of glass management product that provides additional security capabilities for TrueNAS systems. This white paper addresses both products which are developed and supported by iXsystems. This white paper does not address the TrueNAS SCALE software, with or without an Enterprise license.

Security and data protection are very important to many industries using TrueNAS, including federal government departments, healthcare providers, and financial institutions. iXsystems understands these requirements and invests significantly in monitoring vulnerabilities, understanding security attacks, meeting the relevant security standards, partnering with companies that provide security technologies, and reducing security risks for our clients. This document is intended to help security professionals understand TrueNAS, TrueCommand, and their security capabilities.

TrueNAS functionality is software-defined and built using many Open Source components. TrueNAS software is also available in Open Source form to its users and the development community. This open model enables users and industry to be assured that the software is secure and does not have backdoors or other vulnerabilities that may compromise its security or provide access to user data.

TrueCommand is a multi-system management application, which helps control and monitor your TrueNAS storage. It assists in managing the TrueNAS systems via REST APIs, WebSocket APIs, and a web user interface. It also administers the users and groups that may manage each TrueNAS system. A web proxy service is provided to each TrueNAS system which provides password security and audit logs of all configuration changes. While TrueCommand is not an Open Source project, the software can be made available for inspection.

iXsystems has implemented reasonable administrative, technical, and physical safeguards to help protect against security incidents and privacy breaches involving an iXsystems product provided those products are used in accordance with iXsystems instructions for use. However, as systems and threats evolve, no system can be protected against all vulnerabilities and we consider our customers the most important partner in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins, and/or responsible disclosures to customers and regulators. iXsystems continuously strives to improve security and privacy throughout the product lifecycle using practices such as:

- Privacy and security by design
- Product and supplier risk assessment
- Vulnerability and patch management
- Secure coding practices and analysis
- Vulnerability scanning and third-party testing
- Access controls appropriate to customer data
- Rapid incident response
- Clear paths for two-way communication between customers and iXsystems

The purpose of this document is to detail how iXsystems security and privacy practices have been applied to TrueNAS, what you should know about security maintenance for this product, and how we can partner with you to ensure security throughout this product's lifecycle. If you would like to report a potential product-related privacy or security issue (incident, breach or vulnerability), please use the online Security Disclosure Form at https://security.ixsystems.com/ or contact our Security Team at security@ixsystems.com

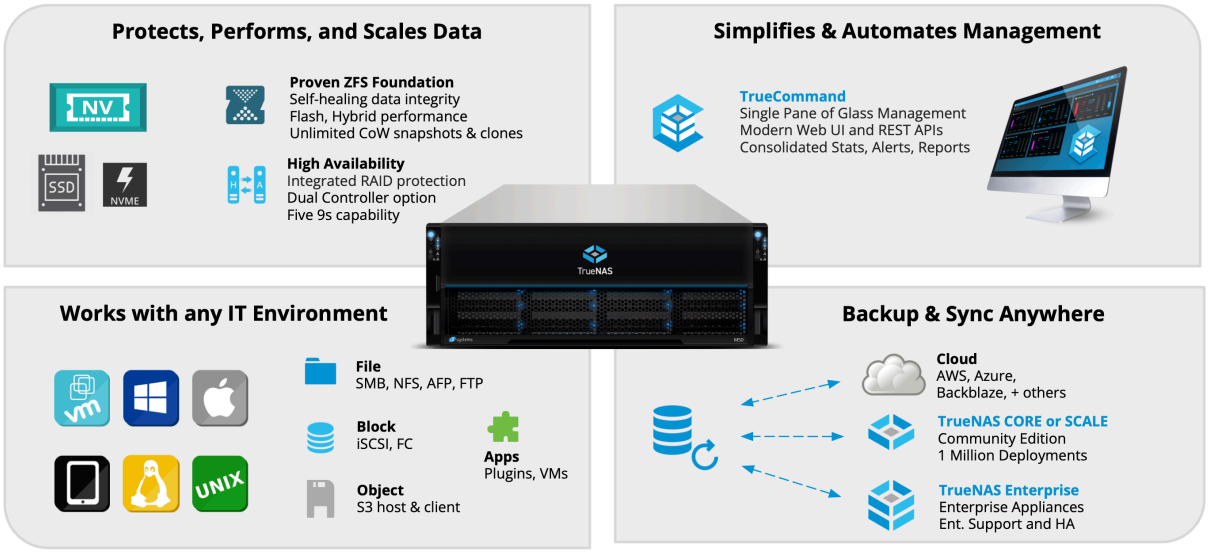
CONTENTS

1 Product Description

TrueNAS is a unified storage system which supports block, file, and object storage services. There are three primary platforms: the M-Series, the R-Series, and the X-Series. The TrueNAS software runs on these platforms and is managed by TrueCommand, a single pane of glass management system. This document covers:

- TrueNAS M-Series
- TrueNAS 13.0-U5.1 release - this includes FreeBSD 13.1-RELEASE-p7 as its OS
- TrueCommand 2.0 release

Below is a diagram describing the key functions and capabilities of TrueNAS.



2 Hardware Specifications

The M-Series is built using the following hardware:

- M-Series Chassis: 4U with optional NVMe drive bays
- Intel® Scalable Xeon® Processors: 10/16 Core
- DDR4 RAM - 64 to 768 GB (model dependent)
- Chelsio NICs - 10/25/40/100 GbE
- Broadcom 9300 Series SAS HBAs - 8e or 8i
- SuperMicro X11 Motherboard and BMC
- Power supplies: 1200 - 1600W CRPS

The TrueNAS X-Series has the same software as the TrueNAS M-Series but uses more compact and lower power hardware specifications:

- X-Series Chassis: 2U with 12 × 3.5” SAS drive bays
- Intel® Xeon® Processors: 6 Core
- DDR4 RAM - 32 or 64 GB
- Chelsio/Intel® NICs - 10/25/40 GbE
- Celestica Motherboard and BMC
- Power supplies: 500W

3 Operating System and Software Components

TrueNAS Enterprise 13.0 is built from FreeBSD 13-RELEASE and expands on the features provided in the Open Source TrueNAS CORE 13.0 release. Apart from the OS, this software includes a number of Open Source components (libraries and modules) from third parties as indicated in Appendix A.

TrueNAS 13.0 also provides the ability to add and run optional software from third parties through the "Plugin" system, or arbitrary software through the FreeBSD "jails" system. This additional software is not covered by this document, and additional software delivered via plugin or jail should be separately validated.

4 Network Ports and Services

TrueNAS provides a range of different storage services and uses TCP/IP for both data and management. The TCP ports and services that are listened for are:

Inbound Port	Protocol	Service Name	Description of Service	Encrypted	Defaults
80/443	TCP	HTTP/HTTPS	Web interface REST API WebSockets API	Optional	Open
22	TCP	SSH/SFTP	Secure Shell Secure FTP ZFS Replication Rsync over SSH	Yes	Closed
111/2049	TCP/UDP	NFS v3	Network File Service	No	Closed
137/138/139/445	TCP/UDP	SMB	Windows File Service	Optional	Closed
548	TCP	AFP	Apple File Service	No	Closed
20/21	TCP	FTP	File Transfer Protocol	No	Closed
443	TCP	WebDAV	HTTPS access to files	Yes	Closed
3260	TCP	iSCSI	Block storage over IP	Optional	Closed
9000	TCP	S3 API	Object storage over IP	Yes	Closed
837	TCP	Rsync	Remote synchronization	Optional	Closed
Not defined	UDP	Wireguard	Point-to-point encryption	Yes	Closed
161/162	TCP	SNMP	Simple Network Monitoring	Optional	Closed

Protocols that are “outgoing” do not listen and accept incoming connections. These protocols and ports are not a security risk and are usually allowed through firewalls. The primary protocols used that may need to be permitted through a firewall are:

Outbound Port	Protocol	Service Name	Description of Service	Encrypted	Defaults
80/443	TCP	HTTP/HTTPS	Software updates and Pro-active support	Optional	Open
25/465	TCP	Sendmail/TLS	Send emails for alerts	No	Outgoing
123	TCP	NTP	Network Time synchronization	Yes	Outgoing
514	TCP	Syslog	Logging of alerts and changes	No	Outgoing

All protocols can be securely encrypted and routed via VPN technologies. This approach is encouraged when using services directly over the Internet or WAN.

5 Transmission of Sensitive Data

TrueNAS transmits user data and administrative data, both of which may be sensitive and valuable. Encryption may be used for some protocols. All protocols can be encrypted via VPN technologies.

Administrative data includes the following:

- HTTP, HTTPS: Configuration and user login data
- SSH: User login information
- SMTP: Alerts and reports
- Syslog: Alerts and diagnostics
- SMB (RPC): Monitoring and configuration
- SNMP: Monitoring and alerts
- REST: Configuration and monitoring
- Websockets: Configuration and monitoring
- Kerberos: User authentication
- LDAP: User authorization

User data is controlled by users and not by TrueNAS. The following protocols are used:

- SMB: User files
- NFS v3/v4: User files
- AFP: User files
- FTP: User files
- WebDAV: User files
- iSCSI: Block data
- FC: Block data
- S3: Object data
- ZFS Replication: any user data
- Rsync: User file replication

6 Storage of Sensitive Data

TrueNAS stores user data and administrative data, both of which may be sensitive and valuable. Encryption may be used. Self-Encrypting Drives (SEDs) are recommended.

Administrative data includes the following:

- FreeBSD configuration
- ZFS file system configuration
- Protocol configuration
- User authentication configuration (e.g., LDAP or AD access)
- Statistics and alerts
- Log data
- MD4 hash of SMB user password

User data is controlled by users and not by TrueNAS. All data within TrueNAS is stored via ZFS. Data can be encrypted by users through:

- Self-Encrypting Drives (SEDs) using the TCG OPAL standard (FIPS 140-2 compliant drives are also available)
- Software encryption of drives (for pools imported from TrueNAS 11.x or earlier)
- Encryption of specific pools or datasets
- KMIP is supported

7 Network and Data Flow Diagram

The flow of data through a TrueNAS system has multiple paths. The primary aspects of the paths are:

TCP/IP: This includes both Ethernet and VPN technology. Proper networking best-practices should be followed to ensure the security of the network to which TrueNAS is connected.

Administration: The TrueNAS platform is managed periodically through the same TCP/IP stack but can be different Ethernet ports. Data does not flow through the Administration software.

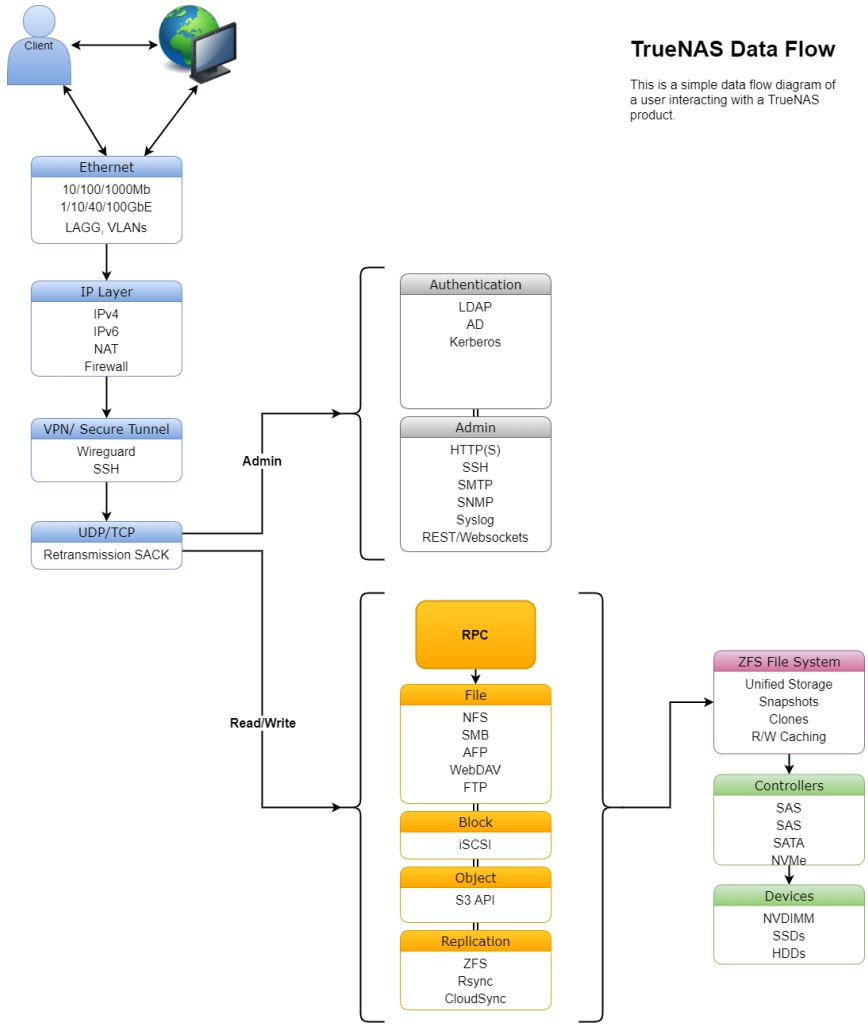
Authentication: Individual users are authenticated using protocols such as LDAP, Active Directory, or Kerberos. Once a user is authenticated and a session is established, data does not flow through the authentication software.

Data Services: File, block, and object services can be used to read and write data. Each user session will use one of these services.

ZFS File System: All data is accessed and managed through ZFS which provides a unified storage pool. If necessary, multiple pools can be leveraged for further isolation of data services.

Storage Devices: Each system has a set of controllers (physical or virtual) and devices such as HDDs, SSDs, and NVDIMMs to store its data.

The diagram below is an approximation of the TrueNAS dataflow.



8 Authentication and Authorization

TrueNAS provides the ability to manage users and groups on each system or to use LDAP/AD/Kerberos to authenticate and authorize users.

Groups and users can be individually created by the “root” account of each system. This is done for smaller standalone systems.

Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) are used for larger installations or enterprises. Each user is authenticated and authorized via a networked protocol. Kerberos provides enhanced security for authentication and simplifies Single Sign On (SSO).

Two Factor Authentication (2FA) can be used with secure administrative access via SSH or WebUI. This approach adds Time-based One Time Password (TOTP) authentication and prevents access in case of password compromise. Enabling 2FA is recommended for any Internet accessible administration portal.

9 Network Controls

TrueNAS is not designed to be publicly visible to the Internet. An external firewall should be utilized in all deployment scenarios in order to protect the system from inbound internet requests. Where services need to be made available via public Internet, proper network security safeguards should be employed, such as VPNs, IP whitelisting, and similar network hardening techniques.

Within TrueNAS is the capability to restrict specific services to an IP address or network interface. Each SMB and NFS share can be further restricted by whitelisting or blacklisting specific IP addresses or subnets.

Most TrueNAS units will have outbound internet access enabled, which allows features such as Proactive Support, Online Updating, Alerting, and connections to TrueCommand Cloud (encrypted via WireGuard). TrueNAS is designed to be operated safely in this manner. However, if security policies dictate that the TrueNAS unit be operated in an offline "air-gapped" environment, TrueNAS is also able to function in this capacity, without the aforementioned internet-enabled features. Administration via TrueCommand for "air-gapped" environments requires a locally installed instance of the TrueCommand software.

10 Encryption

Encryption is provided for data-at-rest and data-in-transit.

Data-at-rest encryption can be provided via:

- Software encryption of each drive (AES-256-XTS) for pools imported from TrueNAS 11.x or earlier
- Self Encrypting Drives (SEDs) using OPAL or FIPS 140.2 (Both AES 256)
- Encryption of specific datasets (AES-256-GCM in version 12.0)

Keys for data-at-rest are managed locally in each system, and the administrator is responsible for storing them securely. Support for Key Management Interface Protocol (KMIP) was introduced in TrueNAS 12.0 and is supported in TrueNAS 13.0.

Data-in-transit has encryption options at many levels:

- HTTPS: Encrypted transport for Administration as well as services such as WebDAV or S3
- SSH: Encrypted protocol for administrative data and ZFS replication (ChaCha20 - 256 bit)
- SMB: File protocol includes its own encryption capability (AES-128-GCM)
- S3: S3 (and other cloud) data can be encrypted before it is written (AES-256)
- OpenVPN: Encrypted transport for accessing data via any IP protocol (AES-256)
- WireGuard: Encrypted transport for accessing data via any IP protocol (ChaCha20 - 256 bit)

The API and web interface for OpenVPN Client and Server are enabled in 13.0. The API and web interface for WireGuard are enabled for TrueCommand access. The API use of WireGuard for data services is in development.

11 Audit Logging

TrueCommand and TrueNAS cooperate to provide configuration audit logging. Each time a TrueCommand user logs into or changes the configuration of a registered TrueNAS system, the login, configuration change, and user identity are logged.

12 Remote Connectivity

Remote connectivity may be needed for administration or data access. Where possible, organizations should use their own secure VPNs and firewalls. Where an external VPN is not available, the following remote access technologies are recommended:

- SSH: Administration, data replication
- SSL/HTTPS: Web UI and Remote File access
- WireGuard: Secure remote access for TrueCommand
- OpenVPN: General purpose remote access to data and administration

TrueCommand removes the need for giving many administrators password access to configure and manage each TrueNAS system. Instead the password is configured within TrueCommand and the TrueCommand admin simply configures which users can access which TrueNAS systems. TrueNAS passwords can be changed without the TrueNAS administrators knowing. None of the TrueNAS administrators need to be provided SSH or direct HTTPS access. TrueCommand provides web proxy access to the TrueNAS systems for the administrator. Whenever an administrator completes a configuration, there is an audit log of the changes made.

TrueCommand also allows for access to TrueNAS systems to be granted and restricted on an as-needed basis, allowing IT departments to segment and restrict access to systems in their TrueNAS fleet while simultaneously being flexible enough to meet business needs as they arise.

13 End-of-Life and End-of-Support

TrueNAS Enterprise systems are sold with up to a 5-year support contract covering both hardware and software. End-of-life notices for systems are placed on our web site and any impacted customers are notified. At the end of their support contract, customers can apply future software upgrades for security fixes to these systems.

Extended support agreements are available for specific deployments of large-scale systems.

14 Secure Coding Practice

TrueNAS is developed with security as a primary concern. Software that comes from a third party is reviewed and validated. Software developed by iXsystems is developed using secure coding practices and automated tools that are relevant for the specific languages being used (Python, C, Go).

Most importantly, any vulnerabilities found are reported as Common Vulnerability and Exposures (CVEs). CVEs that impact a specific release are listed in the release notes. A separate CVE database provides details on all CVEs identified that may be relevant, even if they do not impact TrueNAS.

15 Software Updates

Software patches of included components or middleware are delivered as software updates to TrueNAS. These updates are put through a QA cycle and are also available to users for source code review. Updates are typically provided every 4-6 weeks, but this time period may be reduced for specific security vulnerabilities.

The TrueNAS software is Open Source and enables users to investigate it for vulnerabilities by perusing the code at https://github.com/truenas/. All vulnerabilities detected and reported to iXsystems are reported via the web at security.ixsystems.com.

Software updates can be done online or by downloading a cryptographically signed manual update file. This file can be uploaded to an offline machine via the TrueNAS user interface or other file-sharing protocol. All update files are cryptographically signed by iXsystems and verified upon installation.

Data can be protected across a software update process by using snapshots at the pool or dataset level. The update to a new software revision can be started, stopped, and reverted using these tools. Configurations can be saved and restored within TrueCommand.

16 System Hardening

System hardening is recommended for TrueNAS systems that have sensitive data or are internet attached. Hardening includes secure software updates, the use of secure cryptographic techniques, and the selection and minimization of access protocols. In particular, hardening requires administrative access (e.g SSH) to be restricted to specific clients or IP address ranges.

Specific cryptographic and key management algorithms can be selected. These changes are saved in system configuration and survive a reboot. The changes are done at the FreeBSD level. The defaults are commercial-grade secure.

Access protocols, also known as ports, are restricted by default for greater security. Ports and services are “off” until explicitly enabled by the administrator. SSH ports can be changed to non-standard TCP port numbers to avoid common port 22 brute-force attacks.

Ports can be restricted to specific Ethernet interfaces. For example, the Ethernet interface attached to the Internet may be configured to only allow SSH. Other Ethernet interfaces may be configured to have the normal access protocols such as SMB, NFS, or iSCSI. These actions are done through IP Binding at the service level.

Storage services have their own associated security parameters and protocols. Users, passwords, and groups can be administered locally on each system or the system can be configured with Active Directory (AD) or LDAP authentication. Kerberos can be used for additional authentication services. IP addresses and subnets can be whitelisted or blacklisted for each SMB or NFS share.

SSH access for administration can be disabled on all ports. Instead, administrative access can be provided via IPMI ports which do not have Internet access. This provides a very secure lockdown after a system has been configured.

17 Security Risk Summary

TrueNAS sits within the core of many secure IT infrastructures. Given this role, there is a significant effort to manage security vulnerabilities in both iXsystems software and third-party software. We monitor and report all Common Vulnerabilities and Exposures (CVEs) and have a rapid software development capability to remediate issues.

Most TrueNAS deployments are on networks with no direct incoming Internet access. This is obviously the most secure method for deploying TrueNAS. Where TrueNAS is expected to offer services via the Internet, the users need to be careful and we recommend documenting a specific strategy that encompasses proper security safeguards and technologies.

18 Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and iXsystems, iXsystems subsidiaries, or affiliates (collectively, “iXsystems”). iXsystems does not make any promises or guarantees to customers that any of the methods or suggestions described in this Product Security White Paper will restore a customer’s systems, resolve any issues related to any malicious code, or achieve any other stated or intended results. Customers exclusively assume all risk of utilizing or not utilizing any guidance described in this Product Security White Paper.

Appendix A: Third-Party Software Components

The table shows the third-party packages included in TrueNAS 13.0. This list is subject to change periodically as the software evolves.

Component Name	Description
ap24-mod_mpm_itk	MPM allows vhosts to run under a separate uid and gid
apache24	Apache web server
apr	Apache Portability Library
arcconf	Adaptec SCSI/SAS RAID administration tool
base64	Utility to encode and decode base64 files
beadm	Solaris-like utility to manage Boot Environments on ZFS
bind-tools	Command line tools from BIND: delv, dig, host, nslookup
binutils	GNU binary tools
boost-libs	Free portable C++ libraries (without Boost.Python)
ca_root_nss	Root certificate bundle from the Mozilla Project
cairo	Vector graphics library with cross-device output support
clog	Tcp connection logger daemon
cmdwatch	Watches the output from a command at specified intervals
collectd5	Systems & network statistics collection daemon
convmv	Convert filenames from one encoding to another
cpuid	CPU identification utility
curl	Command line tool for transferring data with URLs
cyrus-sasl	RFC 2222 SASL (Simple Authentication and Security Layer)
cyrus-sasl-gssapi	SASL GSSAPI authentication plugin
db5	Oracle Berkeley DB
dbus	Message bus system for inter-application communication
dbus-glib	GLib bindings for the D-BUS messaging system
dejavu	Bitstream Vera Fonts clone with a wider range of characters
devcpu-data	Intel and AMD CPUs microcode updates
dmidecode	Dumping DMI (SMBIOS) contents in human-readable format
dnsmasq	Lightweight DNS forwarder, DHCP, and TFTP server
dojo	Open-source DHTML toolkit written in JavaScript
drm-fbsd11.2-kmod	DRM modules for the linuxkpi-based KMS components
e2fsprogs	Utilities & library to manipulate ext2/3/4 filesystems
e2fsprogs-libblkid	Blkid library from e2fsprogs package

e2fsprogs-libss	Command-line interface parsing library from e2fsprogs
e2fsprogs-libuuid	UUID library from e2fsprogs package
easy-rsa	Small RSA key management package based on openssl
encodings	X.Org Encoding fonts
expat	XML 1.0 parser written in C
fio	Flexible IO tester
font-bh-ttf	X.Org Bigelow & Holmes TTF font
font-misc-ethiopic	X.Org miscellaneous Ethiopic font
font-misc-meltho	X.Org miscellaneous Meltho font
freetype2	Free and portable TrueType font rendering engine
fribidi	Free Implementation of the Unicode Bidirectional Algorithm
fusefs-libs	FUSE allows filesystem implementation in userspace
fusefs-ntfs	Mount NTFS partitions (read/write) and disk images
fusefs-s3fs	FUSE-based file system backed by Amazon S3
gamin	File and directory monitoring system
gcc9	GNU Compiler Collection 9
gdb	GNU GDB of newer version than comes with the system
gdbm	GNU database manager
gettext-runtime	GNU gettext runtime libraries and programs
git-lite	Distributed source code management tool (lite package)
glib	Some useful routines of C programming
gmake	GNU version of 'make' utility
gmp	Free library for arbitrary precision arithmetic
gnupg	Complete and free PGP implementation
gnutls	GNU Transport Layer Security library
gpu-firmware-kmod	Firmware modules for the linuxkpi-based KMS components
graid5	RAID5 geom class
graphite2	Renderi for complex non-Roman writing systems
grub2-bhyve	Grub-emu loader for bhyve
harfbuzz	OpenType text shaping engine
htop	Better top(1) - interactive process viewer
icu	International Components for Unicode (from IBM)
ifstat	Network interface statistics monitoring tool
inadyn-mt	Simple dynamic dns client
inadyn-troglobit	Dynamic DNS client with SSL/TLS support
indexinfo	Utility to regenerate the GNU info page index
iohyve	bhyve manager utilizing ZFS and other FreeBSD tools
iozone	Performance Test of Sequential File I/O

iperf	Tool to measure maximum TCP and UDP bandwidth
iperf3	Improved tool to measure TCP and UDP bandwidth
ipfs-go	IPFS implementation in Go
ipmitool	CLI to manage IPMI systems
jailme	Setuid version of jexec to allow normal users access to jails
jansson	C library for encoding, decoding, manipulating JSON data
jed	SLang-based text editor
jpeg-turbo	SIMD-accelerated JPEG codec which replaces libjpeg
jq	Lightweight and flexible command-line JSON processor
json-c	JSON (JavaScript Object Notation) implementation in C
kiconvtool	Tool to preload kernel iconv charset tables
ksh93	AT&T KornShell 93
ladvd	Minimal LLDP/CDP/EDP/FDP/NDP sender daemon
ldns	Library for programs conforming to DNS RFCs and drafts
libarchive	Library to create and read streaming archive formats
libassuan	IPC library used by GnuPG and gpgme
libconfuse	Configuration file parsing library
libdnet	Simple interface to low level networking routines
libedit	Command line editor library
libevent	API for executing callback functions on events or timeouts
libffi	Foreign Function Interface
libfontenc	The fontenc Library
libgcrypt	Cryptographic library based on the code from GnuPG
libgpg-error	Common error values for all GnuPG components
libhyve-remote	Library to abstract vnc, rdp and spice protocols
libiconv	Character set conversion library
libidn2	IDNA2008 internationalized domain names
libinotify	Kevent based inotify compatible library
libksba	KSBA is an X.509 Library
liblz4	LZ4 compression library, lossless and very fast
libmspack	Library for Microsoft compression formats
libnghttp2	HTTP/2.0 C Library
liboping	C library, and utility to generate ICMP echo requests
libpci	PCI configuration space I/O made easy
libslang2	Rapid alpha-numeric terminal applications development
libsodium	Library to build higher-level cryptographic tools
libssh2	Library implementing the SSH2 protocol
libsunacl	Wrapper providing SunOS NFSv4 ACL API
libtasn1	ASN.1 structure parser library

libublio	User space caching library
libunistring	Unicode string library
libvncserver	Provide an easy API to a custom vnc server
libxml2	XML parser library for GNOME
libxslt	The XSLT C library for GNOME
lmdb	OpenLDAP Lightning Memory-Mapped Database
lrzsz	Receive/Send files via X/Y/ZMODEM protocol.
lsof	Lists information about open files (similar to fstat(1))
lzo2	Portable speedy, lossless data compression library
mDNSResponde	Bonjour (zero-configuration networking) by Apple
mDNSResponder_nss	Apple mDNS responder - FreeBSD nsswitch module
mbuffer	Tool for buffering data streams
mc	Midnight Commander, a free Norton Commander Clone
mcelog	Collects and decodes Machine Check Exception data
megacli	SAS MegaRAID FreeBSD MegaCLI
mhash	Library for strong hashes such as MD5 and SHA1
minio	Amazon S3 compatible object storage server
minio-client	Minio replacement for file system commands
mkfontscale	Creates an index of scalable font files for X
mksh	MirBSD Korn Shell
mmv	Move/Copy/Append/Link multiple files
mosh	Mobile terminal that supports intermittent connectivity
mpc	Library of complex numbers with arbitrarily high precision
mpfr	Library for multiple-precision floating-point computations
mtools	Collection of tools for manipulating MS-DOS files
nano	Nano's ANOther editor, an enhanced free Pico clone
ncdu	Ncurses du
net-snmp	Extendable SNMP implementation
netatalk3	File server for Mac OS X
netperf	Network performance benchmarking package
nettle	Low-level cryptographic library
nginx	Robust and small WWW server
novnc	HTML5 VNC client
npth	New GNU Portable Threads
nss-pam-ldapd-sasl	Advanced fork of nss_ldap with sasl support
nut	Network UPS Tools
oniguruma	Regular expressions library compatible with POSIX/GNU/Perl
open-vm-tools-nox	Open VMware tools for FreeBSD VMware guests
openldap-sasl-client	LDAP client implementation with SASL2 support

openssh-portable	The portable version of OpenBSD's OpenSSH
openvpn	Secure IP/Ethernet tunnel daemon
p11-kit	Library for loading and enumerating of PKCS#11 modules
p7zip	File archiver with high compression ratio
pam_mkhomedir	Create HOME with a PAM module on demand
pango	Framework for the layout and rendering of i18n text
pciids	Database of all known IDs used in PCI devices
pciutils	PCI configuration utilities
pcre	Perl Compatible Regular Expressions library
perl5	Practical Extraction and Report Language
pigz	Parallel GZIP
pinentry	Collection of simple PIN or passphrase entry dialogs
pinentry-tty	Console version of the GnuPG password dialog
pipewatcher	Pipe watcher to be used in replication
pixman	Low-level pixel manipulation library
pkg	Package manager
plzip	Parallel, lossless data compressor based on the LZMA
png	Library for manipulating PNG images
popt	Getopt(3) like library with a number of enhancements
proftpd	Highly configurable FTP daemon
protobuf	Data interchange format library
pv	Pipe throughput monitor
py37-Babel	Collection of tools for internationalizing Python applications
py37-Flask	Micro web framework
py37-GitPython	Python Git Library
py37-Jinja2	Fast and easy to use stand-alone template engine
py37-MarkupSafe	XML/HTML/XHTML Markup safe string for Python
py37-acme	ACME protocol implementation in Python
py37-aiohttp	Async http client/server framework (asyncio)
py37-aiohttp-wsgi	WSGI adapter for aiohttp
py37-aiorwlock	Read write lock for asyncio
py37-asn1crypto	ASN.1 library with performance and a pythonic API
py37-async_timeout	Timeout context manager for asyncio programs
py37-asyncssh	Python asyncio SSH protocol library
py37-attrs	Python attributes without boilerplate
py37-bcrypt	Modern password hashing
py37-beaker	Session and Caching library with WSGI Middleware
py37-bidict	Bidirectional map implementation and related functionality
py37-boto3	AWS SDK for Python

py37-botocore	Low-level, core functionality of boto
py37-bsd	Python wrappers for various BSD interfaces
py37-bsddb3	Python extension module for BerkeleyDB
py37-cachetools	Extensible memoizing collections and decorators
py37-cam	Python wrapper for FreeBSD CAM
py37-certbot	Let's Encrypt client
py37-certbot-dns-cloudflare	Cloudflare DNS plugin for Certbot
py37-certbot-dns-digitalocean	DigitalOcean DNS Authenticator plugin for Certbot
py37-certbot-dns-google	Google Cloud DNS Authenticator plugin for Certbot
py37-certbot-dns-ovh	OVH DNS Authenticator plugin for Certbot
py37-certifi	Mozilla SSL certificates
py37-cffi	Foreign Function Interface for Python calling C code
py37-chardet	Universal encoding detector
py37-click	Python package for creating command line interfaces
py37-cloudflare	wrapper for the Cloudflare v4 API
py37-coloredlogs	Colored terminal output for Python logging module
py37-configargparse	Drop-in replacement for argparse
py37-configobj	Simple but powerful config file reader and writer
py37-croniter	Iteration support for datetime objects with cron like format
py37-cryptography	Cryptographic recipes and primitives for Python developers
py37-daemon	Well-behaved daemon framework for Python
py37-dateutil	Extensions to the standard Python datetime module
py37-dbus	Python bindings for the D-BUS messaging system
py37-ddt	Data-Driven Tests for Python Unittest
py37-distro	Linux OS platform information API
py37-django-formtools	Bootstrap forms for django
py37-django-json-rpc	Simple JSON-RPC implementation for Django
py37-django-tastypie	Create REST API for Django apps
py37-django110	High-level Python Web Framework
py37-dns-lexicon	Manipulate DNS records
py37-dnspython	DNS toolkit for Python
py37-docutils	Python Documentation Utilities
py37-dojango	Django application for building dojo
py37-fenced	TrueNAS Fence Daemon
py37-future	Clean single-source support
py37-gitdb2	Git Object Database
py37-google-api-python-client	Google API Client Library for Python
py37-google-auth	Google Authentication Library
py37-google-auth-httplib2	Google Authentication Library: httplib2 transport

py37-httplib2	Comprehensive HTTP client library
py37-humanfriendly	Human friendly output for text interfaces
py37-idna	Internationalized Domain Names in Applications (IDNA)
py37-ifaddr	Python Library to enumerate all network interfaces
py37-influxdb	Python Client for InfluxDB
py37-iocage	FreeBSD jail manager written in Python
py37-ipaddr	IPv4/IPv6 manipulation library in Python
py37-isodate	ISO 8601 date/time/duration parser and formatter
py37-itsdangerous	Various helpers to pass data in untrusted environments
py37-jmespath	JSON Matching Expressions
py37-josepy	JOSE protocol implementation in Python
py37-jsonlines	Library with helpers for the jsonlines file format
py37-jsonpickle	Python library for serializing any object graph into JSON
py37-jsonschema	JSON Schema validation for Python
py37-ldap	LDAP module for python, for OpenLDAP2
py37-lockfile	Platform-independent file locking module
py37-lxml	Pythonic binding for the libxml2 and libxslt libraries
py37-mako	Super-fast templating language in Python
py37-markdown	Python implementation of Markdown
py37-markdown2	Fast and complete Python implementation of Markdown
py37-mock	Mock unit tests for Python
py37-multidict	Multidict implementation
py37-netifaces	Getting network addresses from Python 3
py37-netsnmpagent	Python module that facilitates writing Net-SNMP subagents
py37-ntplib	Python NTP library
py37-oauth2	Python library for OAuth version 1.0
py37-oauth2client	OAuth 2.0 client library
py37-onedrivesdk	Official Python OneDrive SDK
py37-openssl	Python interface to the OpenSSL library
py37-packaging	Core utilities for Python packages
py37-paramiko	Python SSH2 protocol library
py37-parsedatetime	Python for parsing 'human readable' date/time expressions
py37-pbr	Python Build Reasonableness
py37-pip	Tool for installing and managing Python packages
py37-ply	Python Lex-Yacc
py37-polib	Python library to parse and manage gettext catalogs
py37-psutil	Process utilities module for Python
py37-pyasn1	ASN.1 toolkit for Python
py37-pyasn1-modules	Collection of ASN.1 data structures

py37-pybonjour	pybonjour 1.1.1 for Python 3
py37-pycparser	C parser in Python
py37-pycryptodome	Cryptographic library for Python
py37-pycryptodomex	Cryptographic library for Python
py37-pydevd	Debugger used in PyDev and PyCharm
py37-pynacl	Networking and Cryptography library
py37-pyparsing	General parsing module for Python
py37-pyrfc3339	Generate and parse RFC 3339 timestamps
py37-pyrsistent	Persistent/Immutable/Functional data structures
py37-pysmi	SNMP/SMI MIB parsing in Python
py37-pysnmp	SNMP framework for Python
py37-pysocks	Python SOCKS module
py37-pytest-runner	Test support for pytest
py37-python-digitalocean	API to manage digitalocean.com droplets
py37-python-mimeparse	Basic functions for handling mime-types in Python
py37-pytz	World Timezone Definitions for Python
py37-raven	Client for Sentry
py37-remote-pdb	Remote vanilla PDB over TCP sockets
py37-requests	HTTP library written in Python for human beings
py37-requests-file	Transport adapter for use with the Requests Python library
py37-requests-toolbelt	Utility belt for advanced users of python-requests
py37-rsa	Pure-Python RSA implementation
py37-s3cmd	Unix-like tools to manipulate stored files from the CLI
py37-s3transfer	Amazon S3 Transfer Manager for Python
py37-setproctitle	Python module to customize the process title
py37-setuptools	Python packages installer
py37-simplejson	Simple, fast, extensible JSON encoder/decoder
py37-six	Python 2 and 3 compatibility utilities
py37-smmap2	Sliding-window memory map manager
py37-snmp_passpersist	Python client library for Net-SNMP pass persist backend
py37-south	Intelligent schema migrations for Django apps
py37-sqlite3	Standard Python binding to the SQLite3 library
py37-sqlparse	Non-validating SQL parser for Python
py37-sysctl	Wrapper for the sysctl system functions
py37-texttable	Module for creating simple ASCII tables
py37-tldextract	Separate the TLD, domain, and subdomains of a URL
py37-tqdm	Fast, extensible progress bar for Python
py37-ujson	Ultra fast JSON encoder and decoder for Python
py37-uritemplate	Python implementation of URI Template

py37-urllib3	HTTP library with thread-safe connection pooling, file post
py37-werkzeug	Python utilities collection for building WSGI applications
py37-ws4py	WebSocket package for Python
py37-xattr	Python wrapper for extended filesystem attributes
py37-yaml	Python YAML parser
py37-yarl	Yet another URL library
py37-zeroconf	Python implementation of multicast DNS service discovery
py37-zope.component	Zope Component Architecture
py37-zope.event	Very basic event publishing system
py37-zope.interface	Interfaces for Python
pydbus-common	Python bindings for the D-BUS messaging system
python	Default version of Python interpreter
python3	Python interpreter
python37	Interpreted object-oriented programming language
pyvmomi	Python SDK for the VMware vSphere API
rclone	Sync files to and from various cloud services
readline	Library for editing command lines as they are typed
rrdtool	Round Robin Database Tools
rsync	Network file distribution/synchronization utility
samba-nsupdate	nsupdate utility with GSS-TSIG support
samba410	Free SMB/CIFS and AD/DC server and client for Unix
scponly	Tiny shell that only permits scp and sftp
screen	Multi-screen window manager
sedutil	Self Encrypting Drive Utility
sg3_utils	Set of utilities that send SCSI commands to devices
sipcalc	IP subnet calculator with IPv6 support
smartmontools	S.M.A.R.T. disk monitoring tools
smp_utils	Utilities to send SAS Serial Management Protocol requests
source-highlight	C/C++ and Java sources to HTML converter
sqlite3	SQL database engine in a C library
stunnel	SSL encryption wrapper for standard network daemons
sudo	Allow others to run commands as root
swagger-ui	OpenAPI spec renderer UI
syslog-ng	Powerful syslogd replacement
throttle	A pipe bandwidth throttling utility
tmux	Terminal Multiplexer
tpm-emulator	Trusted Platform Module (TPM) emulator
trafshow	Full screen visualization of network traffic
trousers	Open-source TCG Software Stack

tw_cli	3ware storage controllers management CLI
uefi-edk2-bhyve	UEFI-EDK2 firmware for bhyve
uefi-edk2-bhyve-csm	UEFI-EDK2 firmware for bhyve with CSM
unison-nox11	User-level file synchronization tool
utf8proc	UTF-8 processing library
uwsgi	Developer-friendly WSGI server which uses uwsgi protocol
vblade	Virtual EtherDrive(R) blade AoE target
vm-bhyve	Management system for bhyve virtual machines
websockify	noVNC-websockify implementation.
wget	Retrieve files from the Net via HTTP(S) and FTP
wgetpaste	Paste to several pastebin services via bash script
wireguard	Fast, modern and secure VPN Tunnel
wireguard-go	WireGuard implementation in Go
xorg-fonts-truetype	X.Org TrueType fonts
xtail	Watches the growth of files or directories
zfs-stats-lite	Display human-readable ZFS statistics
zopfli	Zopfli Compression Algorithm
zsh	The Z shell