ZFS encryption

Features

published: 2020-Feb-14 (c) napp-it.org

Content:

Timetable functions partly under development

1. Napp-it encryption features

Data security with protection against theft, ransomware, sabotage and accidental data lost is mandatory. Data privacy rules like the EU General Data Protection Regulation (DSGVO) demand state of the art storage features in any organisation size, best and most attractive offered with ZFS, snaps and individually encrypted storage and backup.

Basic napp-it Features

- ZFS Encryption with the option of a different key per filesystem
- ZFS encrypted backups
- Encrypted/ raw replication of a locked filesystem (Illumos, OmniOS/OI)
- Keysource prompt, local files or files on a webbased keyserver
  even with a file/webbased method you can always unlock via prompt.
- Keylocations are easily switchable (just copy keyfolders)
- webbased method does not store a key locally

- SMB shares are removed automatically on a lock
- SMB shares can be restored on an unlock

Napp-it Pro Features

- Automount of encrypted filesystems (local or webbased keys needed)
  during server reboot
- User-Lock/Unlock of a filesystem via SMB and optionally a special smbkey
- Auto-Lock/Unlock based on a timetable (under construction)

- Keysplit where the two parts of a key can be stored on different locations
  either (L)ocally or on a (W)ebserver (L1:L1,L1:L2,L1:W1,W1:W1,W1:W2)

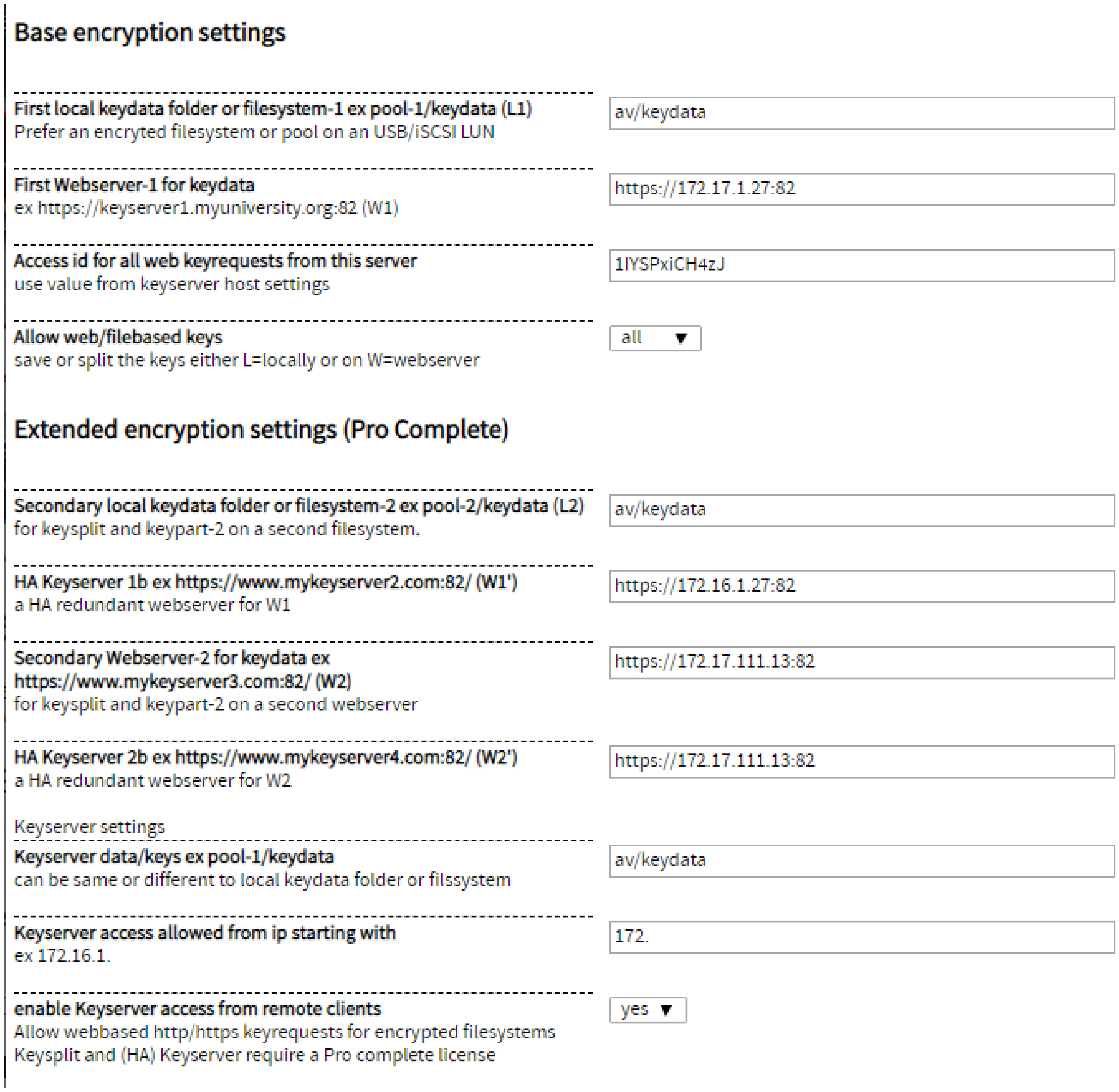
- Keyserver (http or https, Pro complete)
  centralised keymanagement without local keystorage
- Keysplit to store key parts on two independent locations.
- HA keyserver to allow a key request from a second redundant webserver
  W1, W2, W1' and W2'
- Restrict access based on timetable or IP

- Easy keymanagement
  just copy keyfolders between the different locations to copy/backup keys

1.1 ZFS Encryption setup (clientside)

1.1.1 General settings

Setup defaults in menu About > Settings



Base encryption settings

First local keydata folder or filesystem-1 ex pool-1/keydata (L1) Prefer an encryted filesystem or pool on an USB/iSCSI LUN	av/keydata
First Webserver-1 for keydata ex https://keyserver1.myuniversity.org:82 (W1)	https://172.17.1.27:82
Access id for all web keyrequests from this server use value from keyserver host settings	1IYSPxiCH4zJ
Allow web/filebased keys save or split the keys either L=locally or on W=webserver	all ▼

Extended encryption settings (Pro Complete)

Secondary local keydata folder or filesystem-2 ex pool-2/keydata (L2) for keysplit and keypart-2 on a second filesystem.	av/keydata
HA Keyserver 1b ex https://www.mykeyserver2.com:82/ (W1') a HA redundant webserver for W1	https://172.16.1.27:82
Secondary Webserver-2 for keydata ex https://www.mykeyserver3.com:82/ (W2) for keysplit and keypart-2 on a second webserver	https://172.17.111.13:82
HA Keyserver 2b ex https://www.mykeyserver4.com:82/ (W2') a HA redundant webserver for W2	https://172.17.111.13:82

Keyserver settings

Keyserver data/keys ex pool-1/keydata can be same or different to local keydata folder or filssystem	av/keydata
Keyserver access allowed from ip starting with ex 172.16.1.	172.
enable Keyserver access from remote clients Allow webbased http/https keyrequests for encrypted filesystems Keysplit and (HA) Keyserver require a Pro complete license	yes ▼

Local keydata folder.
Below this folder, local keys are stored.

ex av/keydata

This folder should be encrypted (manually unlocked)
or on a removable pool ex USB or on an iSCSI target

Webserver url
When you create a new encrypted filesystem,
keys are stored here when you select W1

ex https://172.16.1.12:82

Access-ID
On a keyserver you must create a folder for any client.
Copy/paste the hostid for this server from the keyserver

ex Aoi7c5TR12hZ

1.2 ZFS Encryption server setup (Keyserver, napp-it Pro Complete)

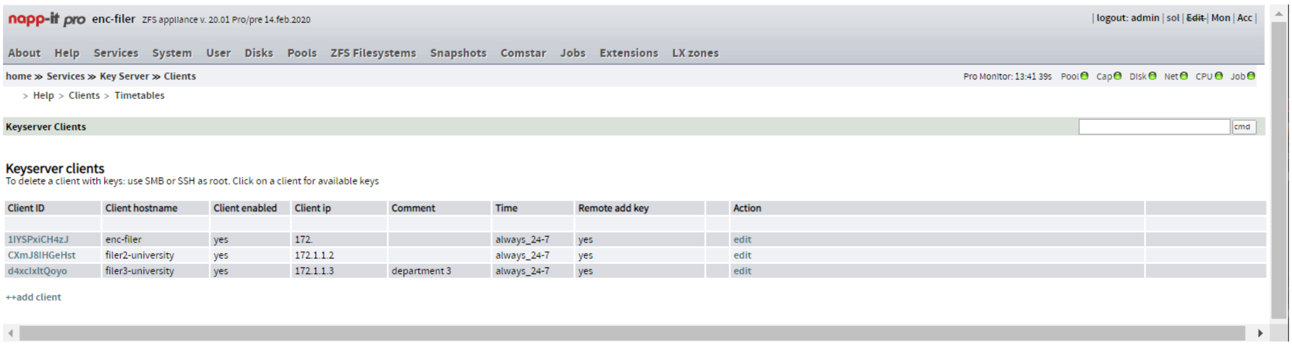
1.2.1 General settings

Setup defaults in menu About > Settings

Keyserver data When this server is a keyserver, place webbased keys below this folder	av/keydata local1, local2 and keyserver folder can be the same as napp-it create a folder local or keyserver below.
Keyserver access allowed A client has access when the ip starts with this number	ex. 172.16
Keyserver enabled Enable/Disable web key requests globally	yes/no

1.2.2 Client settings

Create clients in menu Services > Key Server > Clients


napp-it pro
enc-filer ZFS appliance v. 20.01 Pro/pre 14.feb.2020
| logout: admin | sol | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions LX zones
home » Services » Key Server » Clients
> Help > Clients > Timetables
Pro Monitor: 13:41 39s Pool Cap Disk Net CPU Job
Keyserver Clients
cmd

Keyserver clients

To delete a client with keys: use SMB or SSH as root. Click on a client for available keys

Client ID	Client hostname	Client enabled	Client ip	Comment	Time	Remote add key		Action	
1IYSPxiCH4zJ	enc-filer	yes	172.		always_24-7	yes		edit	
CXmJ8IHGeHst	filer2-university	yes	172.1.1.2		always_24-7	yes		edit	
d4xclxltQoyo	filer3-university	yes	172.1.1.3	department 3	always_24-7	yes		edit	

++add client

Create an entry for each client for whom you want to store keys. The keys are stored below the keyserver filesystem. If you want a second keyserver W2 for the second keyoart, copy over the keyfolder to the second keyserver. In a keyfolder ex keydata/keyserver/clients/d4xclxltQoyo you will find a folder for keypart-1 and keypart-2 what makes it easy to copy/move/backup keys or keyparts.

Folder structure under keyserverfs:

/keyserver	you can share this via SMB (root only)
/keyserver/clients	
/keyserver/clients/CXmJ8IHGeHst	for a client with this id
/keyserver/clients/CXmJ8IHGeHst/defaults.cfg	client settings
/keyserver/clients/CXmJ8IHGeHst/keys-part1/	filesystem keys/ keypart-1
/keyserver/clients/CXmJ8IHGeHst/keys-part2/	filesystem keys keypart2

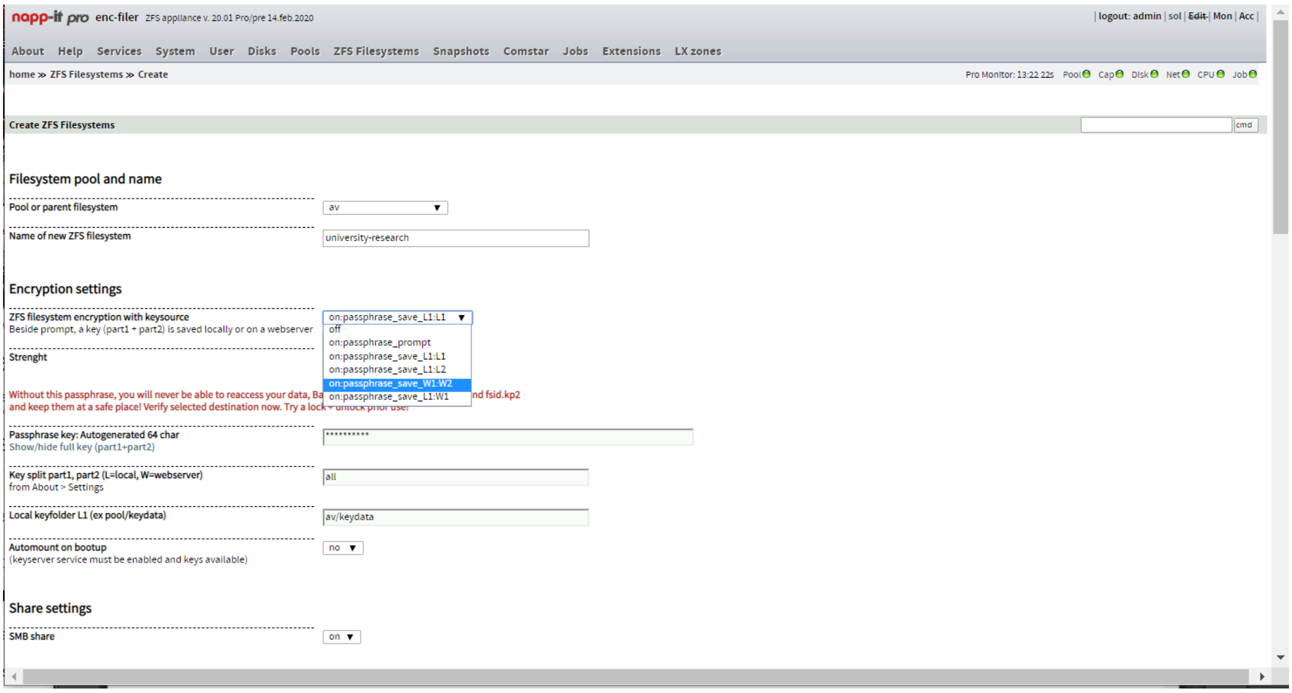
/keyserver/logs
/keyserver/timetables

Folder structure for local keys below keyfs

/local/keys-part1	filesystem keys/ keypart-1
/local/keys-part2	filesystem keys/ keypart-2

1.3 ZFS Create encrypted filesystems

1.3.1 ZFS Filesystem > Create (requires Oracle Solaris or newest OmniOS/OI with newest pool version)


napp-it pro enc-filer ZFS appliance v. 20.01 Pro/pre 14.feb.2020
| logout: admin | sol | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions LX zones
home » ZFS Filesystems » Create
Pro Monitor: 13:22 22s Pool Cap Disk Net CPU Job
cmd

Create ZFS Filesystems

Filesystem pool and name

Pool or parent filesystem: av ▼

Name of new ZFS filesystem: university-research

Encryption settings

ZFS filesystem encryption with keysource
Beside prompt, a key (part1 + part2) is saved locally or on a webserver: on:passphrase_save_L1:L1 ▼

- off
- on:passphrase_prompt
- on:passphrase_save_L1:L1
- on:passphrase_save_L1:L2
- on:passphrase_save_W1:W2
- on:passphrase_save_L1:W1

Strenght

Without this passphrase, you will never be able to reaccess your data, Ba… nd fsid.kp2
and keep them at a safe place! Verify selected destination now. Try a lock + unlock prior use!

Passphrase key: Autogenerated 64 char
Show/hide full key (part1+part2): **********

Key split part1, part2 (L=local, W=webserver)
from About > Settings: all

Local keyfolder L1 (ex pool/keydata): av/keydata

Automount on bootup
(keyserver service must be enabled and keys available): no ▼

Share settings

SMB share: on ▼

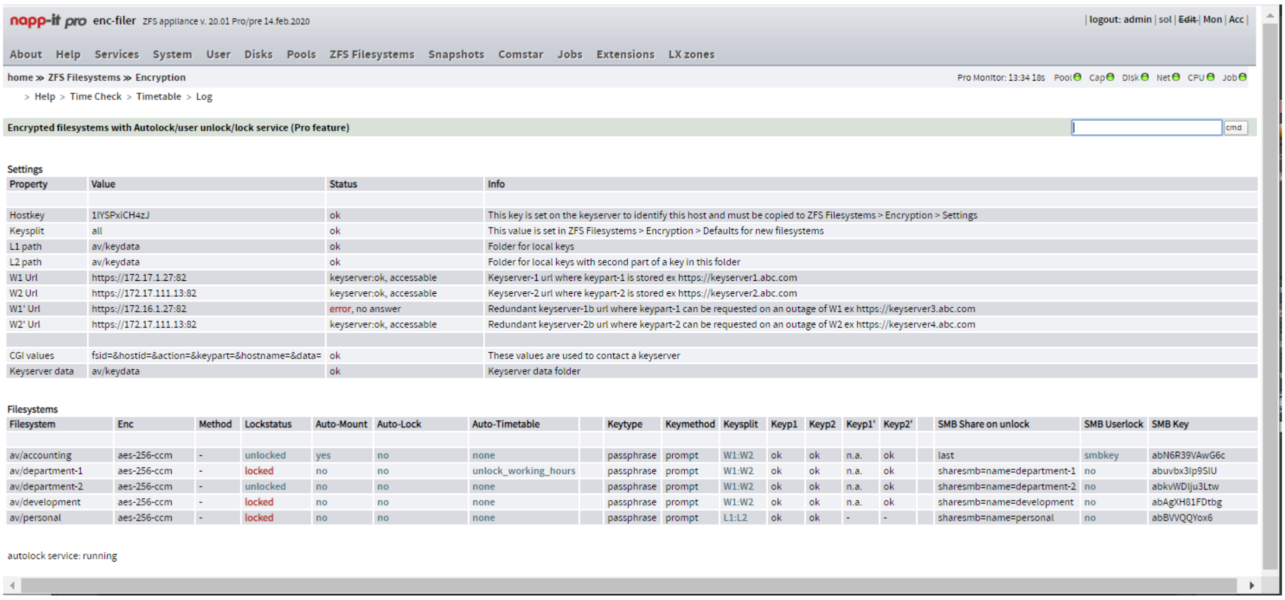
If you select a webbased location, the key is uploaded during creation (requires you have created a client entry on the keyserver(s) and copied the client id over to About > Settings)

If you want to use two webserver, you must create a client folder on the first webserver and copy it over to the second webserver via sftp or a SMB share.

In the passphrase line you can click show/hide to view the passphrase.
You can copy backup now (or backup the files later). If you loose keys you will never be able to access data

1.4 Details of encrypted filesystems

1.4.1 Open menu ZFS Filesystems > Encryption


napp-it pro enc-filer ZFS appliance v. 20.01 Pro/pre 14.feb.2020
| logout: admin | sol | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions LX zones
home » ZFS Filesystems » Encryption
Pro Monitor: 13:34 18s Pool Cap Disk Net CPU Job
> Help > Time Check > Timetable > Log
cmd

Encrypted filesystems with Autolock/user unlock/lock service (Pro feature)

Settings

Property	Value	Status	Info
Hostkey	1IYSPxiCH4zJ	ok	This key is set on the keyserver to identify this host and must be copied to ZFS Filesystems > Encryption > Settings
Keysplit	all	ok	This value is set in ZFS Filesystems > Encryption > Defaults for new filesystems
L1 path	av/keydata	ok	Folder for local keys
L2 path	av/keydata	ok	Folder for local keys with second part of a key in this folder
W1 Url	https://172.17.1.27:82	keyserver:ok, accessable	Keyserver-1 url where keypart-1 is stored ex https://keyserver1.abc.com
W2 Url	https://172.17.111.13:82	keyserver:ok, accessable	Keyserver-2 url where keypart-2 is stored ex https://keyserver2.abc.com
W1' Url	https://172.16.1.27:82	error, no answer	Redundant keyserver-1b url where keypart-1 can be requested on an outage of W1 ex https://keyserver3.abc.com
W2' Url	https://172.17.111.13:82	keyserver:ok, accessable	Redundant keyserver-2b url where keypart-2 can be requested on an outage of W2 ex https://keyserver4.abc.com
CGI values	fsid=&hostid=&action=&keypart=&hostname=&data=	ok	These values are used to contact a keyserver
Keyserver data	av/keydata	ok	Keyserver data folder

Filesystems

Filesystem	Enc	Method	Lockstatus	Auto-Mount	Auto-Lock	Auto-Timetable		Keytype	Keymethod	Keysplit	Keyp1	Keyp2	Keyp1'	Keyp2'		SMB Share on unlock	SMB Userlock	SMB Key
av/accounting	aes-256-ccm	-	unlocked	yes	no	none		passphrase	prompt	W1:W2	ok	ok	n.a.	ok		last	smbkey	abN6R39VAwG6c
av/department-1	aes-256-ccm	-	locked	no	no	unlock_working_hours		passphrase	prompt	W1:W2	ok	ok	n.a.	ok		sharesmb=name=department-1	no	abuvbx3Ip9SIU
av/department-2	aes-256-ccm	-	unlocked	no	no	none		passphrase	prompt	W1:W2	ok	ok	n.a.	ok		sharesmb=name=department-2	no	abkvWDIju3Ltw
av/development	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	W1:W2	ok	ok	n.a.	ok		sharesmb=name=development	no	abAgXH81FDtbg
av/personal	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	L1:L2	ok	ok	-	-		sharesmb=name=personal	no	abBVVQQYox6

autolock service: running

Settings:
Infos about your encryption related settings. (read only)

Filesystems:
This is an overview of encrypted filesystems and their setting. You can lock/unlock and modify settings like Automount (during server boot), Auto_lock (timer based lock/unlock) and the according Timetable and SMB Userlock.

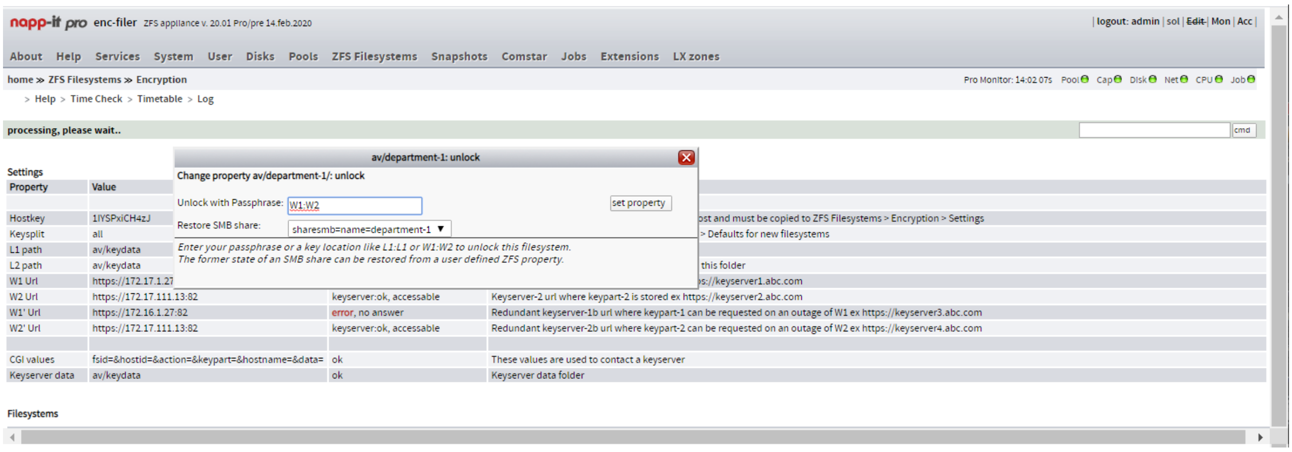
You can check availability of local or webbased keylocations like the two webserver W1 and W2 and their HA/ failover alternatives W1' and W2'.

autolock service: running state

This service is needed for SMB user lock/unlock and timer based lock/unlock.
You can start/stop this service in menu Services.

1.4.2 Unlock a filesystem

When you clock on „locked" in the row of a filesystem you can unlock the filesystem


napp-it pro enc-filer ZFS appliance v. 20.01 Pro/pre 14.feb.2020
| logout: admin | sol | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions LX zones
home » ZFS Filesystems » Encryption
Pro Monitor: 14:02 07s Pool Cap Disk Net CPU Job
> Help > Time Check > Timetable > Log
cmd
set property

processing, please wait..

av/department-1: unlock

Change property av/department-1/: unlock

Unlock with Passphrase: W1:W2

Restore SMB share: sharesmb=name=department-1 ▼

Enter your passphrase or a key location like L1:L1 or W1:W2 to unlock this filesystem.
The former state of an SMB share can be restored from a user defined ZFS property.

Settings

Property	Value		
Hostkey	1IYSPxiCH4zJ		ost and must be copied to ZFS Filesystems > Encryption > Settings
Keysplit	all		> Defaults for new filesystems
L1 path	av/keydata		
L2 path	av/keydata		this folder
W1 Url	https://172.17.1.27		s://keyserver1.abc.com
W2 Url	https://172.17.111.13:82	keyserver:ok, accessable	Keyserver-2 url where keypart-2 is stored ex https://keyserver2.abc.com
W1' Url	https://172.16.1.27:82	error, no answer	Redundant keyserver-1b url where keypart-1 can be requested on an outage of W1 ex https://keyserver3.abc.com
W2' Url	https://172.17.111.13:82	keyserver:ok, accessable	Redundant keyserver-2b url where keypart-2 can be requested on an outage of W2 ex https://keyserver4.abc.com
CGI values	fsid=&hostid=&action=&keypart=&hostname=&data=	ok	These values are used to contact a keyserver
Keyserver data	av/keydata	ok	Keyserver data folder

Filesystems

You can accept he default keylocation or you can enter a different like L1:L1 or L1:L2. You can also copy in the real key to unlock directly. As an option you can restore the SMB share or unlock without a share enabled.

In any case, the key is not stored locally as the unlock functionality is based on prompt where the key is entered directly in the background via an „Expect" functionality.

If you want to reorganize your keylocations ex from L1 to L1 or W1 to L1, just copy over the keys to the new location and modify the keylocation in menu ZFS Filesystems > Encryption.

2. More on ZFS Encryption

ZFS encryption as a ZFS filesystem property is in Oracle Solaris 11.x and with Open-ZFS in OmniOS 151032+ and OpenIndiana 2019.10. To enable encryption update OS and Pool version.

Encryption as a ZFS property has huge advantages over device or disk based encryption that are available on the different Open-ZFS plattforms (BSD, Illumos or Linux) in a non-compatible way as they work below ZFS on OS level and not for ZFS filesystems but for the whole pool with a single key for all filesystems.

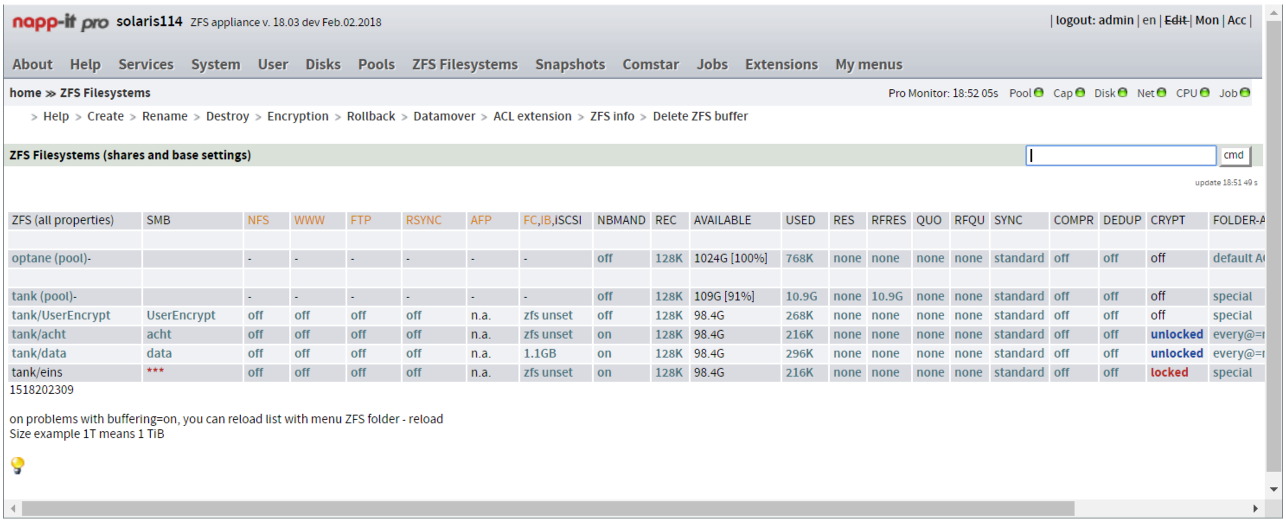
ZFS embedded encryption allows a key per filesystem for different levels of security and access time. For backups you can access unlocked data or you can backup encrypted data with encrypted ZFS replication. You can lock access to very sensitive data strictly to working hours with extended access to other areas while they remain protected in case of a theft.

Especially the last aspect becomes more and more important in the light of new rules regarding sensitive personal data like the EU DGSVO that will be a common EU law from may 2018. It demands among others a state of the art data security at technical level. You must define not only the exact amound of data, who has access, why is this access granted and how long even for backup is data kept but you must also ensure the security of the data itself and minimising the risk. In every case this can only guaranteed with encryption to avoid a hacking outside working hours and to secure data in case of a hardware theft. and with a backup mechanism that includes encryption. The EU fines if you have not fullfilled the regulatory demands are hefty with up to 4% of the worldwide revenue in severe cases.

Currently Oracle Solaris and newest Open-ZFS has ZFS-Encryption at filesystem level with replication to encrypted destinations . Illumos with OmniOS/O adds a raw replication mode where transfer and destination is encrypted with the source key or a replication of a single unencrypted filesystem to an encrypted target (already created or created during zfs receive)

The encryption property must be set when you create a new filesystem. You can define a security level like aes-256-ccm, a keyformat like raw, hex or passphrase and a keysource like prompt, file, https or a keyserver.
see https://docs.oracle.com/cd/E53394_01/html/E54801/gkkih.html#scrolltoc

2.1 ZFS locking/ unlocking


napp-it pro solaris114 ZFS appliance v. 18.03 dev Feb.02.2018
| logout: admin | en | ~~Edit~~ | Mon | Acc |
About
Help
Services
System
User
Disks
Pools
ZFS Filesystems
Snapshots
Comstar
Jobs
Extensions
My menus
home » ZFS Filesystems
Pro Monitor: 18:52 05s Pool Cap Disk Net CPU Job
> Help > Create > Rename > Destroy > Encryption > Rollback > Datamover > ACL extension > ZFS info > Delete ZFS buffer
cmd
update 18:51 49 s

ZFS Filesystems (shares and base settings)

ZFS (all properties)	SMB	NFS	WWW	FTP	RSYNC	AFP	FC,IB,iSCSI	NBMAND	REC	AVAILABLE	USED	RES	RFRES	QUO	RFQU	SYNC	COMPR	DEDUP	CRYPT	FOLDER-A
optane (pool)-		-	-	-	-	-	-	off	128K	1024G [100%]	768K	none	none	none	none	standard	off	off	off	default A
tank (pool)-		-	-	-	-	-	-	off	128K	109G [91%]	10.9G	none	10.9G	none	none	standard	off	off	off	special
tank/UserEncrypt	UserEncrypt	off	off	off	off	n.a.	zfs unset	off	128K	98.4G	268K	none	none	none	none	standard	off	off	off	special
tank/acht	acht	off	off	off	off	n.a.	zfs unset	on	128K	98.4G	216K	none	none	none	none	standard	off	off	unlocked	every@=
tank/data	data	off	off	off	off	n.a.	1.1GB	on	128K	98.4G	296K	none	none	none	none	standard	off	off	unlocked	every@=
tank/eins	***	off	off	off	off	n.a.	zfs unset	on	128K	98.4G	216K	none	none	none	none	standard	off	off	locked	special

1518202309

on problems with buffering=on, you can reload list with menu ZFS folder - reload
Size example 1T means 1 TiB

As a basic napp-it free feature, you can lock/ unlock a filesystem in menu ZFS Filesystems. Handling is similar to other ZFS properties like sharing or compress (simply click on the property you want to modify). This requires full access to Storage Management. After reboot all encrypted filesystems remail locked until they are unlocked manually with a key that can be different for every filesystem.

2.2 Keysource

ZFS encryption requires a key per filesystem. On a smaller setup you can use prompt as keysource. This means that you must enter the key manually to unlock a filesystem. For locking you do not need a key.

With many filesystems or when you do not want to give a key to storage operators, you can use file, https (web) or a keyserver as source. The keysource is a ZFS property. Once defined and accessable you can lock/ unlock a filesystem without knowing the key as long as the keysource is available.

For a private/soho setup you may use an USB stick where you place the filebased keys to allow a simple locking/ unlocking. If you remove the stick nobody can unlock the filesystem. Handling is simple. On the evening you lock your filesystems and in the morning you plug in your stick and unlock the filesystems (keep a copy of the keys elsewhere as backup). If you forget to unplug the Stick on a theft or someone has copied the stick, this method is unsecure.

More secure is a remote keyserver with restricted access with splitted keys. You can also use one or two local filesystems for one or bot keyparts. You should use local keys only in a Soho environment ex with keys on an USB stick or a remote iSCSI Lun.

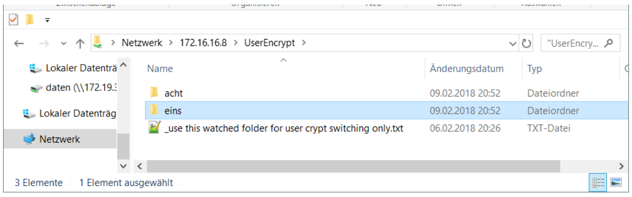
2.3 User locking/unlocking

If you use a ZFS filer for different user groups with different security needs or access times, you may want to allow users ex a head of a department to lock/ unlock their data themselves without help of a storage admin and without access to the storage management software.

This requires an auth based mechanism that must be integrated into the storage system. While one can think of a lot of sophisticated methods, I follow the Keep it Simple approach. There is already a secure method to restrict access to server resources based on local or zentralized AD users and this is SMB where you can restrict access to shares, folders and files or track access via file auditing (Solaris 11.4, see https://docs.oracle.com/cd/E37838_01/html/E61027/osmaa-whatsnew.html#OSMAAosmaa-whatsnew).

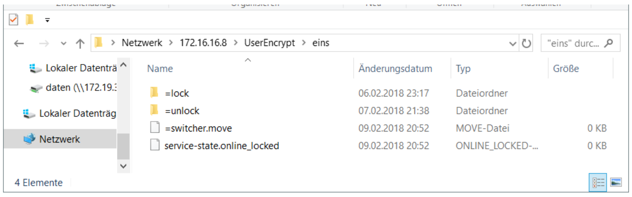
SMB does not offer a method to control service states. To allow locking/ unlocking of filesystems, napp-it can create a SMB share with a watched folder per encrypted filesystem. Only authorized users have access to these folders. In these folders a user will find a switching file and a file with the service and locking state as filename. A simple move of the switching file (=switcher.move) into a subfolder „lock" or „unlock" will initite a locking or unlocking (requires that Solaris has access to the keys with a file, web or keyserver based method). You can extend this with an SMB key. Copy the switching file then to your desktop, insert the SMB key und use thisn file to unlock.

Napp-it watched SMB folders



Name	Änderungsdatum	Typ
acht	09.02.2018 20:52	Dateiordner
eins	09.02.2018 20:52	Dateiordner
_use this watched folder for user crypt switching only.txt	06.02.2018 20:26	TXT-Datei

SMB share UserAuth with a subfolder per encrypted filesystem



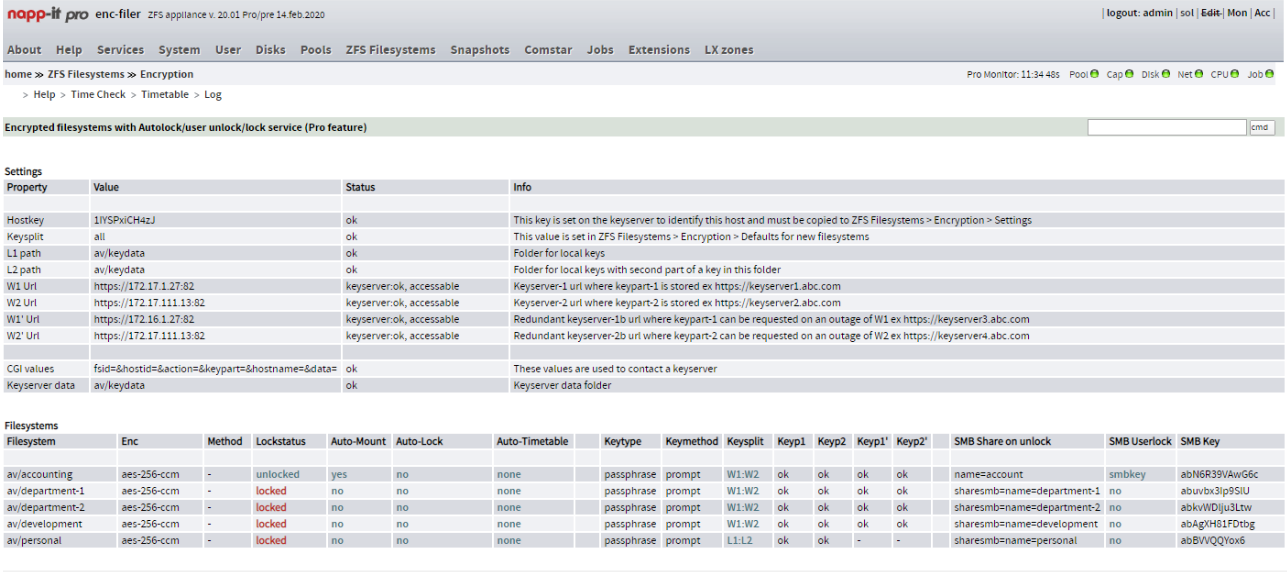
Name	Änderungsdatum	Typ	Größe
=lock	06.02.2018 23:17	Dateiordner	
=unlock	07.02.2018 21:38	Dateiordner	
=switcher.move	09.02.2018 20:52	MOVE-Datei	0 KB
service-state.online_locked	09.02.2018 20:52	ONLINE_LOCKED-...	0 KB

Watched folders =lock and =unlock with a switcher file that locks/ unlocks a filesystem by moving the file into a subfolder and a status file.

2.4 Setup user locking/unlocking

To enable userlocking via watched folders you must

- create an encrypted filesystem with a (L) or (W) as keysource
- set userlock to on or smbkey in menu ZFS Filesystems > Encryption
- enable autolock service (Menu services, this is a Pro Feature)
- enable smb share of of the UserEncrypt filesystem, set permissions


napp-it pro enc-filer ZFS appliance v. 20.01 Pro/pre 14.feb.2020
| logout: admin | sol | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions LX zones
home » ZFS Filesystems » Encryption
Pro Monitor: 11:34 48s Pool Cap Disk Net CPU Job
> Help > Time Check > Timetable > Log
cmd

Encrypted filesystems with Autolock/user unlock/lock service (Pro feature)

Settings

Property	Value	Status	Info
Hostkey	1IYSPxiCH4zJ	ok	This key is set on the keyserver to identify this host and must be copied to ZFS Filesystems > Encryption > Settings
Keysplit	all	ok	This value is set in ZFS Filesystems > Encryption > Defaults for new filesystems
L1 path	av/keydata	ok	Folder for local keys
L2 path	av/keydata	ok	Folder for local keys with second part of a key in this folder
W1 Url	https://172.17.1.27:82	keyserver:ok, accessable	Keyserver-1 url where keypart-1 is stored ex https://keyserver1.abc.com
W2 Url	https://172.17.111.13:82	keyserver:ok, accessable	Keyserver-2 url where keypart-2 is stored ex https://keyserver2.abc.com
W1' Url	https://172.16.1.27:82	keyserver:ok, accessable	Redundant keyserver-1b url where keypart-1 can be requested on an outage of W1 ex https://keyserver3.abc.com
W2' Url	https://172.17.111.13:82	keyserver:ok, accessable	Redundant keyserver-2b url where keypart-2 can be requested on an outage of W2 ex https://keyserver4.abc.com
CGI values	fsid=&hostid=&action=&keypart=&hostname=&data=	ok	These values are used to contact a keyserver
Keyserver data	av/keydata	ok	Keyserver data folder

Filesystems

Filesystem	Enc	Method	Lockstatus	Auto-Mount	Auto-Lock	Auto-Timetable		Keytype	Keymethod	Keysplit	Keyp1	Keyp2	Keyp1'	Keyp2'		SMB Share on unlock	SMB Userlock	SMB Key
av/accounting	aes-256-ccm	-	unlocked	yes	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		name=account	smbkey	abN6R39VAwG6c
av/department-1	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		sharesmb=name=department-1	no	abuvbx3Ip9SIU
av/department-2	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		sharesmb=name=department-2	no	abkvWDIju3Ltw
av/development	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		sharesmb=name=development	no	abAgXH81FDtbg
av/personal	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	L1:L2	ok	ok	-	-		sharesmb=name=personal	no	abBVVQQYox6

- now set SMB Userlock to yes

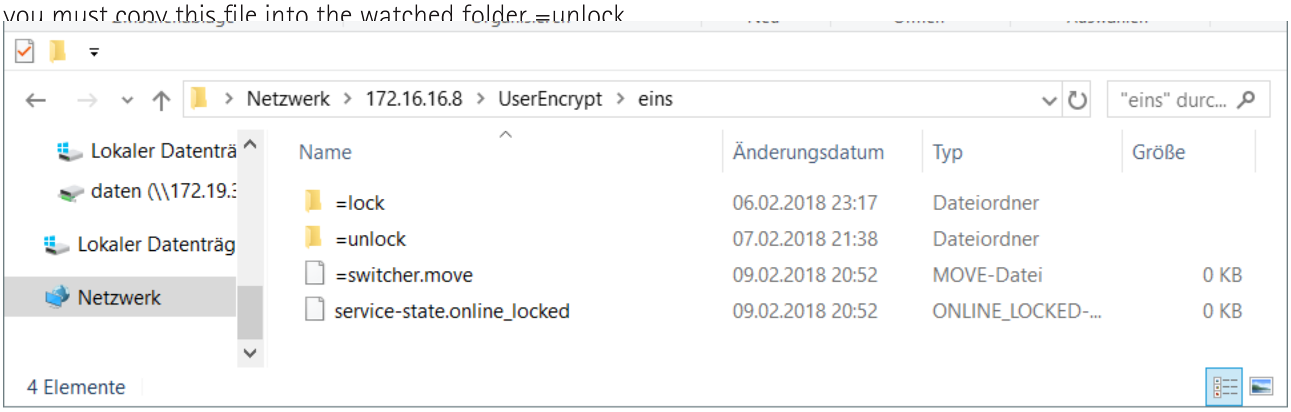
In a next step, you must start the autolock service in menu Services > autolock.
This will check for and optionally create a „UserEncrypt" ZFS filesystem with a watched subfolders per encrypted filesystem.

At this point you can enable/ disable the whole userlock functionality be enabling or disabling the SMB share UserEncrpt and setup ACL permissions for this share or more specific for the subfolders.
Tipp: You can set permissions for any user when you SMB connect as root.

A user with permissions can now lock/unlock a filesystem by simply moving the switcher file into the subfolders /=lock or /=unlock and check service and lockstate with a service control file that is updated automatically.

- or set SMB Userlock to yes

With smbkey as method, you must copy the control file =switcher.move to your desktop. Open the file with an editor and insert the smbkey (from menu ZFS Filesystems > Encryption). To unlock a filesystem with userlock=smbkey, you must copy this file into the watched folder =unlock



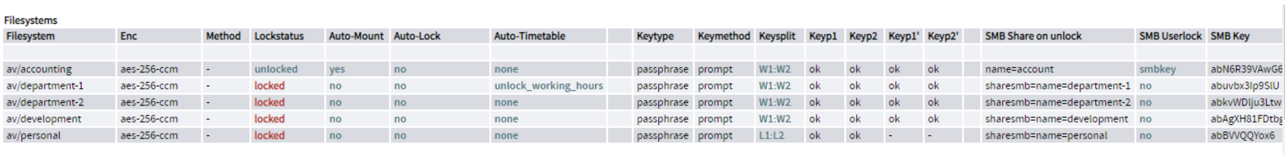
Name	Änderungsdatum	Typ	Größe
=lock	06.02.2018 23:17	Dateiordner	
=unlock	07.02.2018 21:38	Dateiordner	
=switcher.move	09.02.2018 20:52	MOVE-Datei	0 KB
service-state.online_locked	09.02.2018 20:52	ONLINE_LOCKED-...	0 KB

watched folder for filesystem tank/eins

2.5 Enable auto locking/unlocking (under development)

If user-locking is working you can add auto-locking.
This means that a filesystem can be automatically unlocked and/or locked example always in the evening or automatically unlicked at working hourse. This will limit the risk of a dataloss due a hack.

To enable Autolock, select a timetable in menu ZFS filesystems and set Autolock to yes



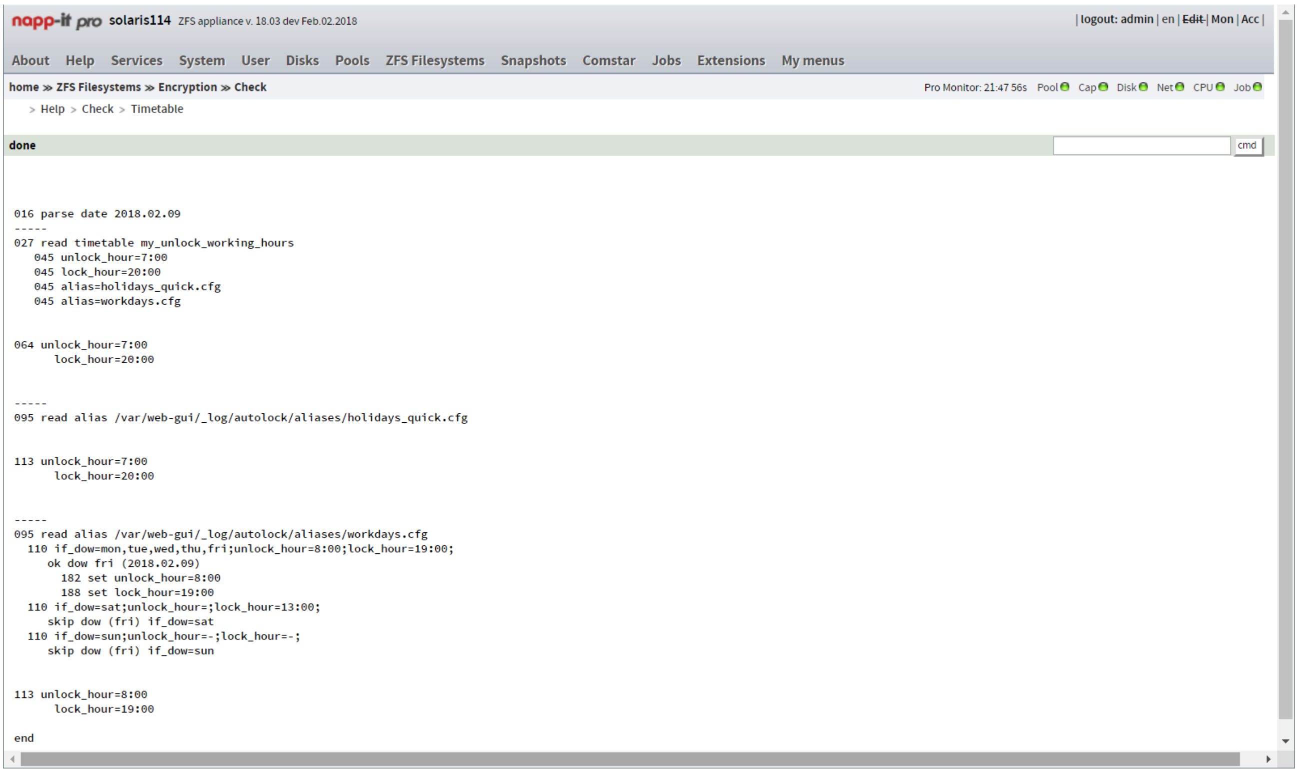
Filesystems

Filesystem	Enc	Method	Lockstatus	Auto-Mount	Auto-Lock	Auto-Timetable		Keytype	Keymethod	Keysplit	Keyp1	Keyp2	Keyp1'	Keyp2'		SMB Share on unlock	SMB Userlock	SMB Key
av/accounting	aes-256-ccm	-	unlocked	yes	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		name=account	smbkey	abN6R39VAwG6
av/department-1	aes-256-ccm	-	locked	no	no	unlock_working_hours		passphrase	prompt	W1:W2	ok	ok	ok	ok		sharesmb=name=department-1	no	abuvbx3Ip9SIU
av/department-2	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		sharesmb=name=department-2	no	abkvWDIju3Ltw
av/development	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	W1:W2	ok	ok	ok	ok		sharesmb=name=development	no	abAgXH81FDtbg
av/personal	aes-256-ccm	-	locked	no	no	none		passphrase	prompt	L1:L2	ok	ok	-	-		sharesmb=name=personal	no	abBVVQQYox6

Test a timetable

Use menu ZFS filesystems > Encryption > Check to parse a timetable for a given date.
The timetable for this check is a file in /var/web-gui/_log/autolock/timetables/my_unlock_working_hours.cfg

```
# defaults
unlock_hour=7:00
lock_hour=20:00                              # can be overwritten by rules, interval 15min

# overwrite lock/unlock per holidays.cfg (day of week) with exit
alias=holidays_quick.cfg

# overwrite lock/unlock per workday (day of week)
alias=workdays.cfg
```

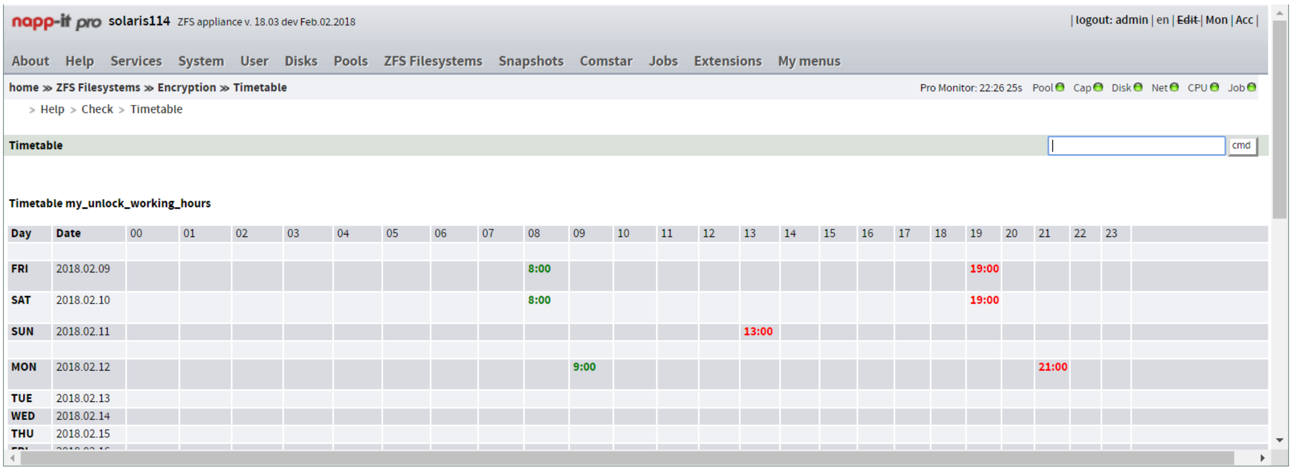

napp-it pro solaris114 ZFS appliance v. 18.03 dev Feb.02.2018
| logout: admin | en | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions My menus
home » ZFS Filesystems » Encryption » Check
Pro Monitor: 21:47 56s Pool Cap Disk Net CPU Job
> Help > Check > Timetable
cmd

done

```
016 parse date 2018.02.09
-----
027 read timetable my_unlock_working_hours
   045 unlock_hour=7:00
   045 lock_hour=20:00
   045 alias=holidays_quick.cfg
   045 alias=workdays.cfg


064 unlock_hour=7:00
      lock_hour=20:00


-----
095 read alias /var/web-gui/_log/autolock/aliases/holidays_quick.cfg


113 unlock_hour=7:00
      lock_hour=20:00


-----
095 read alias /var/web-gui/_log/autolock/aliases/workdays.cfg
  110 if_dow=mon,tue,wed,thu,fri;unlock_hour=8:00;lock_hour=19:00;
     ok dow fri (2018.02.09)
       182 set unlock_hour=8:00
       188 set lock_hour=19:00
  110 if_dow=sat;unlock_hour=;lock_hour=13:00;
     skip dow (fri) if_dow=sat
  110 if_dow=sun;unlock_hour=-;lock_hour=-;
     skip dow (fri) if_dow=sun


113 unlock_hour=8:00
      lock_hour=19:00

end
```

2.6 Timetables (under development)

You can print a timetable to control the autolock function (unlock time and lock time) for next weeks, months or year in menu „ZFS Filesystems > Encryption > Timetable“ for a selected timetable


napp-it pro solaris114 ZFS appliance v. 18.03 dev Feb.02.2018
| logout: admin | en | ~~Edit~~ | Mon | Acc |
About Help Services System User Disks Pools ZFS Filesystems Snapshots Comstar Jobs Extensions My menus
home » ZFS Filesystems » Encryption » Timetable
Pro Monitor: 22:26 25s Pool Cap Disk Net CPU Job
> Help > Check > Timetable
Timetable
cmd

Timetable my_unlock_working_hours

Day	Date	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
FRI	2018.02.09									8:00											19:00				
SAT	2018.02.10									8:00											19:00				
SUN	2018.02.11														13:00										
MON	2018.02.12										9:00												21:00		
TUE	2018.02.13																								
WED	2018.02.14																								
THU	2018.02.15																								

2.7 Setup Timetables (under development)

Timetables are textfiles in /var/web-gui/_log/autolock/timetables/. If you want to setup your own timetable, create a new timetable file and start the name with my. Do not modify default timetables as they are overwritten on updates. In a timetable you can set unlock_hour and lock_hour as defaults and add aliases where the time is set.

```
##########
Timetables
##########

Timetables are used to define lock_hour and/or unlock_hour time for current date
Day/ Date settings always based on aliases

Timetable work like a firewall that is processing lock or unlock from top to bottom:
The first matching value does the job (cancel or trigger)

#################
Timetable example
#################  working_time.cfg with entries like

# defaults
unlock_hour=7:00
lock_hour=20:00                                # can be overwritten by rules, interval 15min

# priority setting with exit
alias=my_priority_quick.cfg

# overwrite lock/unlock per holidays.cfg (day of week) with exit
alias=holidays.quick.cfg

# overwrite lock/unlock per workday (day of week)
alias=workday.cfg
```

2.7.1 Aliases (under development)

Aliases are textfiles in /var/web-gui/_log/autolock/aliases/. If you want to setup your own alias or modify one, create a new alias file and start the name with my. Do not modify default aliases as they are overwritten on updates. In an alias you can set unlock_hour and lock_hour as defaults and define and/ or rules to modify unlock_hour or lock_hour. If you use the same aliasname like a default alias, every reference to the default will be automatically replaced by the my one. Exampe my_holiday.cfg overwrites holiday.cfg automatically.

#######
Aliases
#######

Aliases can be used as references in timetables to specify a date, a day of week or an hour either as a single value or a date range like 18.2-25.2 (hour must be a single value, dow can be a list like mo,di,fr). (you should not use a concrete time or date in a timetable)

If you want to modify aliases, duplicate an alias file with some name that starts with my_.
It will be then used automaticalls instead the default one.

You can also create other my_aliases.cfg for other rules

##
Alias files can contain a if_dow, if_day, if_month, if_year, if_date, if_between (yyyy.mm.dd-yyyy.mm.dd)
If you define more than one if, the are AND related. If you use a commalist, they are OR related

```
# example dow
if_dow=mon,tue,wed,thu,fri;   unlock_hour=8:00; lock_hour=21:00;        # without exit -> continue parsing
if_dow=sa;                    unlock_hour=8:00; lock_hour=13:00;        # without exit -> continue parsing
if_dow=sun;                   unlock_hour=;   lock_hour=;               # no autolock/unlock

# example quick (holiday or priority rules)
if_between=2018.12.23-2019.01.06;  unlockhour=;    lockhour=21:00;    exit;        # exit at the end means a quick rule

# example multiple ifs
if_between=2018.12.23-2019.01.06;  if_dow=sun; unlockhour=;  lockhour=13:00; exit;   # exit at the end means a quick rule,
```

In general
Rules are based on keywords if_day, if_dow (mon to sun), if_month, if_year, if_between and exit
Rules are separated with „ ; " in an and manner and within the same key with a commo for or relations ex if_dow=sat,sun

At the moment, edit the timetables and aliases with WinSCP.

3.0 more manuals

https://www.napp-it.org/manuals/index_en.html