SOC TALK

security_onion

@bugg

What is Security Onion?

- Like Kali for security monitoring
- A bunch of tools in one place
  - Full ELK Stack (Elastic/Logstash/Kibana)
  - Snort
  - Bro
  - Suricata
  - Wazuh
  - Squil
  - And More! CALL NOW!
- Easy setup & configuration
- FOSS (Free, Open-Source Software)
- Nothing to do with TOR!

What do you do with it?

- Monitor Stuff!
- IDS (Intrusion Detection System)
  - Bro, Snort, etc.
- HIDS (Host-Intrusion Detection System)
  - OSSEC, etc.
- Log Management
  - ELK Stack, etc.
- And More!

How Easy is *“Easy setup & configuration”*?

Download and Verify

16.04.5.3 ISO image:
https://github.com/Security-Onion-Solutions/security-onion/releases/download/v16.04.5.3/securityonion-16.04.5.3.iso

Signature for ISO image:
https://github.com/Security-Onion-Soluti

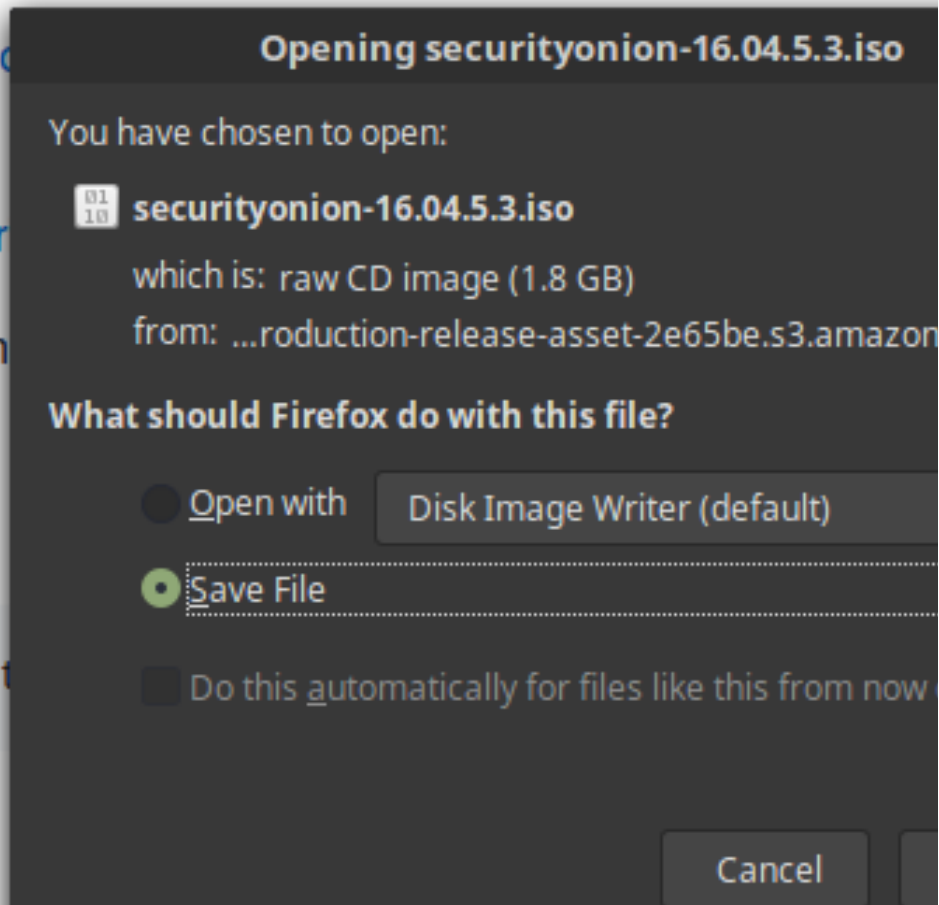
Signing key:
https://raw.githubusercontent.com/Secur

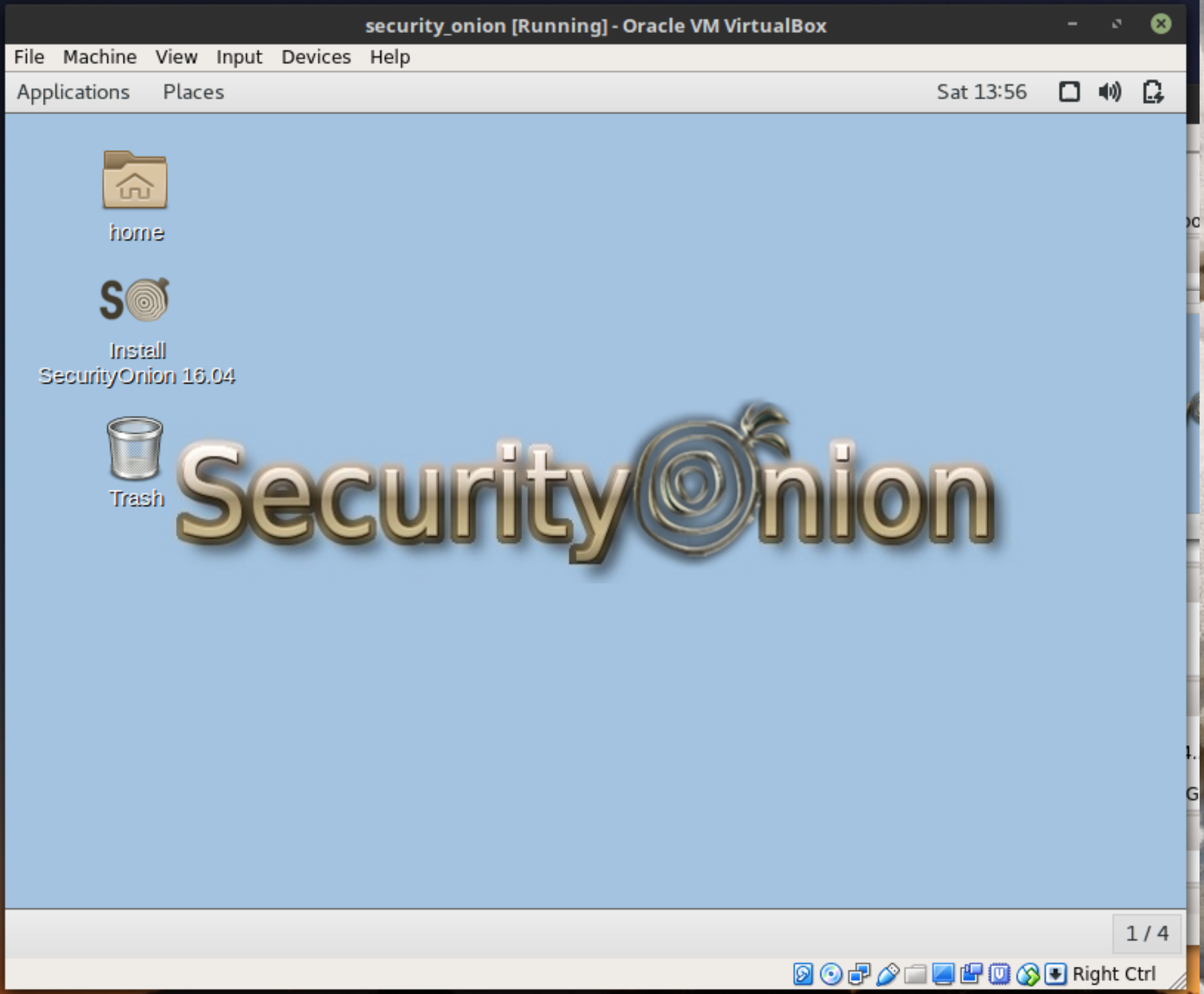
For example, here are the steps you can
image.

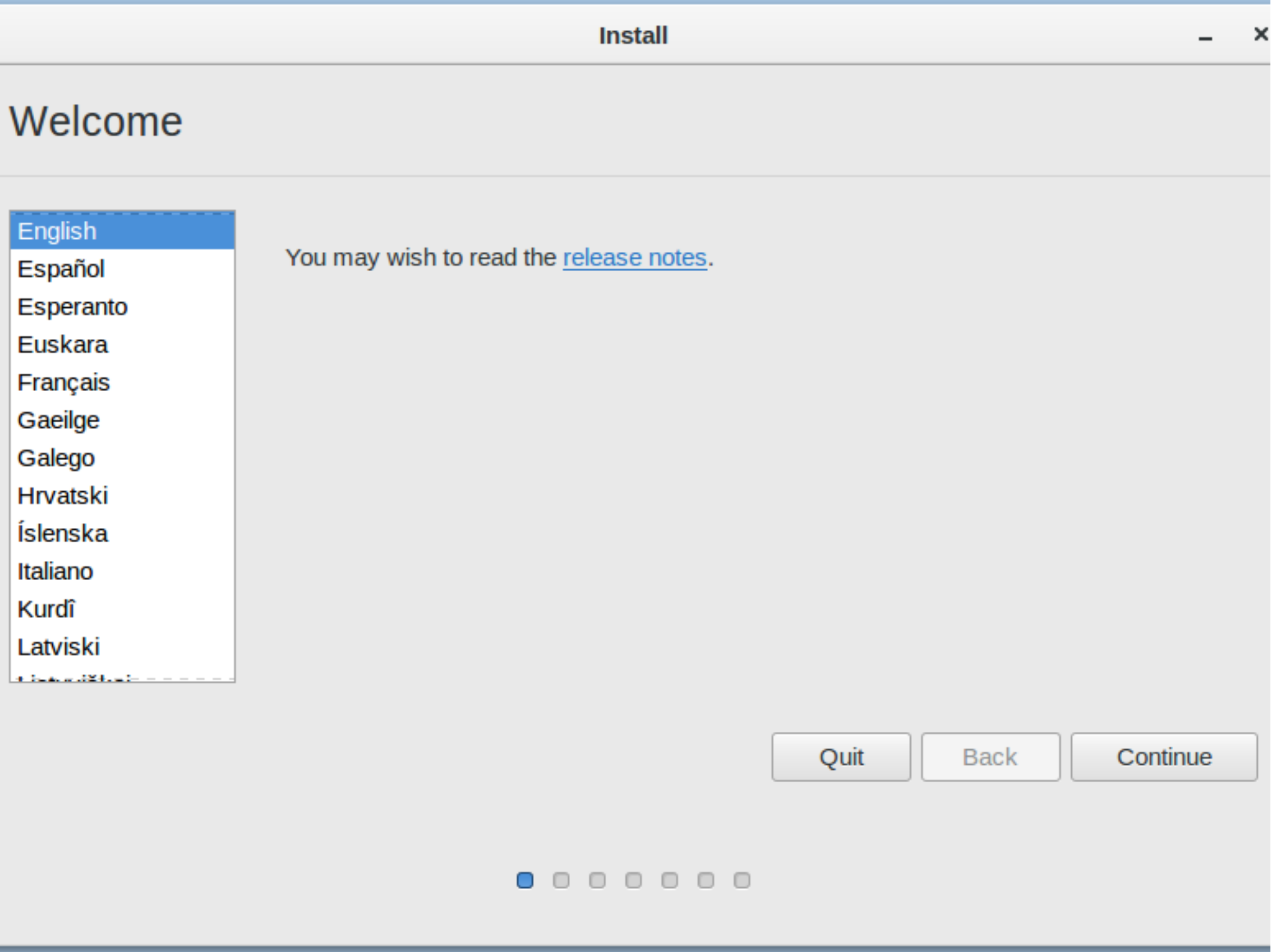
Download the signing key:

```
wget https://raw.githubusercontent
```

Import the signing key:




security_onion [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Sat 13:56
home
Install SecurityOnion 16.04
Trash
SecurityOnion
1 / 4
Right Ctrl


Install
Welcome
English
Español
Esperanto
Euskara
Français
Gaeilge
Galego
Hrvatski
Íslenska
Italiano
Kurdî
Latviski
You may wish to read the release notes.
Quit
Back
Continue

Install

Preparing to install SecurityOnion

- [x] Download updates while installing SecurityOnion

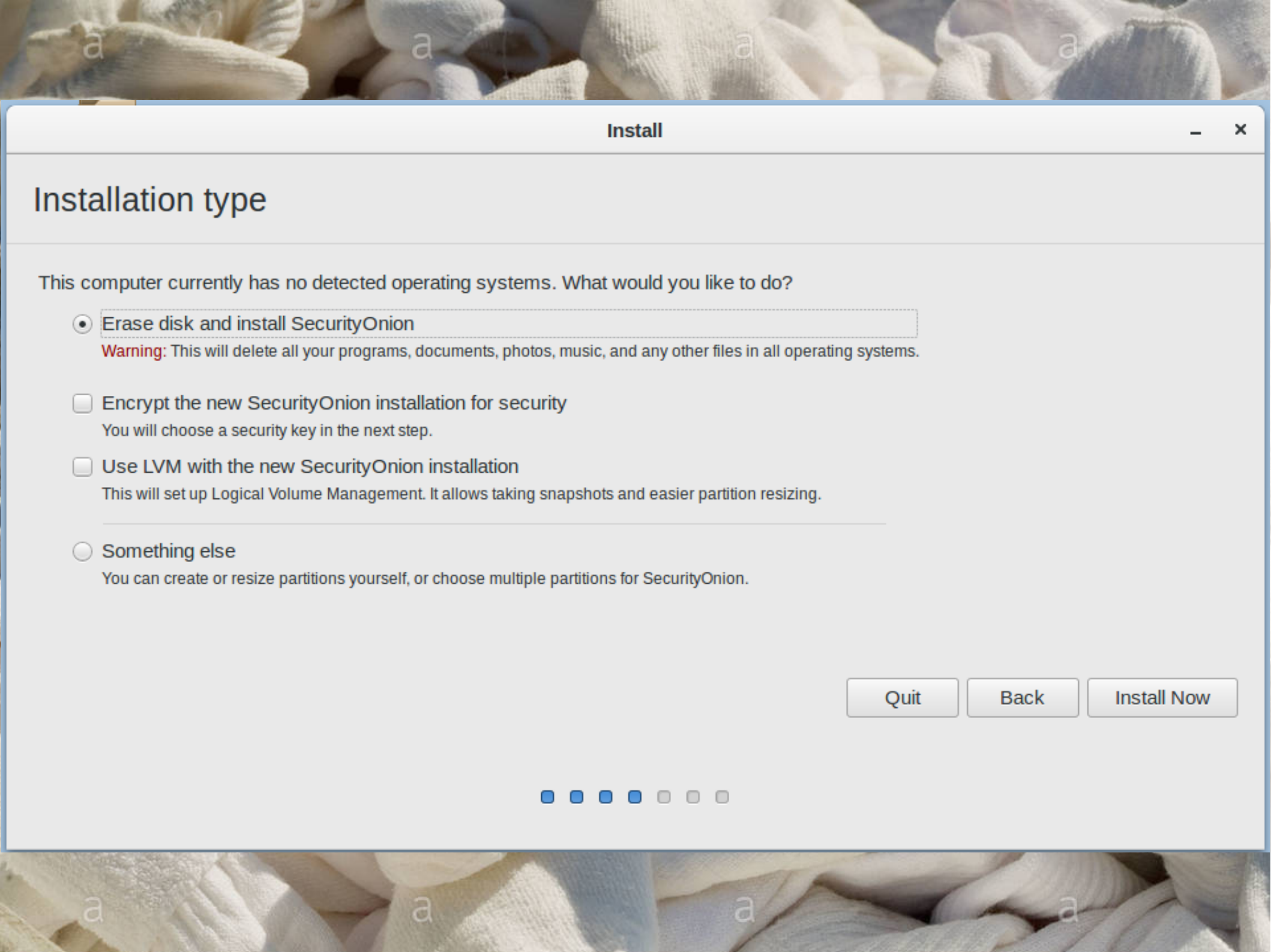
  This saves time after installation.

- [x] Install third-party software for graphics and Wi-Fi hardware, Flash, MP3 and other media

  This software is subject to license terms included with its documentation. Some is proprietary.

  Fluendo MP3 plugin includes MPEG Layer-3 audio decoding technology licensed from Fraunhofer IIS and Technicolor SA.

Quit Back Continue


Install
Installation type
This computer currently has no detected operating systems. What would you like to do?
Erase disk and install SecurityOnion
Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.
Encrypt the new SecurityOnion installation for security
You will choose a security key in the next step.
Use LVM with the new SecurityOnion installation
This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing.
Something else
You can create or resize partitions yourself, or choose multiple partitions for SecurityOnion.
Quit
Back
Install Now

Install

Where are you?

Denver

Back Continue

Install

Keyboard layout

Choose your keyboard layout:

English (Ghana)	English (US)
English (Nigeria)	English (US) - Cherokee
English (South Africa)	English (US) - English (Colemak)
English (UK)	English (US) - English (Dvorak alternative international no dead keys)
English (US)	English (US) - English (Dvorak)
Esperanto	English (US) - English (Dvorak, international with dead keys)
Estonian	English (US) - English (Macintosh)
Faroese	English (US) - English (Programmer Dvorak)
Filipino	English (US) - English (US, alternative international)

Type here to test your keyboard

Detect Keyboard Layout

Back Continue

Install

Who are you?

Your name:

Your computer's name: security-onion

The name it uses when it talks to other computers.

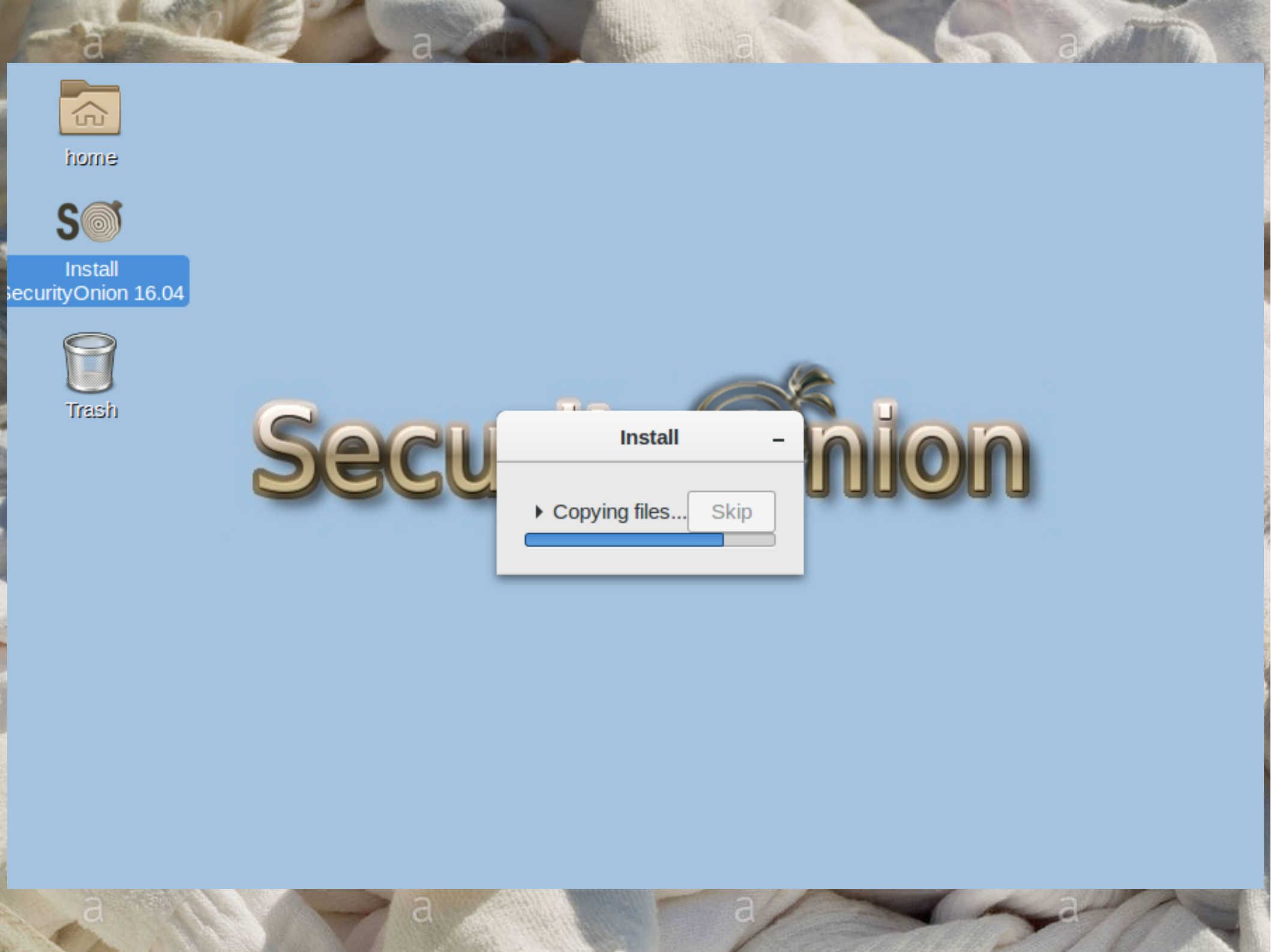
Pick a username: user

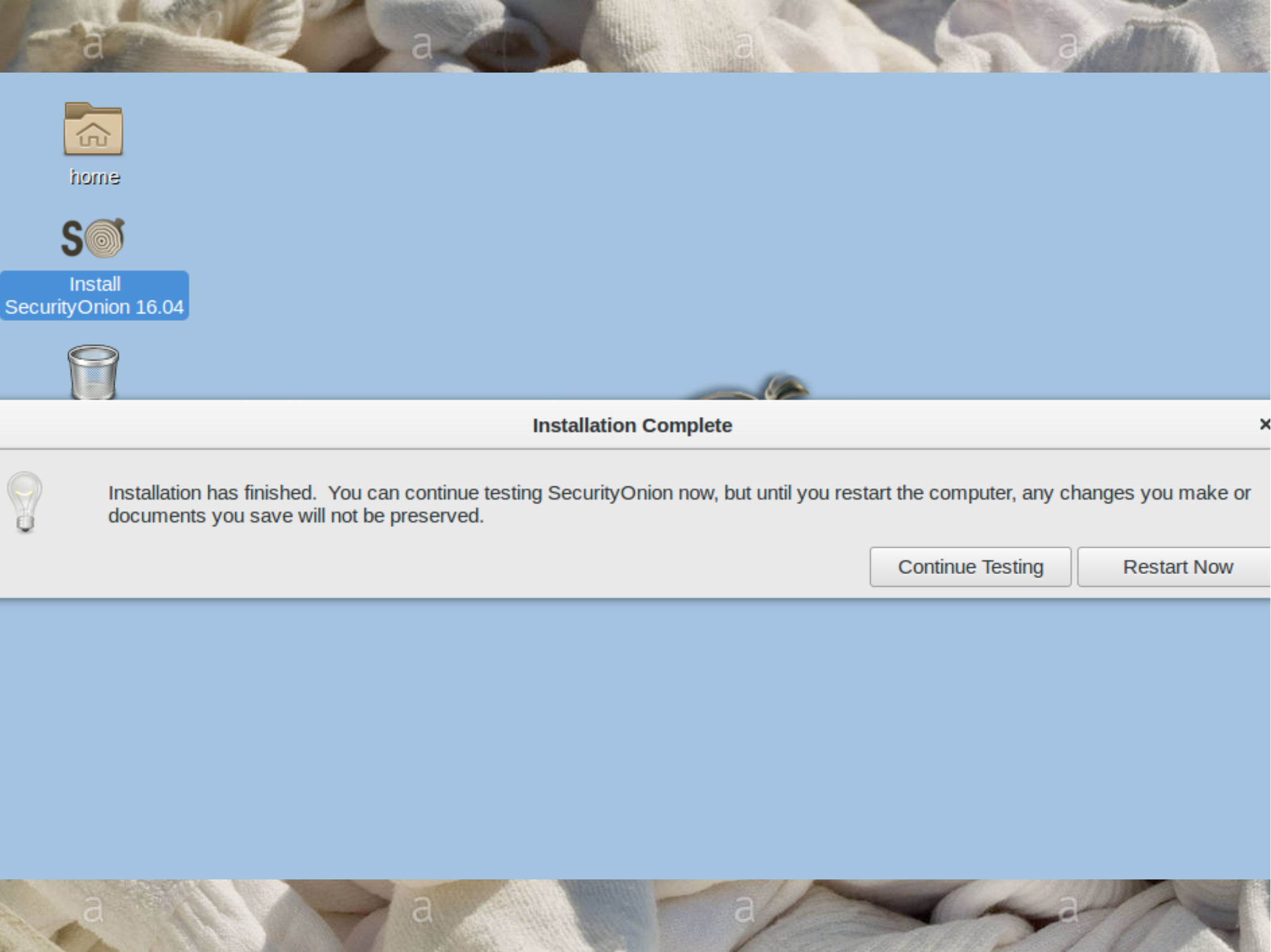
Choose a password: •••••••• Weak password

Confirm your password: ••••••••

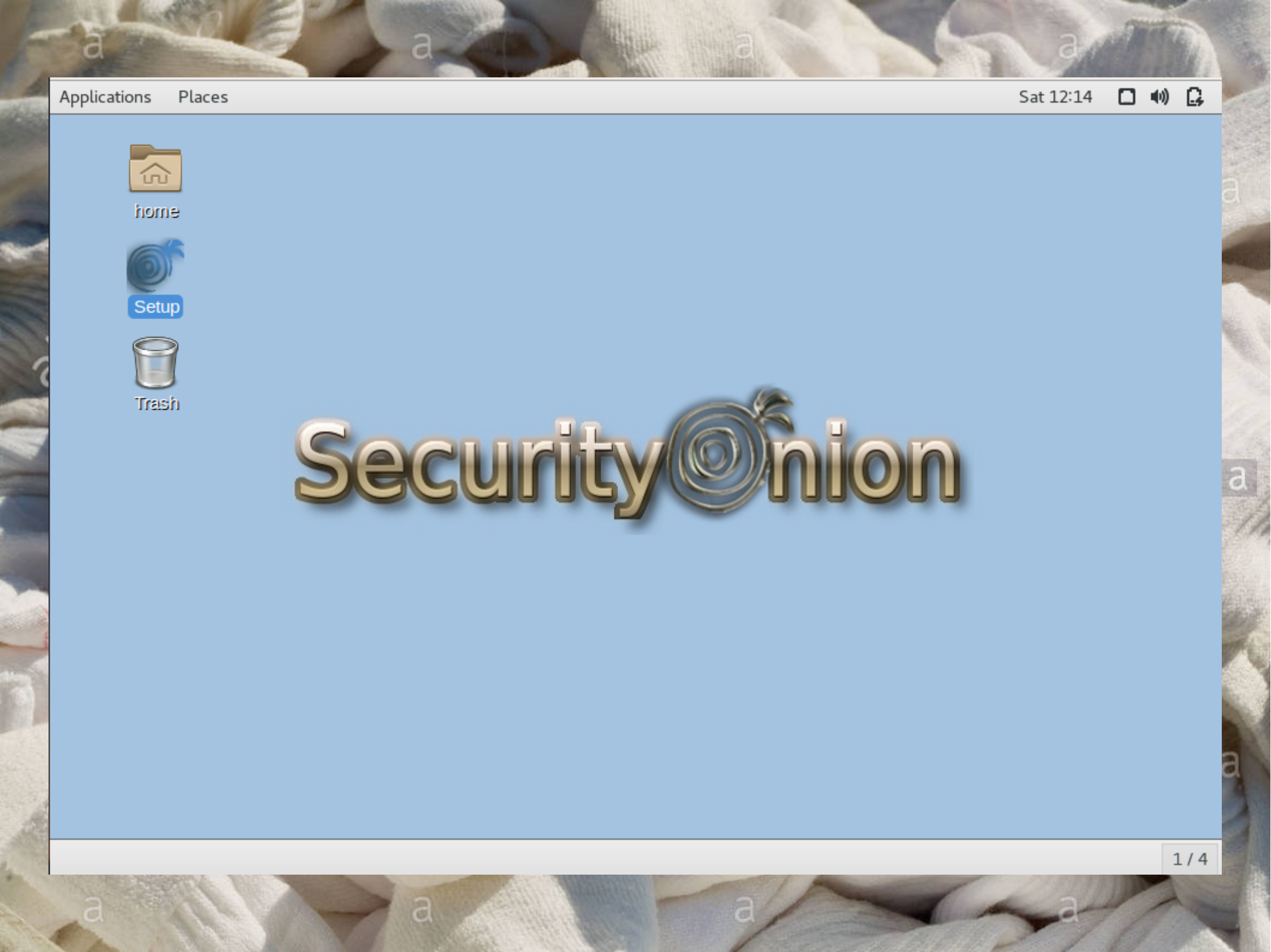
- ( ) Log in automatically
- (•) Require my password to log in
  - [ ] Encrypt my home folder

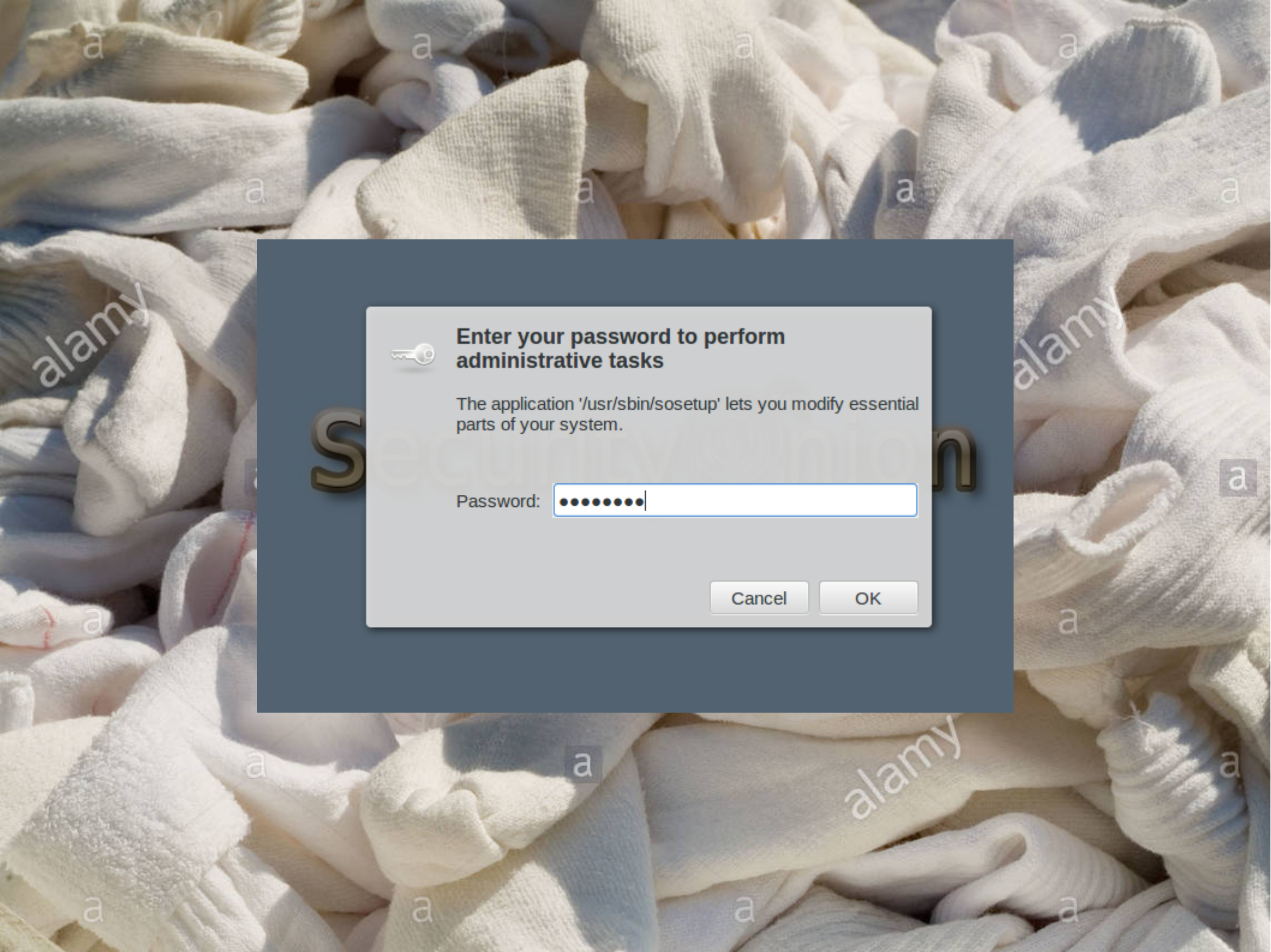
Back Continue

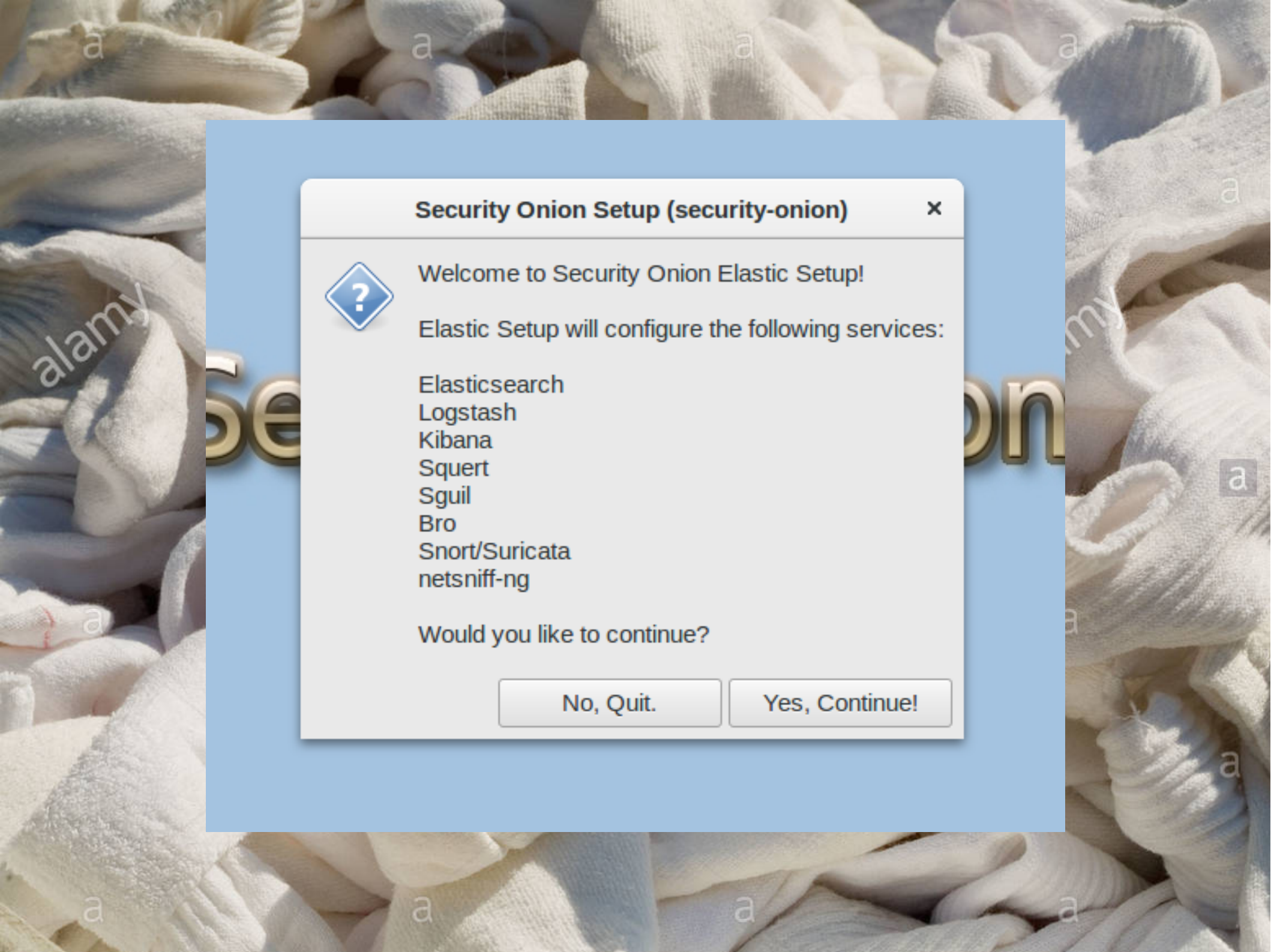

home
Install SecurityOnion 16.04
Trash
Install
Copying files...
Skip

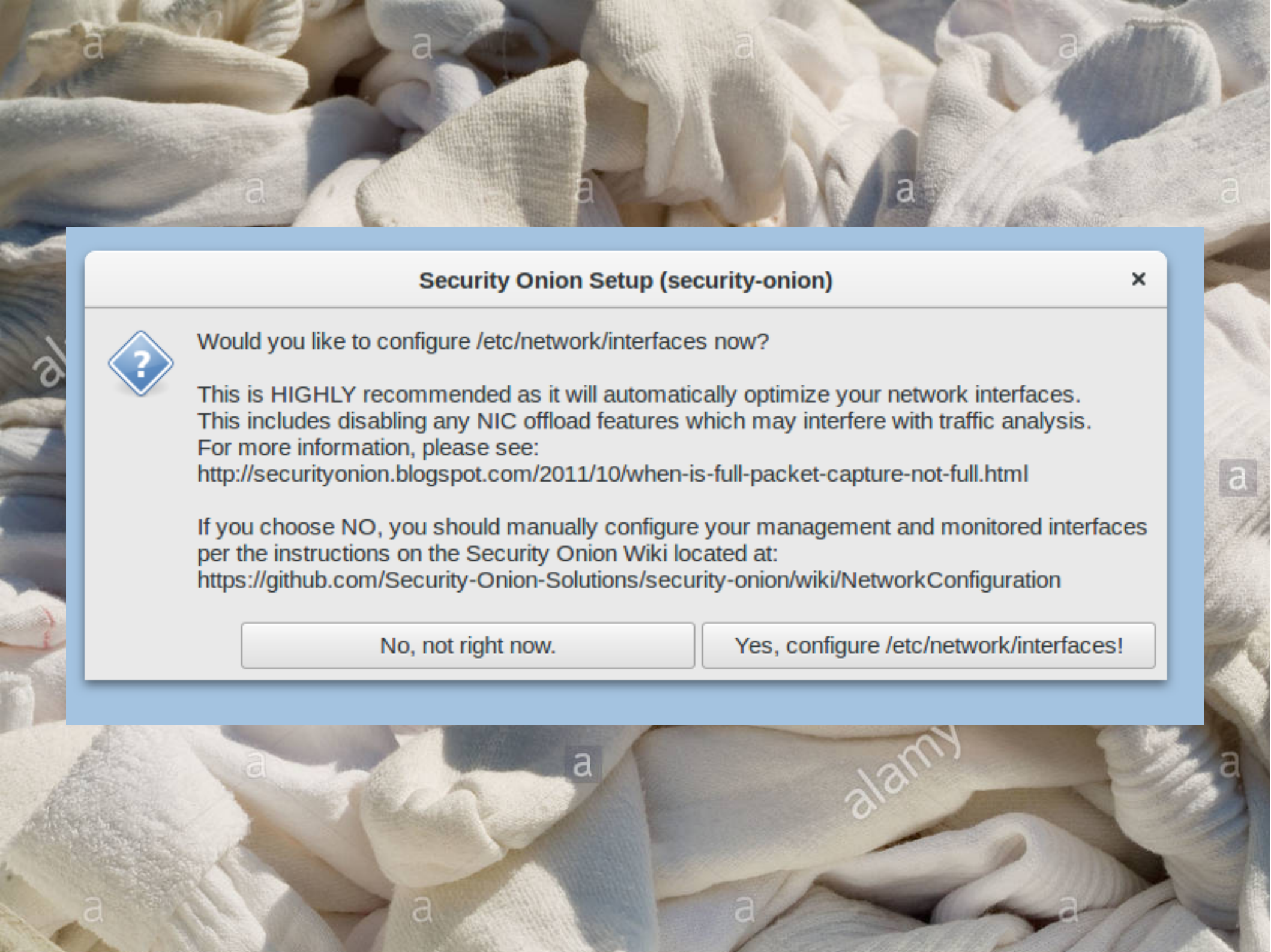

home
Install SecurityOnion 16.04
Installation Complete
Installation has finished. You can continue testing SecurityOnion now, but until you restart the computer, any changes you make or documents you save will not be preserved.
Continue Testing
Restart Now

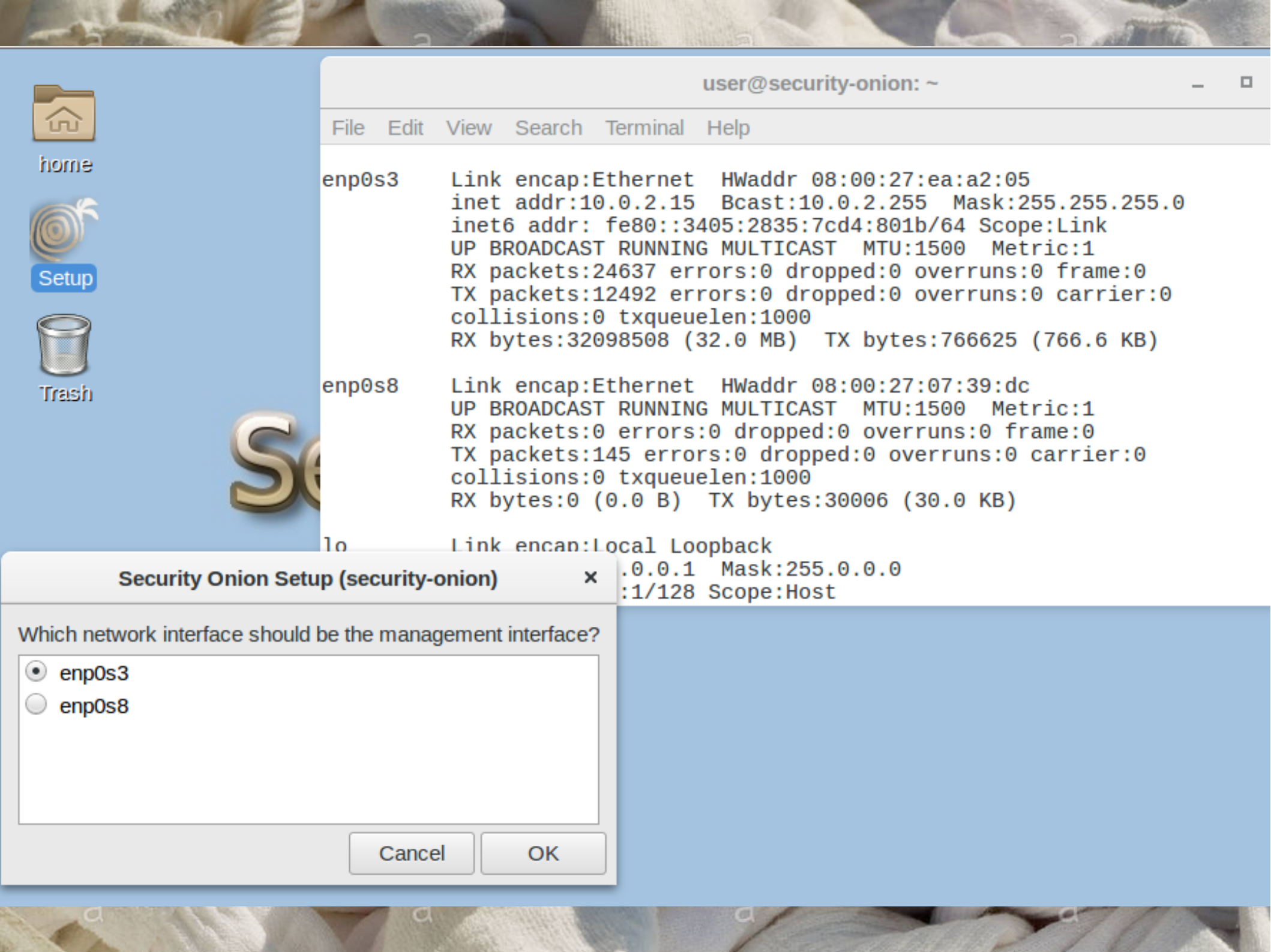

security-onion
en_US
27 Oct, 12:14
Security Onion
user
Cancel
Log In

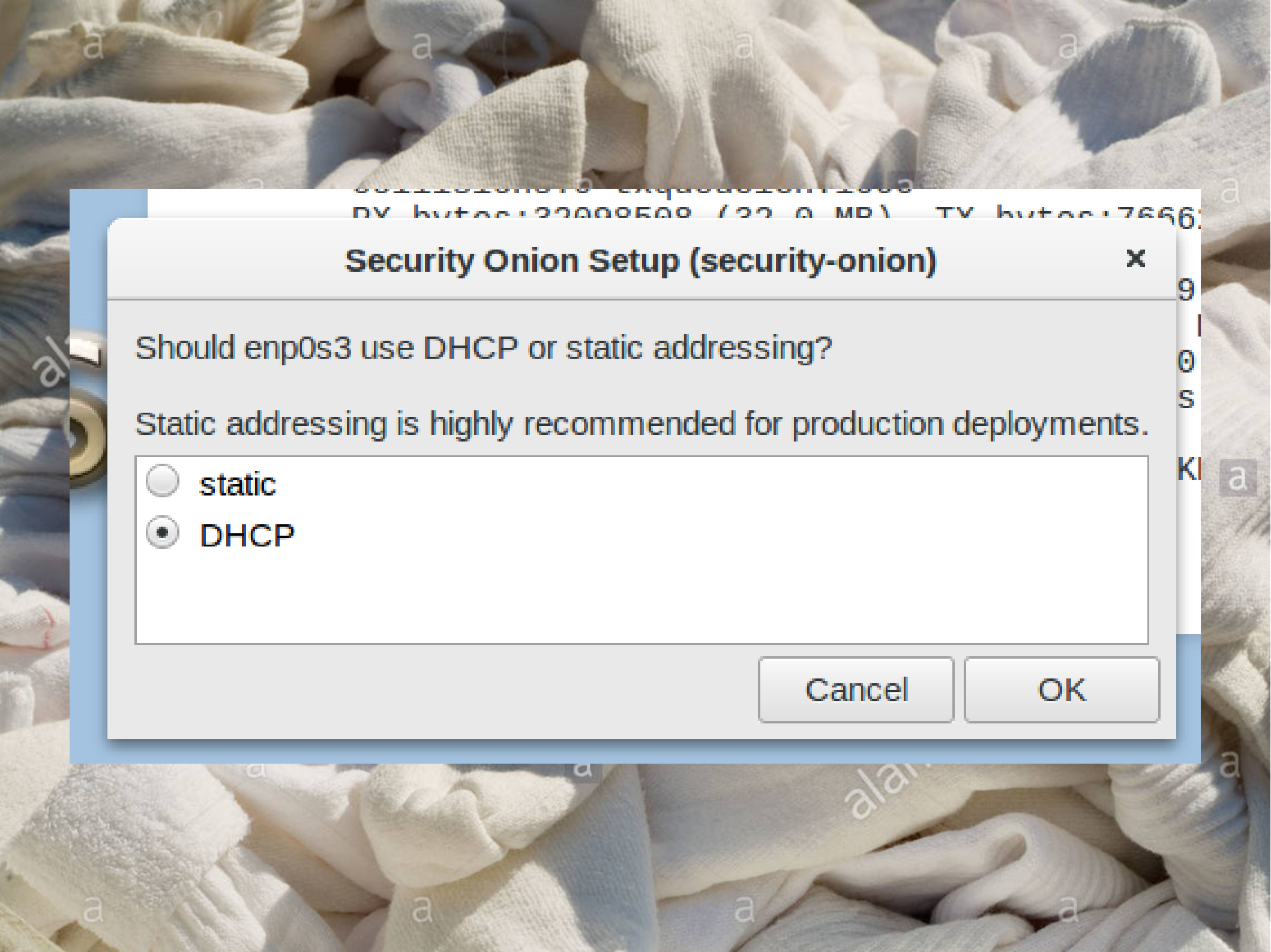

Applications
Places
Sat 12:14
home
Setup
Trash
SecurityOnion
1 / 4

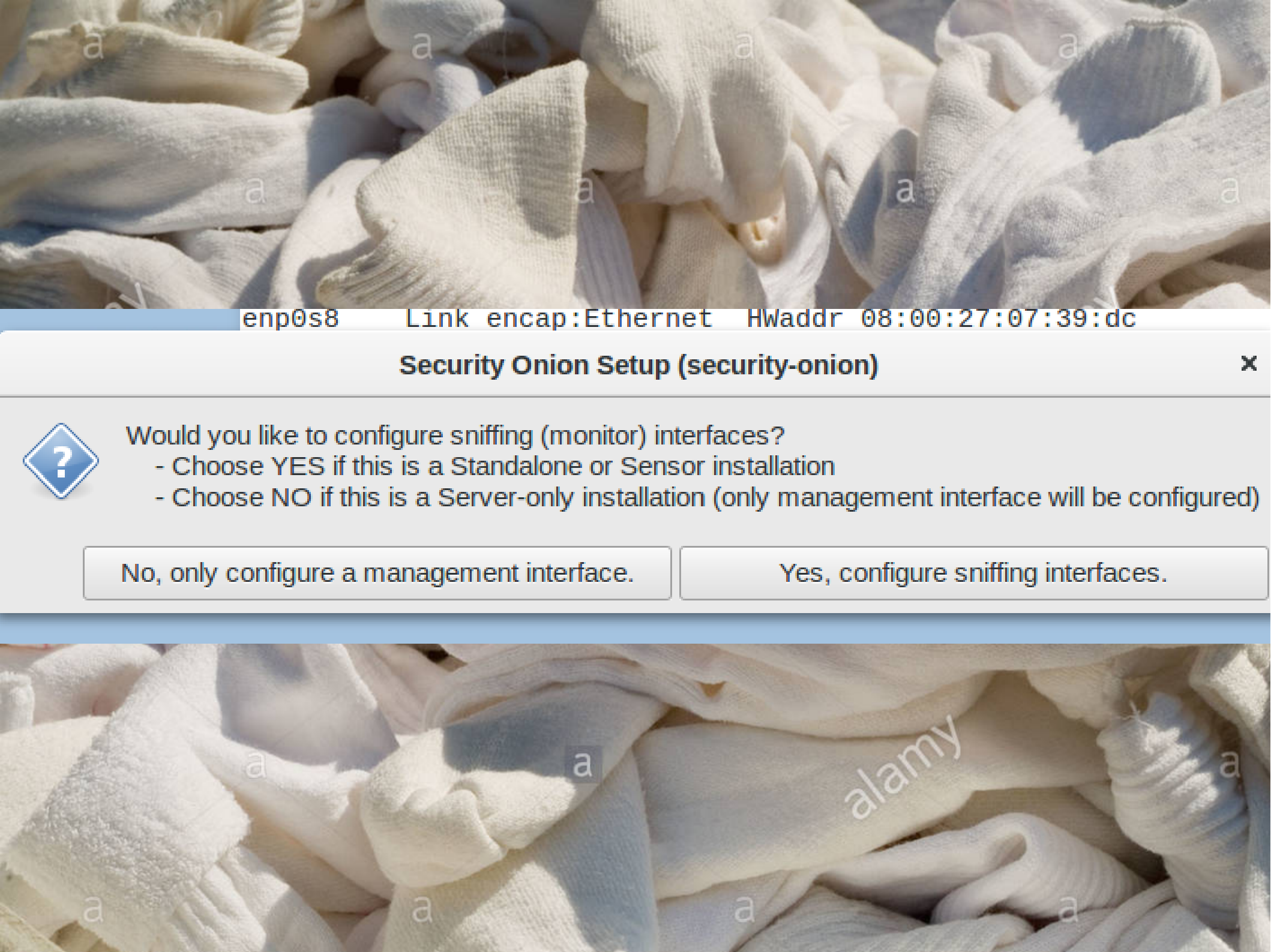

Enter your password to perform administrative tasks
The application '/usr/sbin/sosetup' lets you modify essential parts of your system.
Password:
Cancel
OK

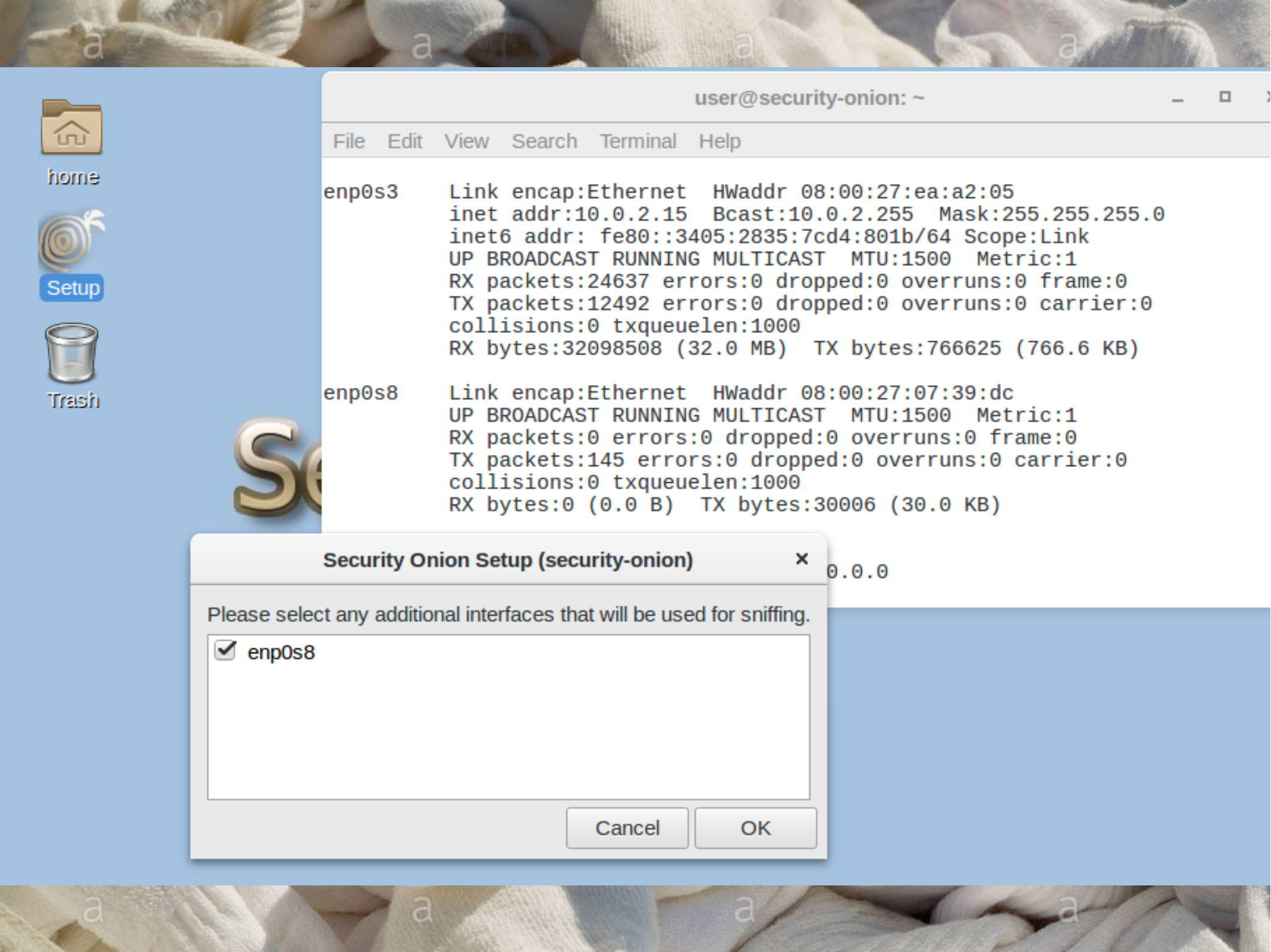

Security Onion Setup (security-onion)
Welcome to Security Onion Elastic Setup!
Elastic Setup will configure the following services:
Elasticsearch
Logstash
Kibana
Squert
Sguil
Bro
Snort/Suricata
netsniff-ng
Would you like to continue?
No, Quit.
Yes, Continue!


Security Onion Setup (security-onion)
Would you like to configure /etc/network/interfaces now?
This is HIGHLY recommended as it will automatically optimize your network interfaces.
This includes disabling any NIC offload features which may interfere with traffic analysis.
For more information, please see:
http://securityonion.blogspot.com/2011/10/when-is-full-packet-capture-not-full.html
If you choose NO, you should manually configure your management and monitored interfaces per the instructions on the Security Onion Wiki located at:
https://github.com/Security-Onion-Solutions/security-onion/wiki/NetworkConfiguration
No, not right now.
Yes, configure /etc/network/interfaces!


home
Setup
Trash
user@security-onion: ~
File Edit View Search Terminal Help
enp0s3 Link encap:Ethernet HWaddr 08:00:27:ea:a2:05
inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::3405:2835:7cd4:801b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:24637 errors:0 dropped:0 overruns:0 frame:0
TX packets:12492 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:32098508 (32.0 MB) TX bytes:766625 (766.6 KB)
enp0s8 Link encap:Ethernet HWaddr 08:00:27:07:39:dc
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:145 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:30006 (30.0 KB)
lo Link encap:Local Loopback
.0.0.1 Mask:255.0.0.0
:1/128 Scope:Host
Security Onion Setup (security-onion)
Which network interface should be the management interface?
enp0s3
enp0s8
Cancel
OK


Security Onion Setup (security-onion)
Should enp0s3 use DHCP or static addressing?
Static addressing is highly recommended for production deployments.
static
DHCP
Cancel
OK


enp0s8 Link encap:Ethernet HWaddr 08:00:27:07:39:dc
Security Onion Setup (security-onion)
Would you like to configure sniffing (monitor) interfaces?
- Choose YES if this is a Standalone or Sensor installation
- Choose NO if this is a Server-only installation (only management interface will be configured)
No, only configure a management interface.
Yes, configure sniffing interfaces.


home
Setup
Trash
user@security-onion: ~
File Edit View Search Terminal Help
enp0s3 Link encap:Ethernet HWaddr 08:00:27:ea:a2:05
inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::3405:2835:7cd4:801b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:24637 errors:0 dropped:0 overruns:0 frame:0
TX packets:12492 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:32098508 (32.0 MB) TX bytes:766625 (766.6 KB)
enp0s8 Link encap:Ethernet HWaddr 08:00:27:07:39:dc
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:145 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:30006 (30.0 KB)
0.0.0
Security Onion Setup (security-onion)
Please select any additional interfaces that will be used for sniffing.
enp0s8
Cancel
OK

collisions:0 txqueuelen:1000

Security Onion Setup (security-onion)

We're about to do the following:

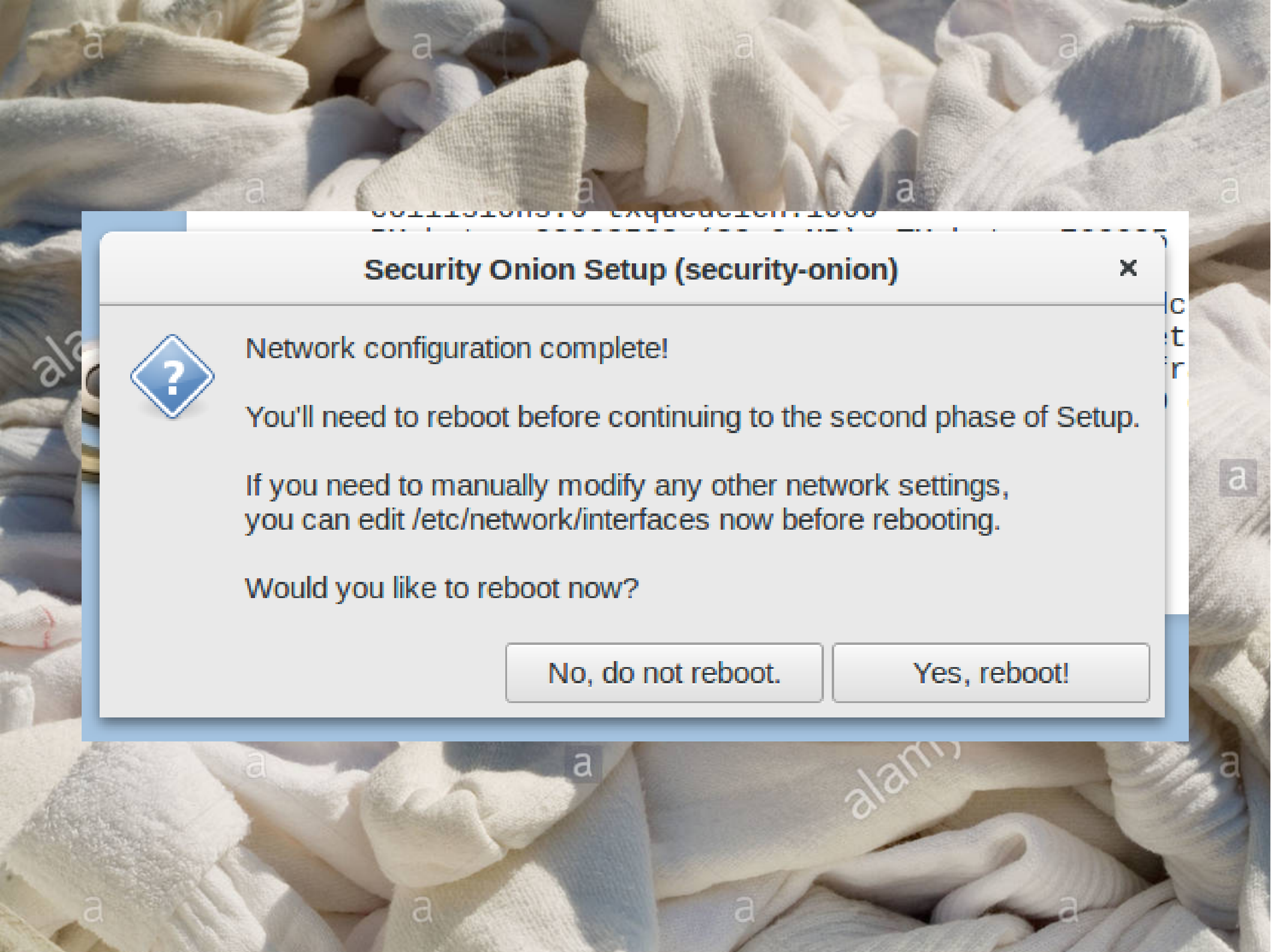
- Backup existing network configuration to /etc/network/interfaces.bak
- Configure the management interface enp0s3 using DHCP.
- Configure the following interface(s) for sniffing:
  enp0s8

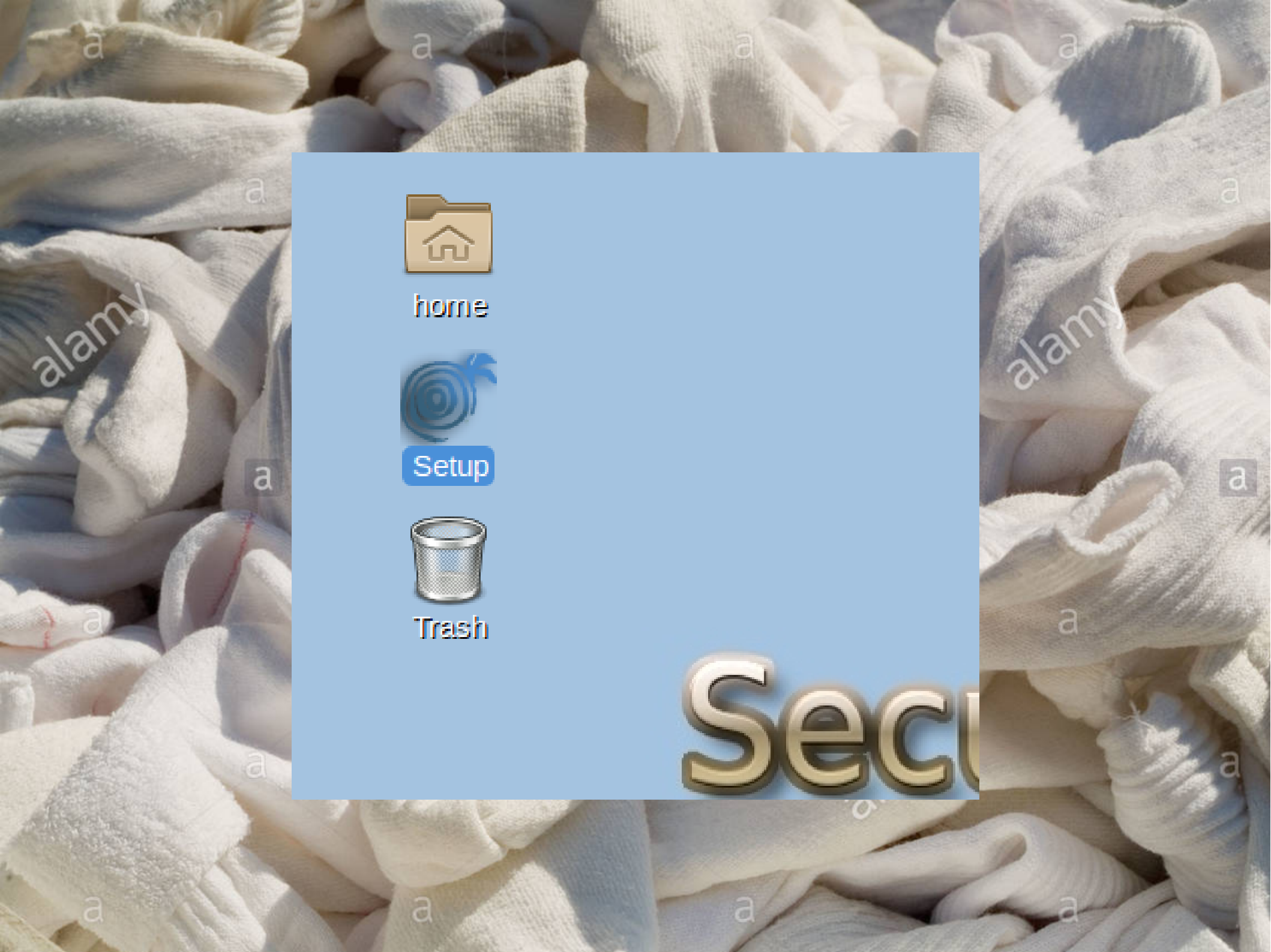
We're about to make changes to your system!

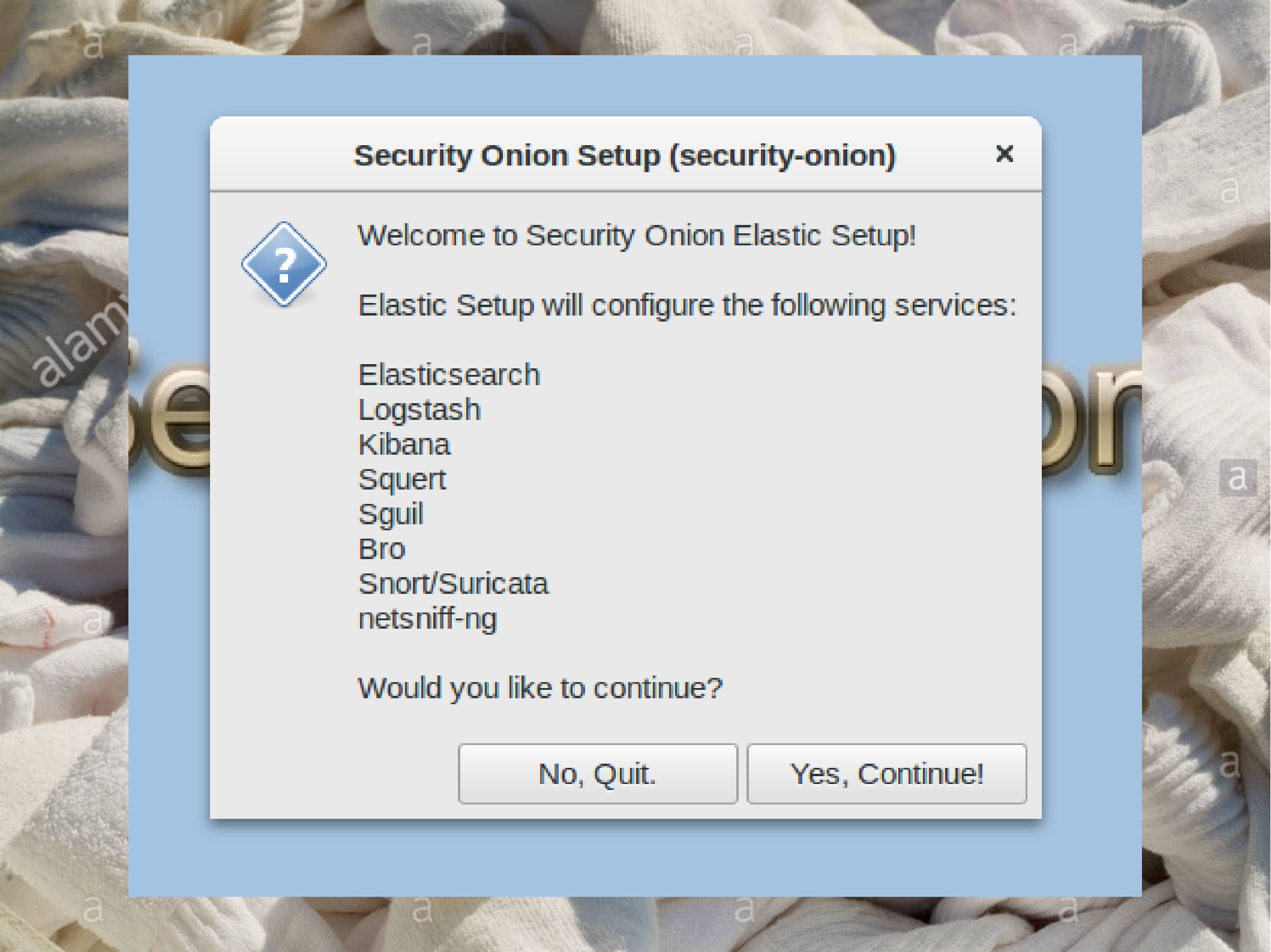
Would you like to continue?

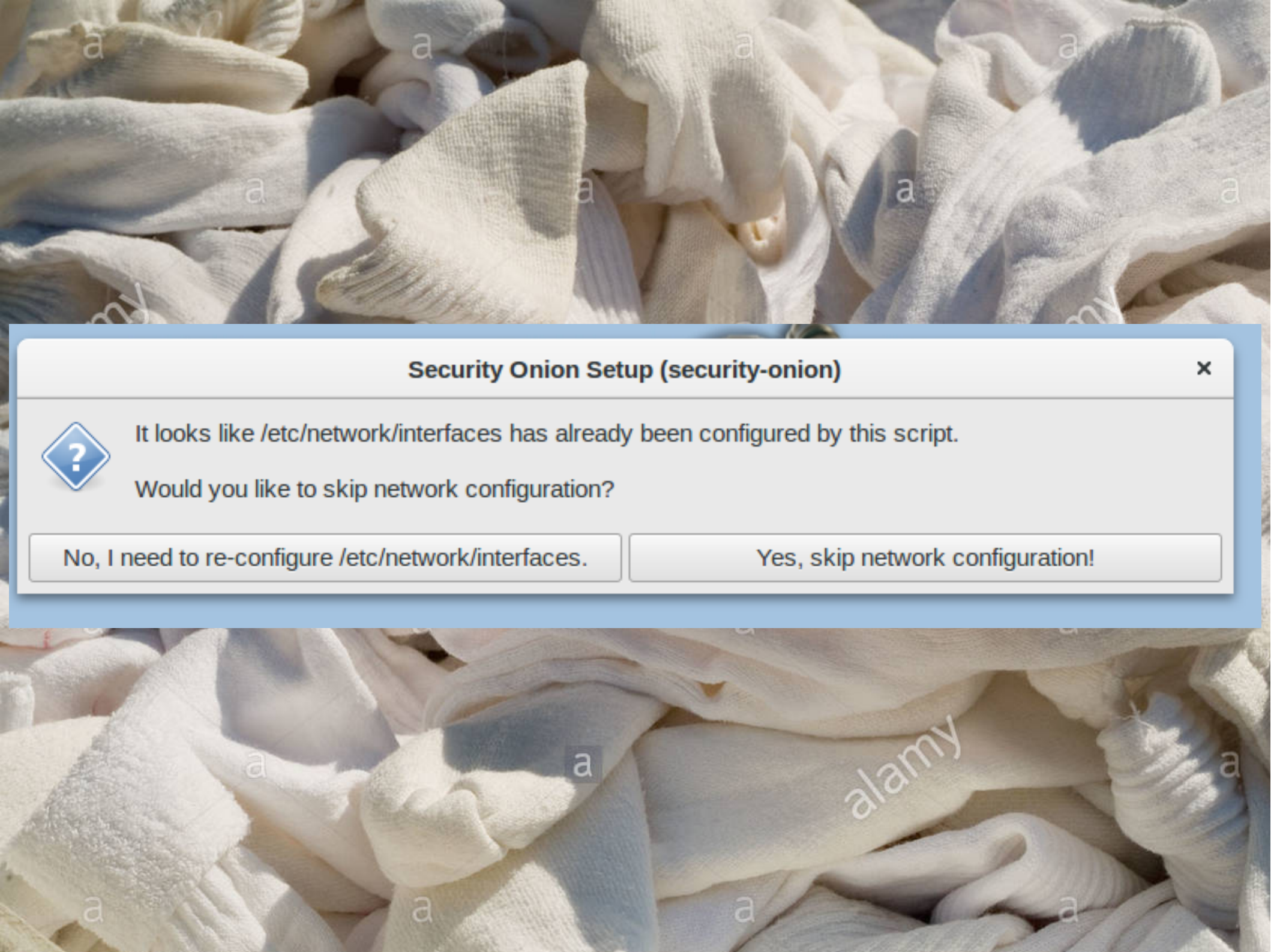
No, do not make changes.

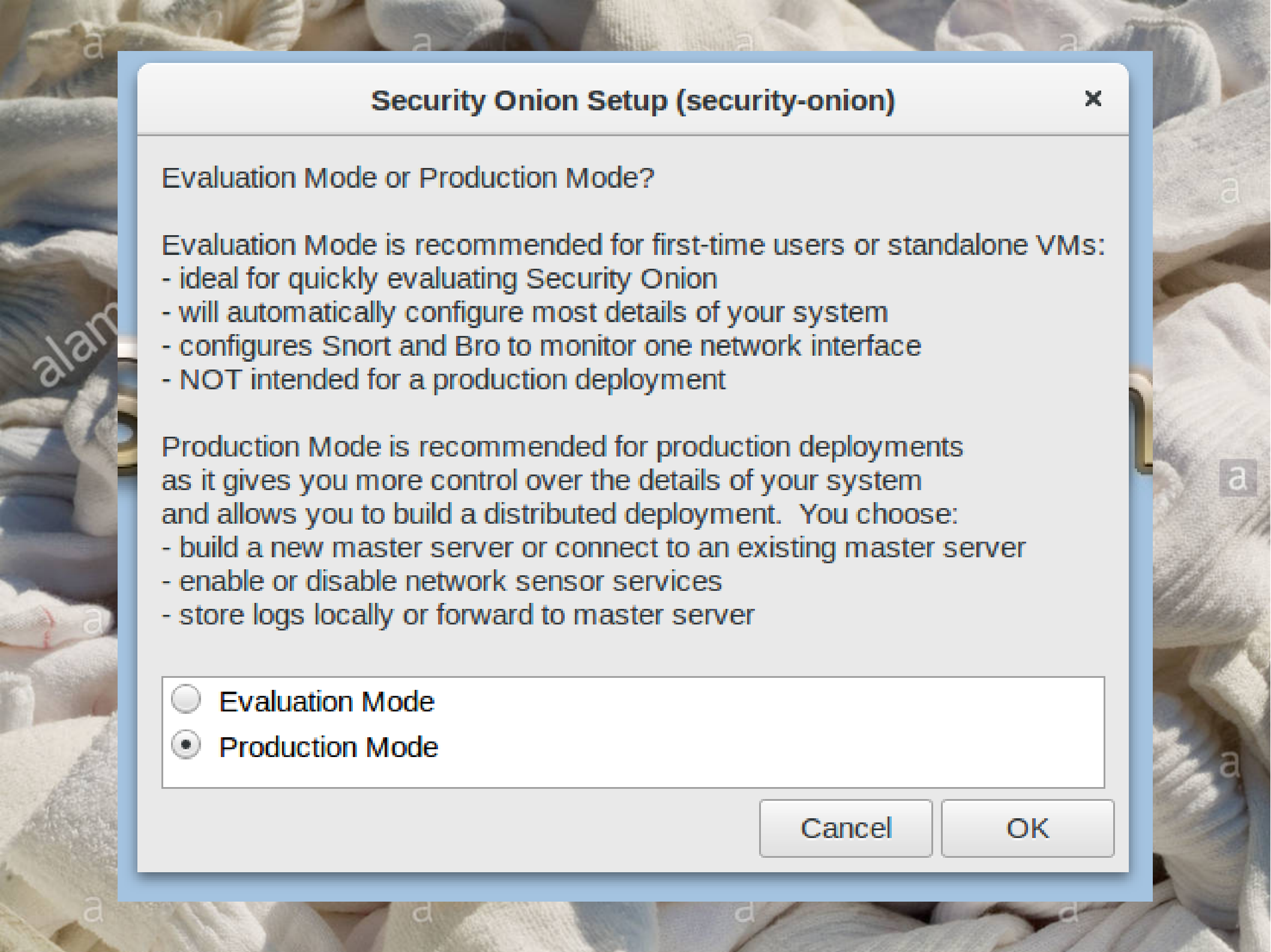
Yes, make changes!

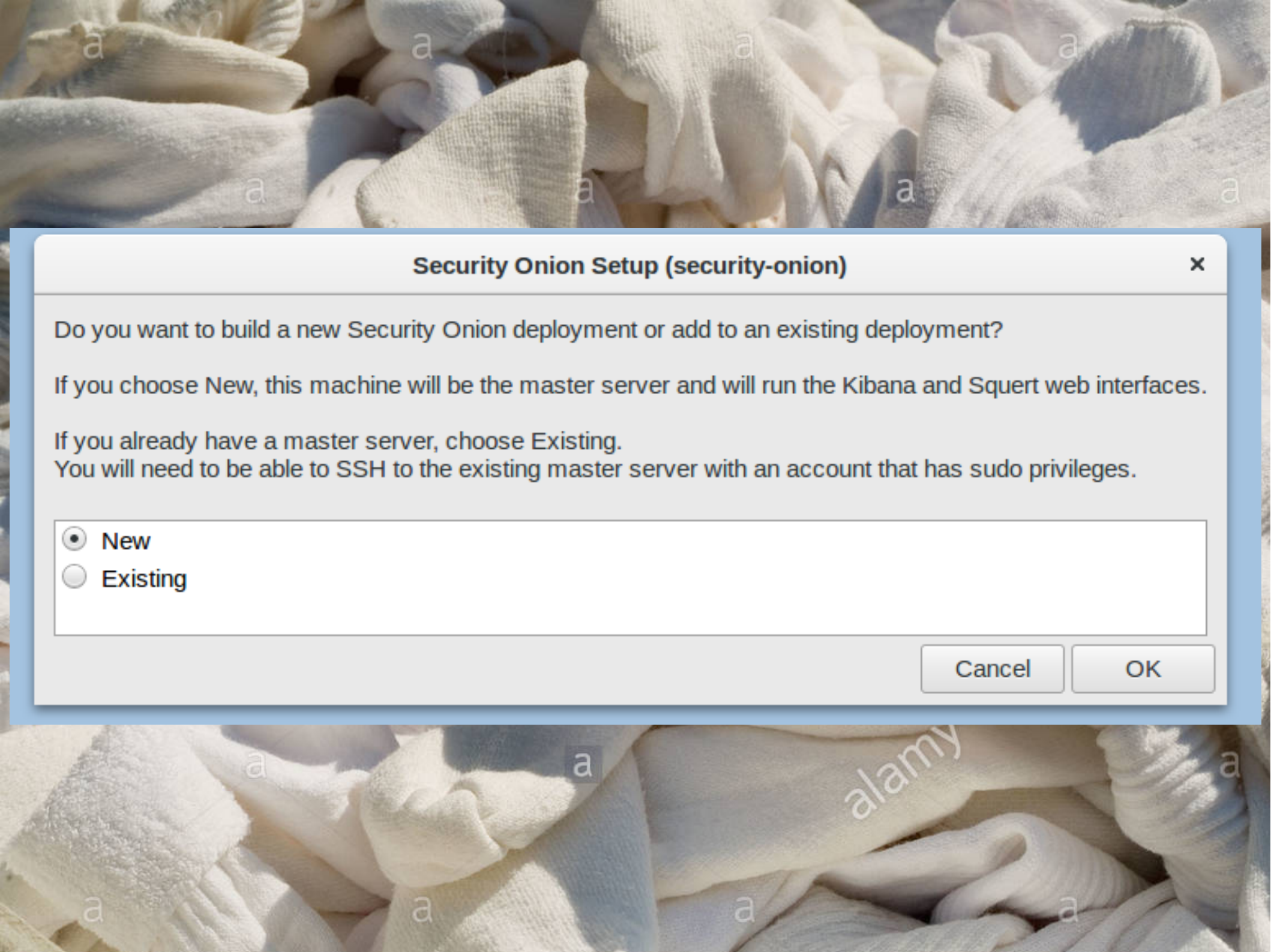

Security Onion Setup (security-onion)
Network configuration complete!
You'll need to reboot before continuing to the second phase of Setup.
If you need to manually modify any other network settings,
you can edit /etc/network/interfaces now before rebooting.
Would you like to reboot now?
No, do not reboot.
Yes, reboot!

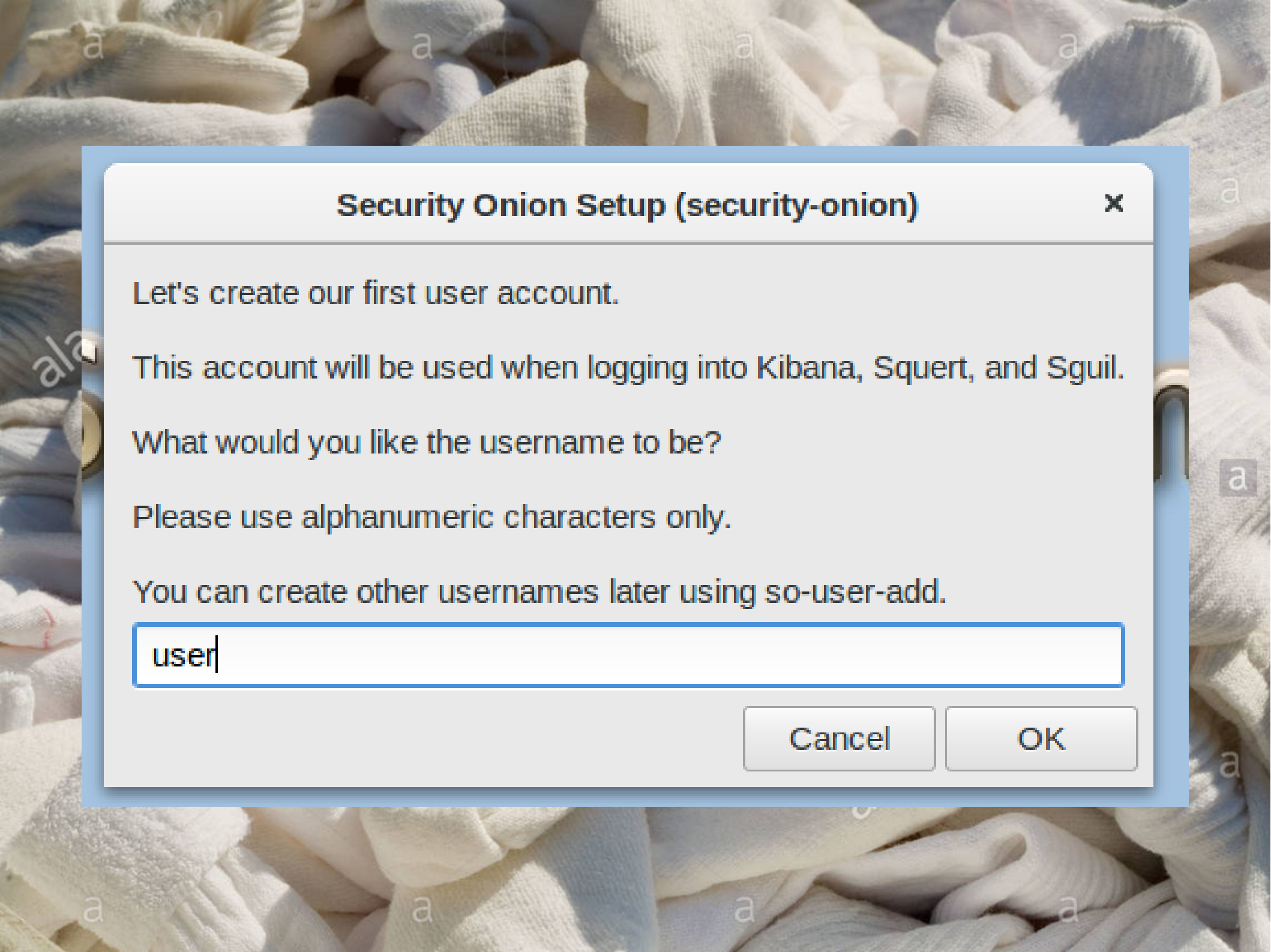

home
Setup
Trash

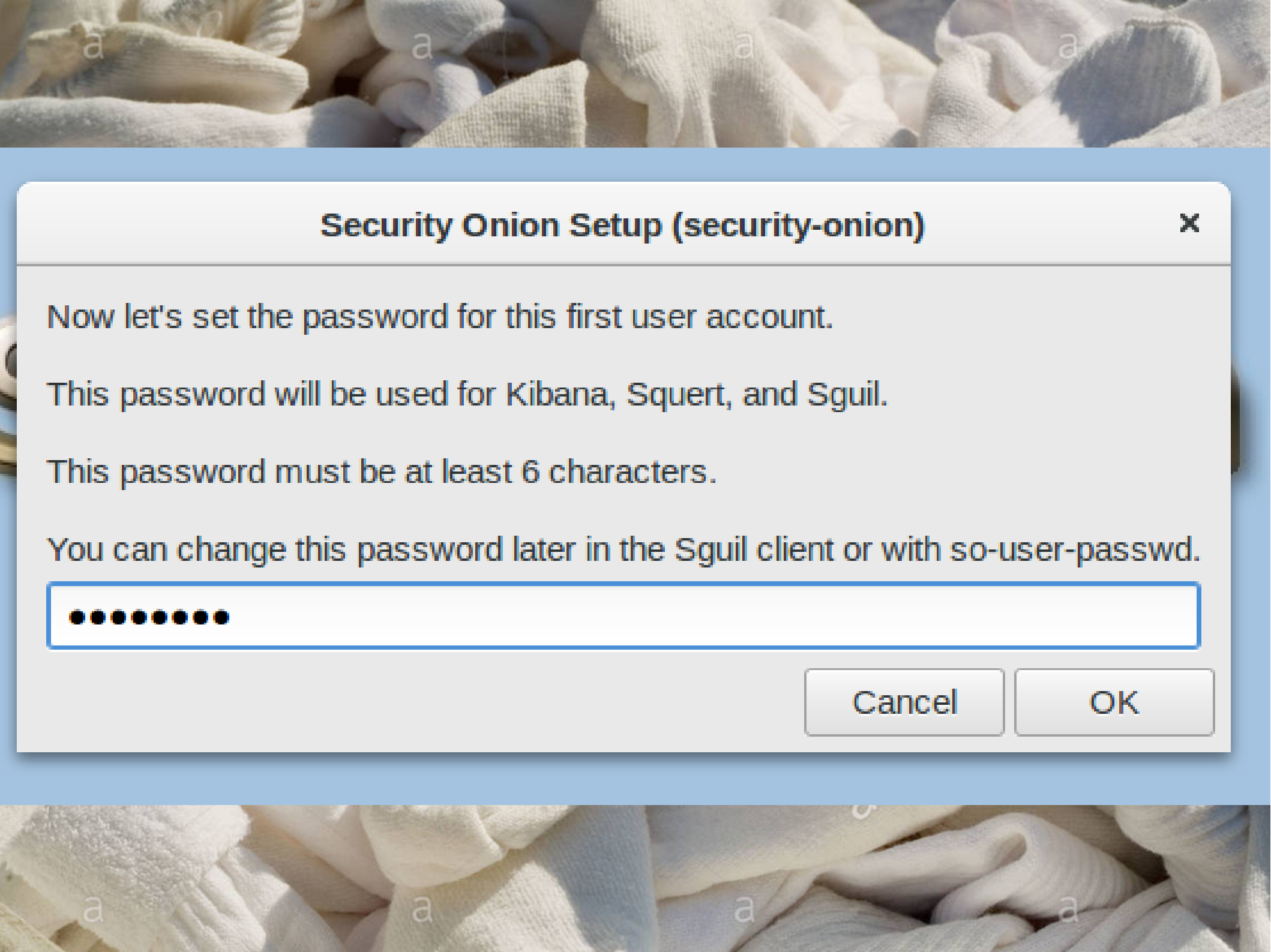

Security Onion Setup (security-onion)
Welcome to Security Onion Elastic Setup!
Elastic Setup will configure the following services:
Elasticsearch
Logstash
Kibana
Squert
Sguil
Bro
Snort/Suricata
netsniff-ng
Would you like to continue?
No, Quit.
Yes, Continue!

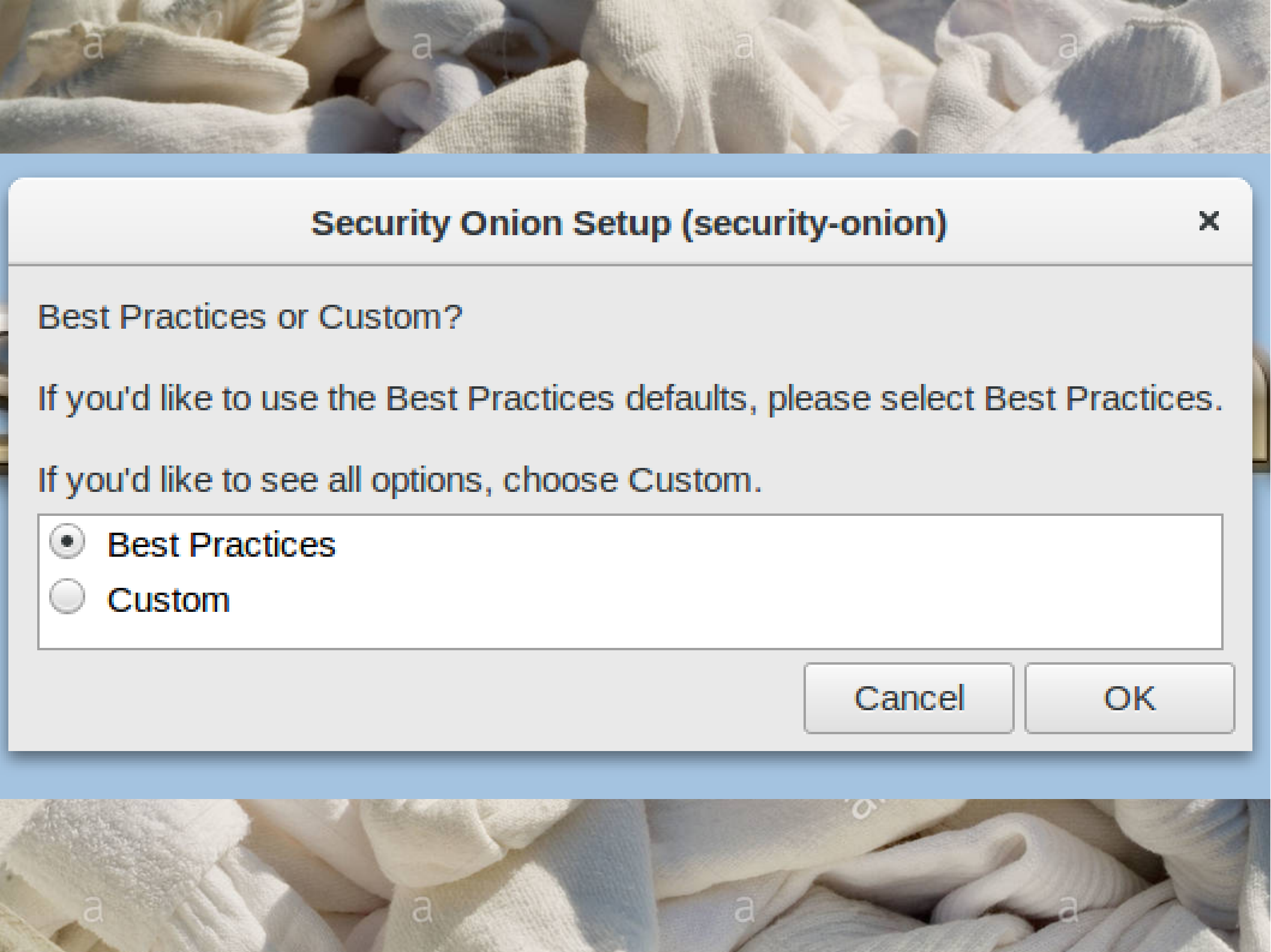

Security Onion Setup (security-onion)
It looks like /etc/network/interfaces has already been configured by this script.
Would you like to skip network configuration?
No, I need to re-configure /etc/network/interfaces.
Yes, skip network configuration!


Security Onion Setup (security-onion)
Evaluation Mode or Production Mode?
Evaluation Mode is recommended for first-time users or standalone VMs:
- ideal for quickly evaluating Security Onion
- will automatically configure most details of your system
- configures Snort and Bro to monitor one network interface
- NOT intended for a production deployment
Production Mode is recommended for production deployments
as it gives you more control over the details of your system
and allows you to build a distributed deployment. You choose:
- build a new master server or connect to an existing master server
- enable or disable network sensor services
- store logs locally or forward to master server
Evaluation Mode
Production Mode
Cancel
OK


Security Onion Setup (security-onion)
Do you want to build a new Security Onion deployment or add to an existing deployment?
If you choose New, this machine will be the master server and will run the Kibana and Squert web interfaces.
If you already have a master server, choose Existing.
You will need to be able to SSH to the existing master server with an account that has sudo privileges.
New
Existing
Cancel
OK


Security Onion Setup (security-onion)
Let's create our first user account.
This account will be used when logging into Kibana, Squert, and Sguil.
What would you like the username to be?
Please use alphanumeric characters only.
You can create other usernames later using so-user-add.
user
Cancel
OK


Security Onion Setup (security-onion)
Now let's set the password for this first user account.
This password will be used for Kibana, Squert, and Sguil.
This password must be at least 6 characters.
You can change this password later in the Sguil client or with so-user-passwd.
Cancel
OK


Security Onion Setup (security-onion)
Best Practices or Custom?
If you'd like to use the Best Practices defaults, please select Best Practices.
If you'd like to see all options, choose Custom.
Best Practices
Custom
Cancel
OK

Security Onion Setup (security-onion)

Which IDS ruleset would you like to use?

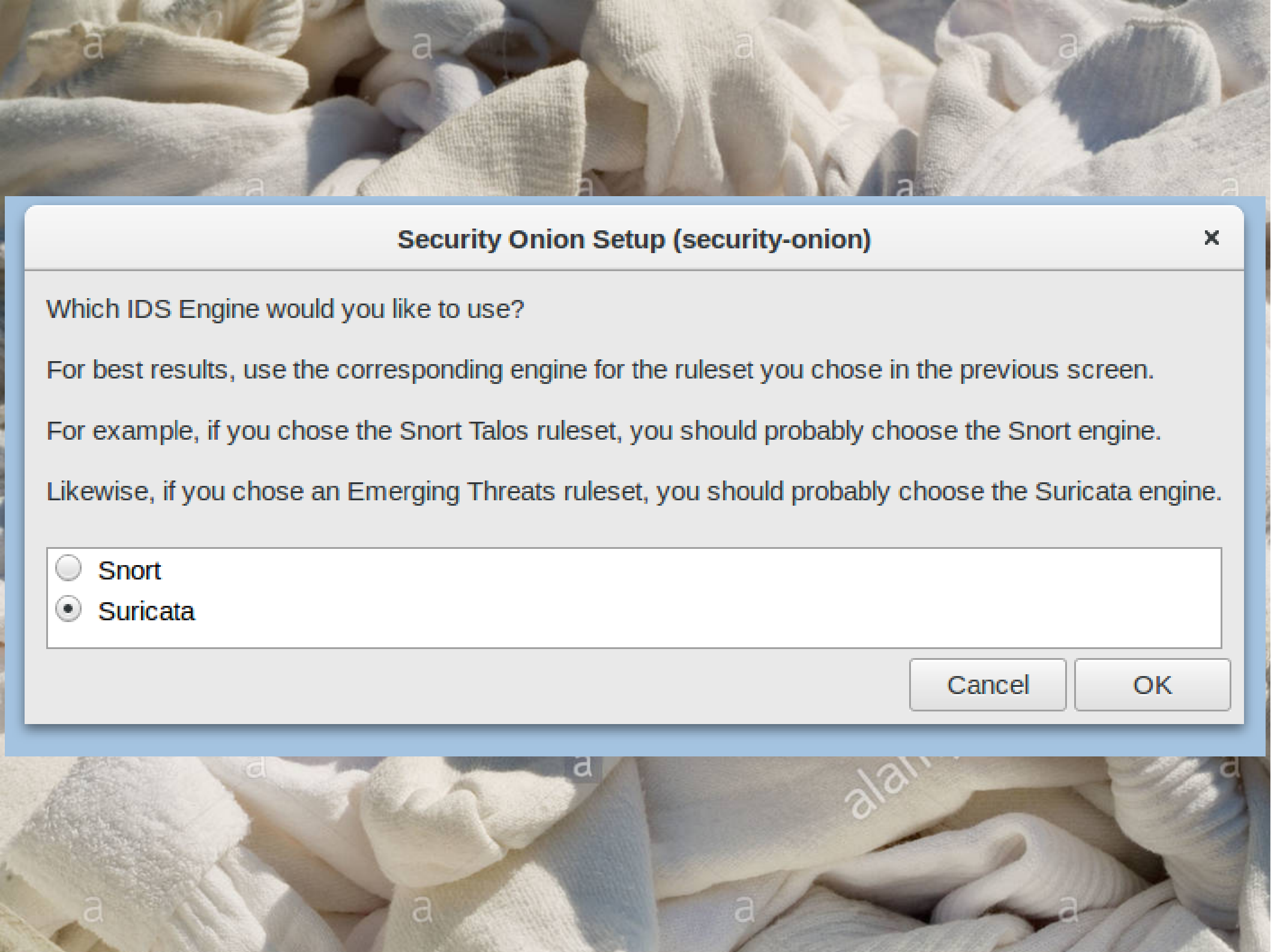
This master server is responsible for downloading the IDS ruleset from the Internet.

Sensors then pull a copy of this ruleset from the master server.

If you select a commercial ruleset, it is your responsibility to purchase enough licenses for all of your sensors in compliance with your vendor's policies.

(•) Emerging Threats Open	no oinkcode required
( ) Emerging Threats PRO	requires ETPRO oinkcode
( ) Snort Subscriber (Talos) ruleset and Emerging Threats NoGPL ruleset	requires Snort Subscriber oinkcode
( ) Snort Subscriber (Talos) ruleset only and set a Snort Subscriber policy	requires Snort Subscriber oinkcode

Cancel OK


Security Onion Setup (security-onion)
Which IDS Engine would you like to use?
For best results, use the corresponding engine for the ruleset you chose in the previous screen.
For example, if you chose the Snort Talos ruleset, you should probably choose the Snort engine.
Likewise, if you chose an Emerging Threats ruleset, you should probably choose the Suricata engine.
Snort
Suricata
Cancel
OK

Security Onion Setup (security-onion)

Network sensor services include:

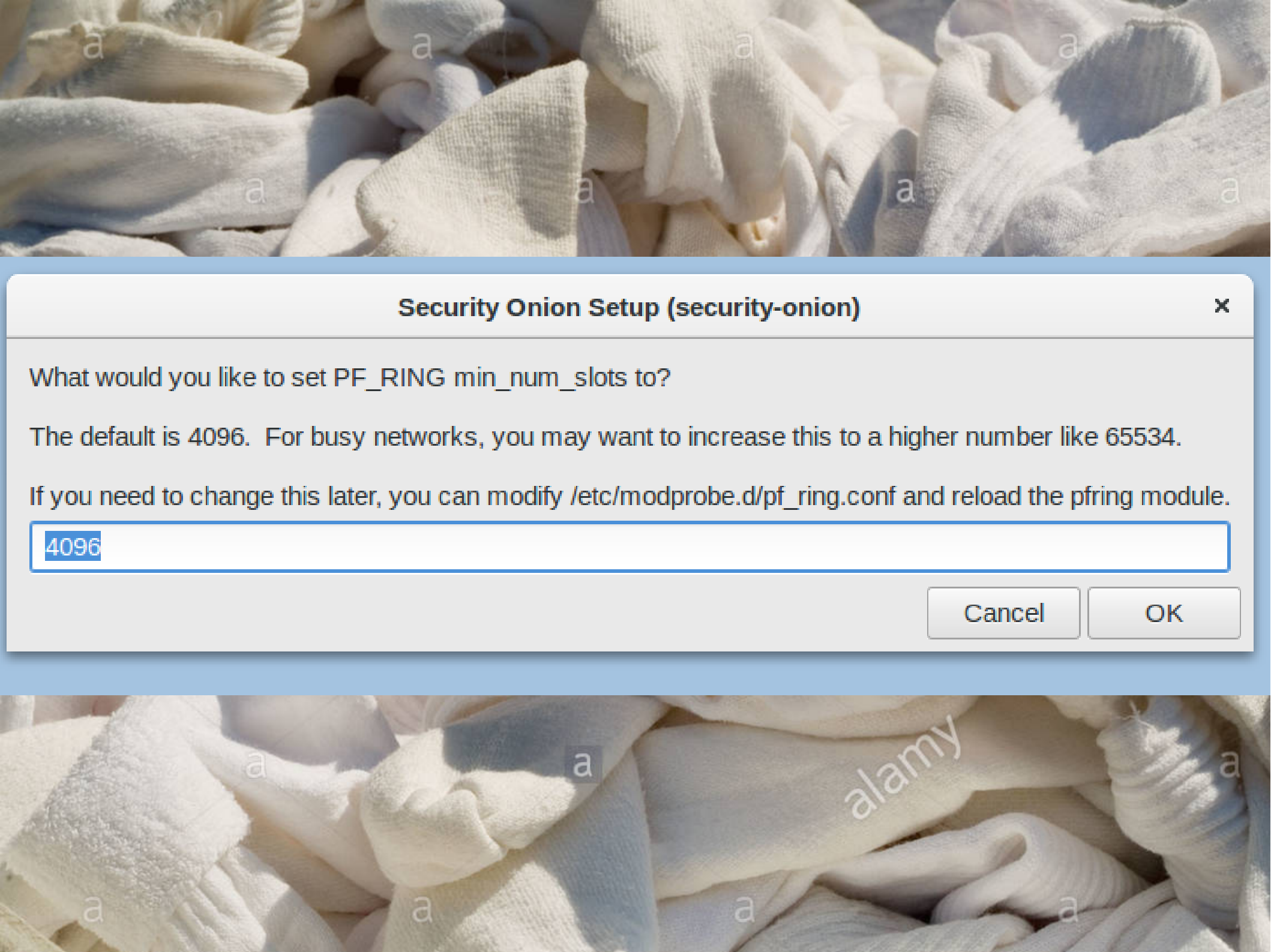
- Snort or Suricata for NIDS alerts
- Bro for protocol logging
- netsniff-ng for full packet capture

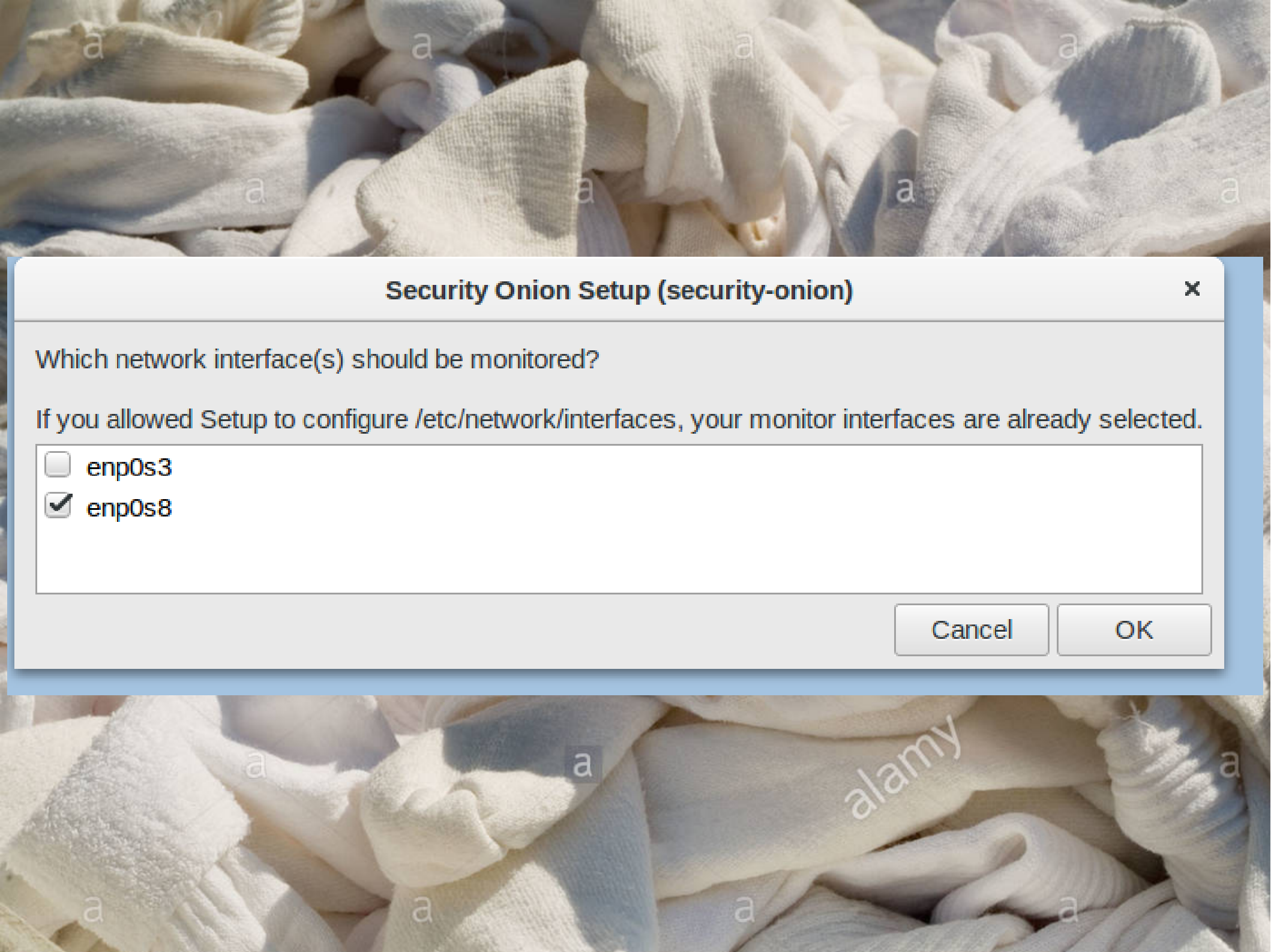
For best performance, we recommend disabling network sensor services on master servers.

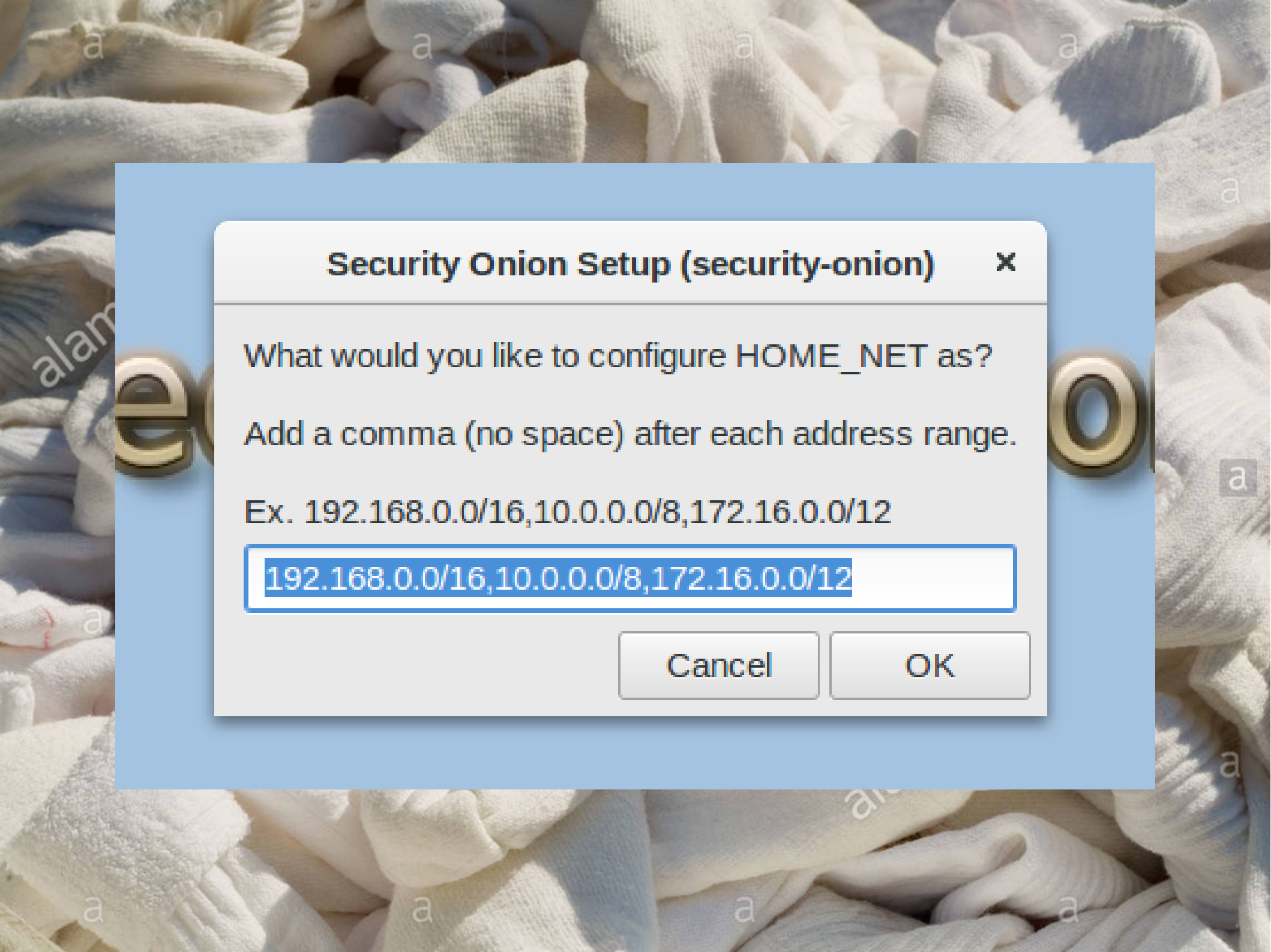
Would you like to enable or disable network sensor services?

- (•) Enable network sensor services
- ( ) Disable network sensor services

Cancel OK


Security Onion Setup (security-onion)
What would you like to set PF_RING min_num_slots to?
The default is 4096. For busy networks, you may want to increase this to a higher number like 65534.
If you need to change this later, you can modify /etc/modprobe.d/pf_ring.conf and reload the pfring module.
4096
Cancel
OK


Security Onion Setup (security-onion)
Which network interface(s) should be monitored?
If you allowed Setup to configure /etc/network/interfaces, your monitor interfaces are already selected.
enp0s3
enp0s8
Cancel
OK


Security Onion Setup (security-onion)
What would you like to configure HOME_NET as?
Add a comma (no space) after each address range.
Ex. 192.168.0.0/16,10.0.0.0/8,172.16.0.0/12
192.168.0.0/16,10.0.0.0/8,172.16.0.0/12
Cancel
OK

Security Onion Setup (security-onion)

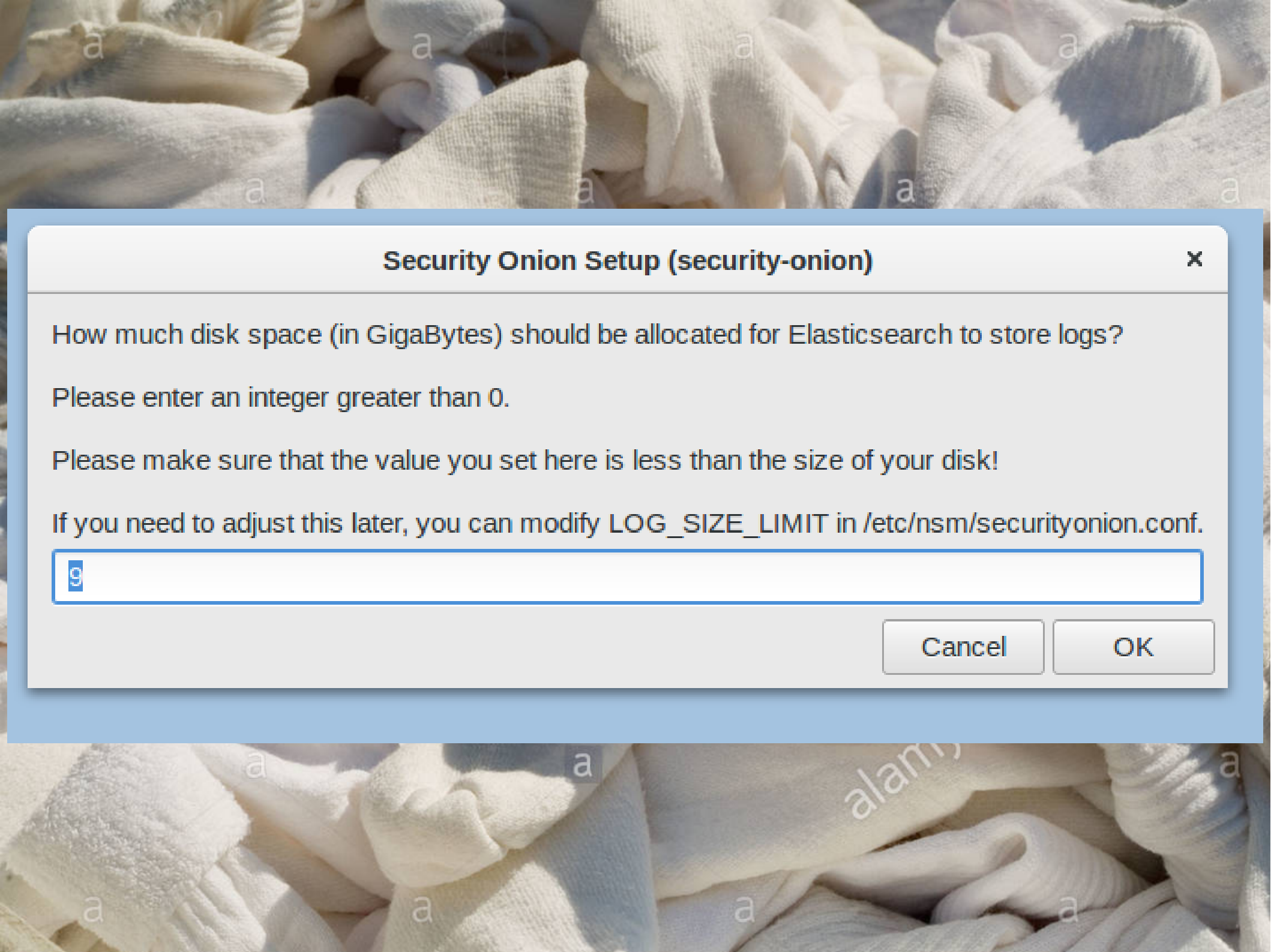
By default, the master server stores logs in its own local Elasticsearch database via a local Logstash instance.

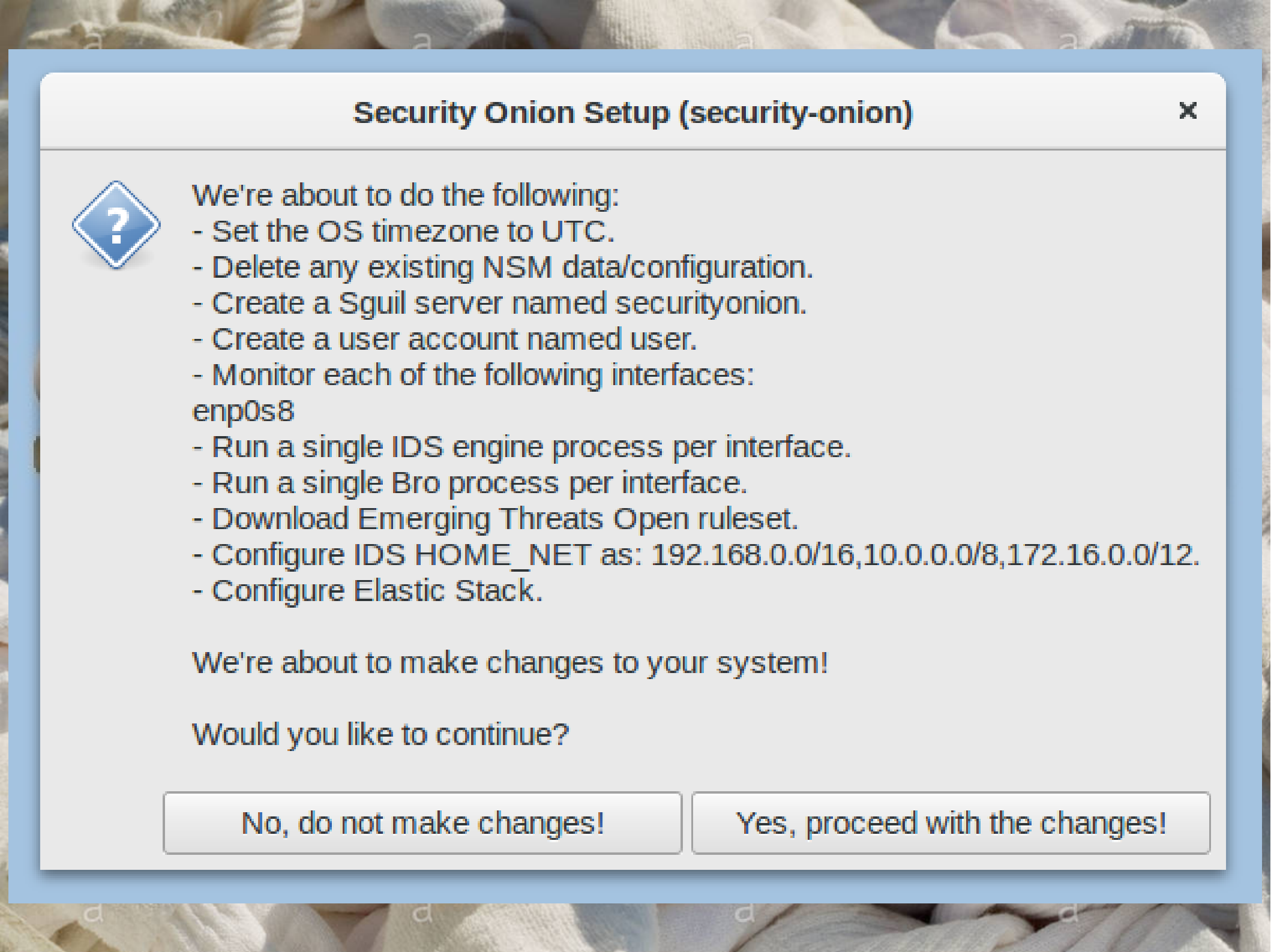
If you want to forward logs from multiple nodes to this master server, then you may overwhelm those single instances of Logstash and El
You may want to consider load balancing these forwarded logs to additional storage nodes.

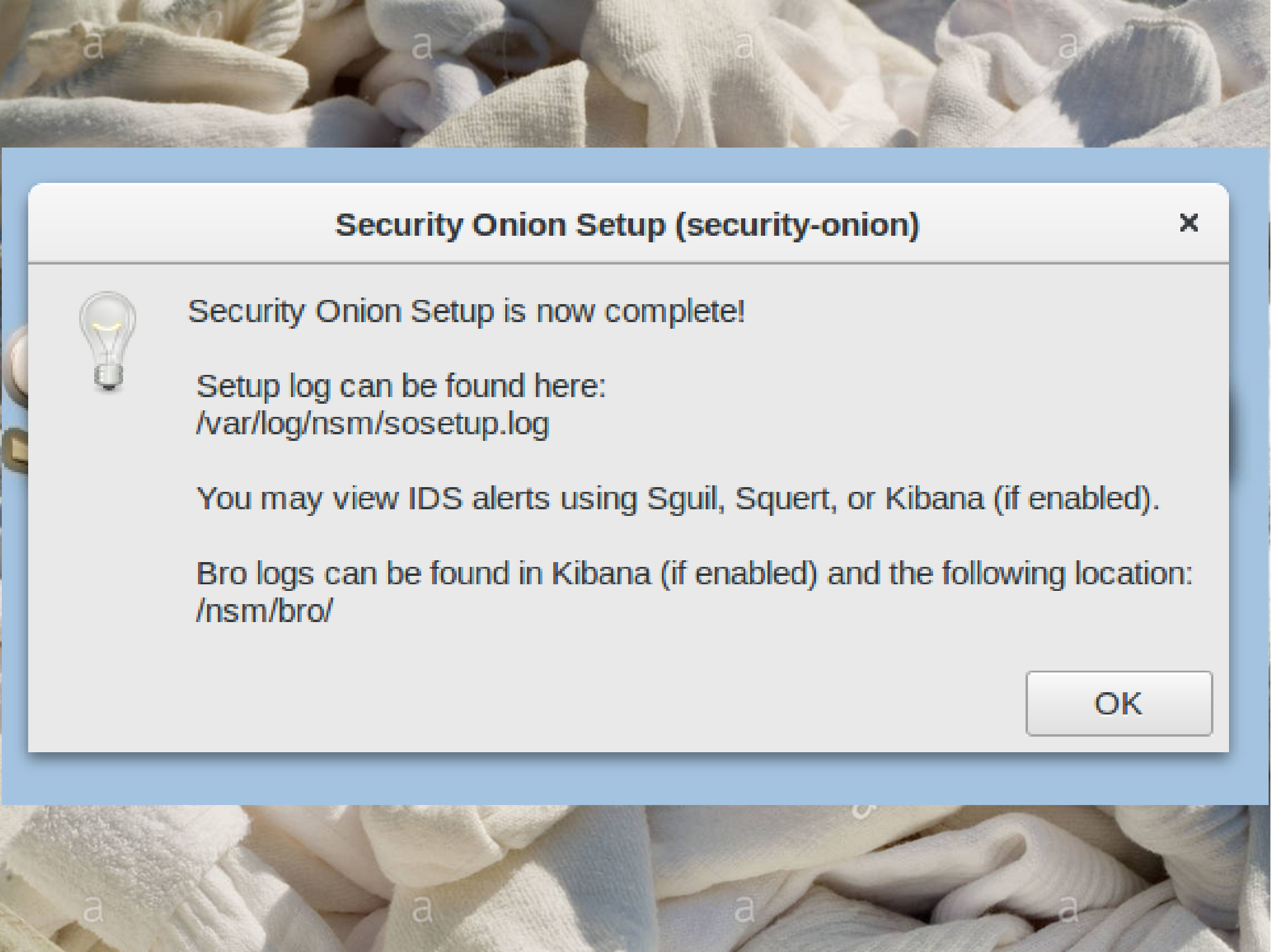
Would you like to store logs locally on security-onion?

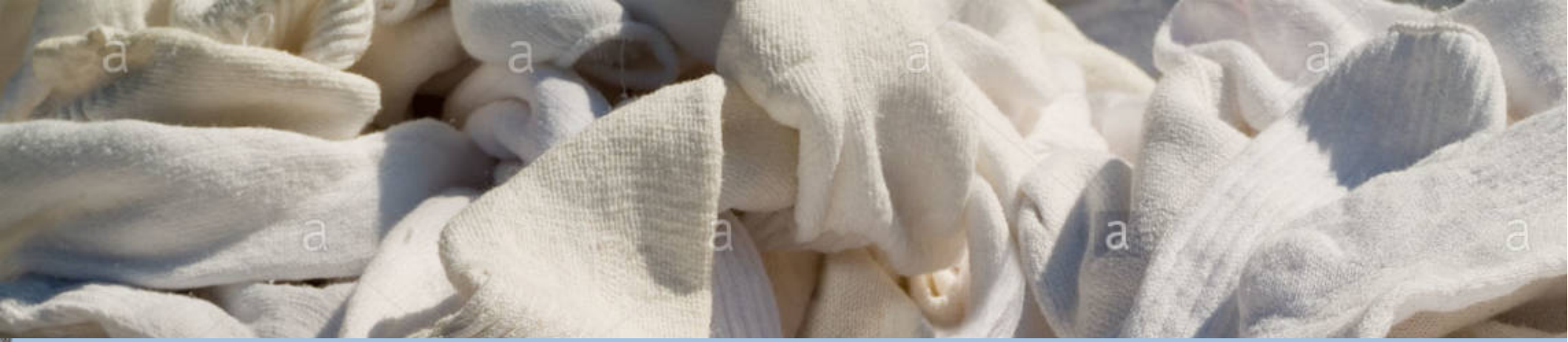
No, I will add storage nodes for load balancing.

Yes, store logs locally.


Security Onion Setup (security-onion)
How much disk space (in GigaBytes) should be allocated for Elasticsearch to store logs?
Please enter an integer greater than 0.
Please make sure that the value you set here is less than the size of your disk!
If you need to adjust this later, you can modify LOG_SIZE_LIMIT in /etc/nsm/securityonion.conf.
9
Cancel
OK


Security Onion Setup (security-onion)
We're about to do the following:
- Set the OS timezone to UTC.
- Delete any existing NSM data/configuration.
- Create a Sguil server named securityonion.
- Create a user account named user.
- Monitor each of the following interfaces:
enp0s8
- Run a single IDS engine process per interface.
- Run a single Bro process per interface.
- Download Emerging Threats Open ruleset.
- Configure IDS HOME_NET as: 192.168.0.0/16,10.0.0.0/8,172.16.0.0/12.
- Configure Elastic Stack.
We're about to make changes to your system!
Would you like to continue?
No, do not make changes!
Yes, proceed with the changes!


Security Onion Setup (security-onion)
Security Onion Setup is now complete!
Setup log can be found here:
/var/log/nsm/sosetup.log
You may view IDS alerts using Sguil, Squert, or Kibana (if enabled).
Bro logs can be found in Kibana (if enabled) and the following location:
/nsm/bro/
OK



Security Onion Setup (security-onion)

You can check the status of your running services with the sostat utilites:

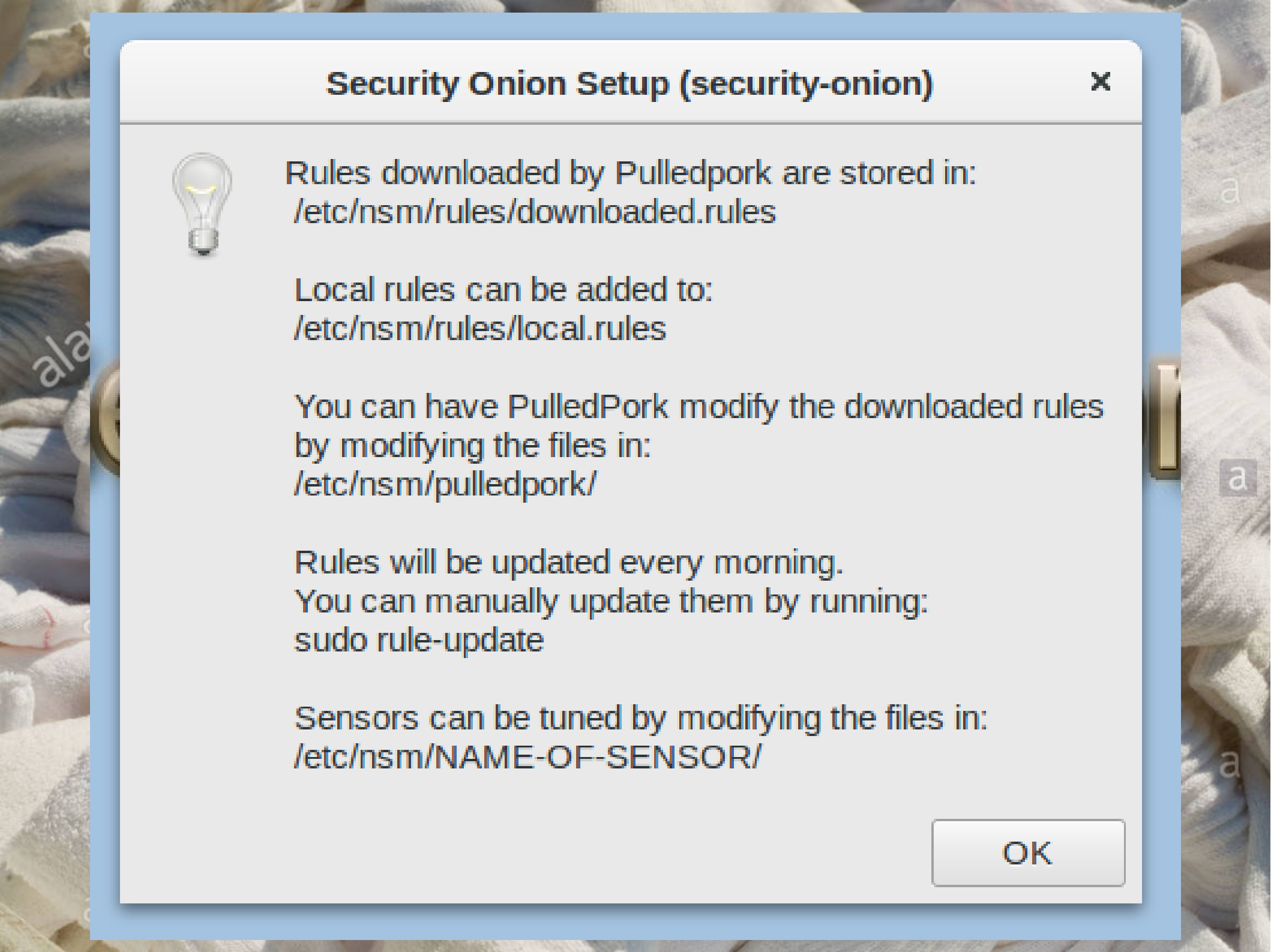
'sudo sostat' will give you DETAILED information about your service status.

'sudo sostat-quick' will give you a guided tour of the sostat output.

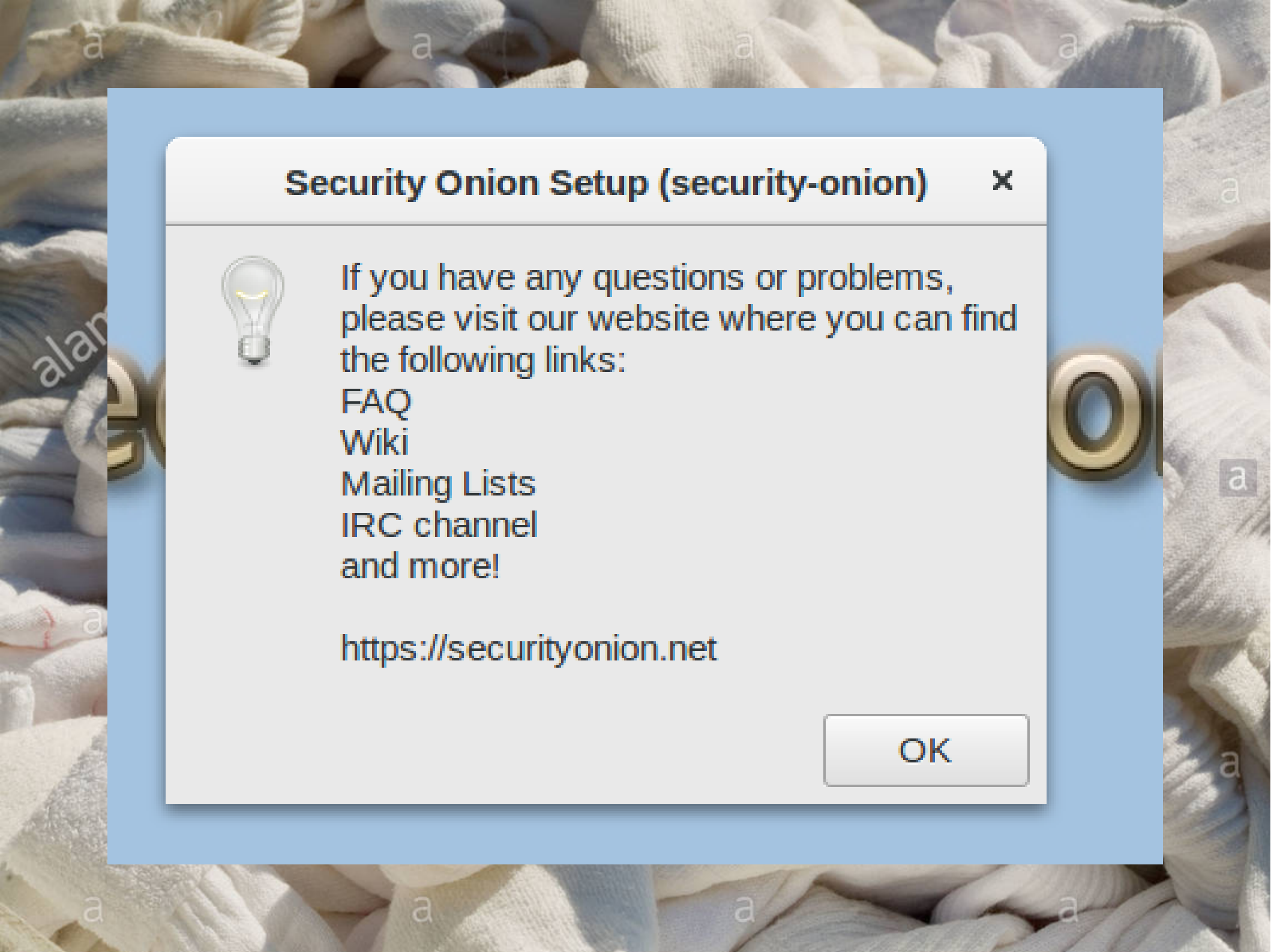
'sudo sostat-redacted' will give you REDACTED information to share with our mailing list if you have questions.

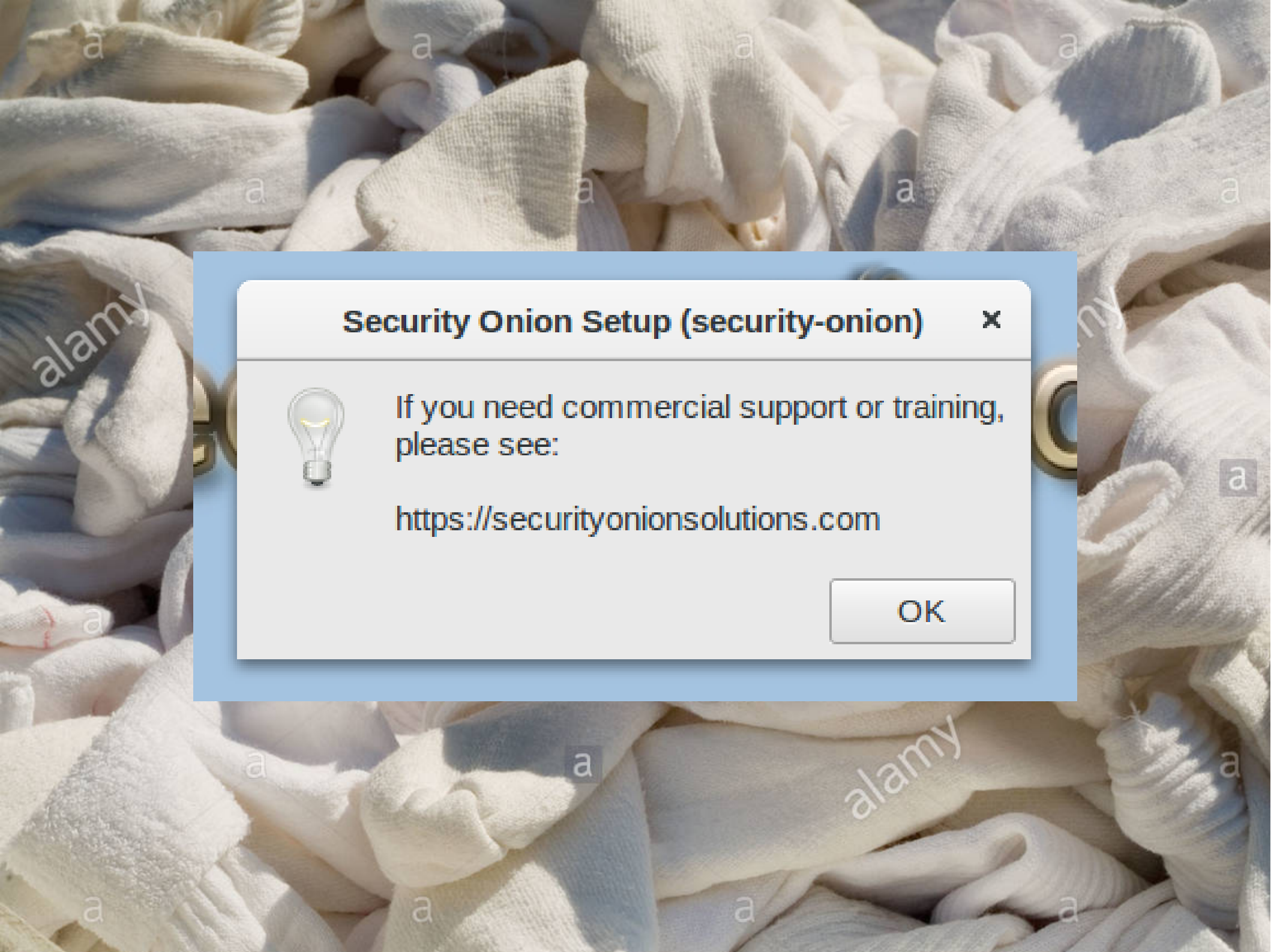
OK

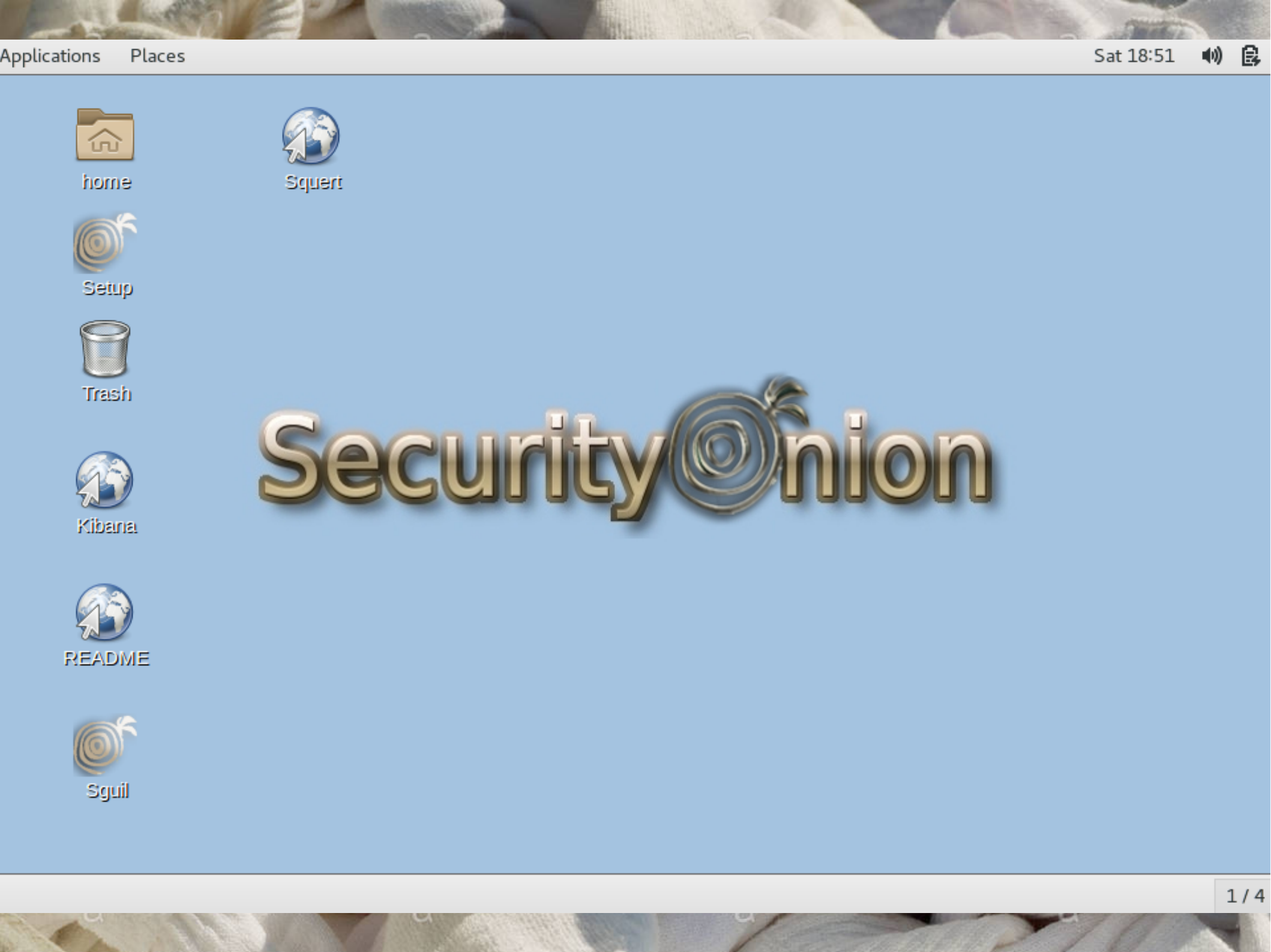
ME


Security Onion Setup (security-onion)
Rules downloaded by Pulledpork are stored in:
/etc/nsm/rules/downloaded.rules
Local rules can be added to:
/etc/nsm/rules/local.rules
You can have PulledPork modify the downloaded rules by modifying the files in:
/etc/nsm/pulledpork/
Rules will be updated every morning.
You can manually update them by running:
sudo rule-update
Sensors can be tuned by modifying the files in:
/etc/nsm/NAME-OF-SENSOR/
OK

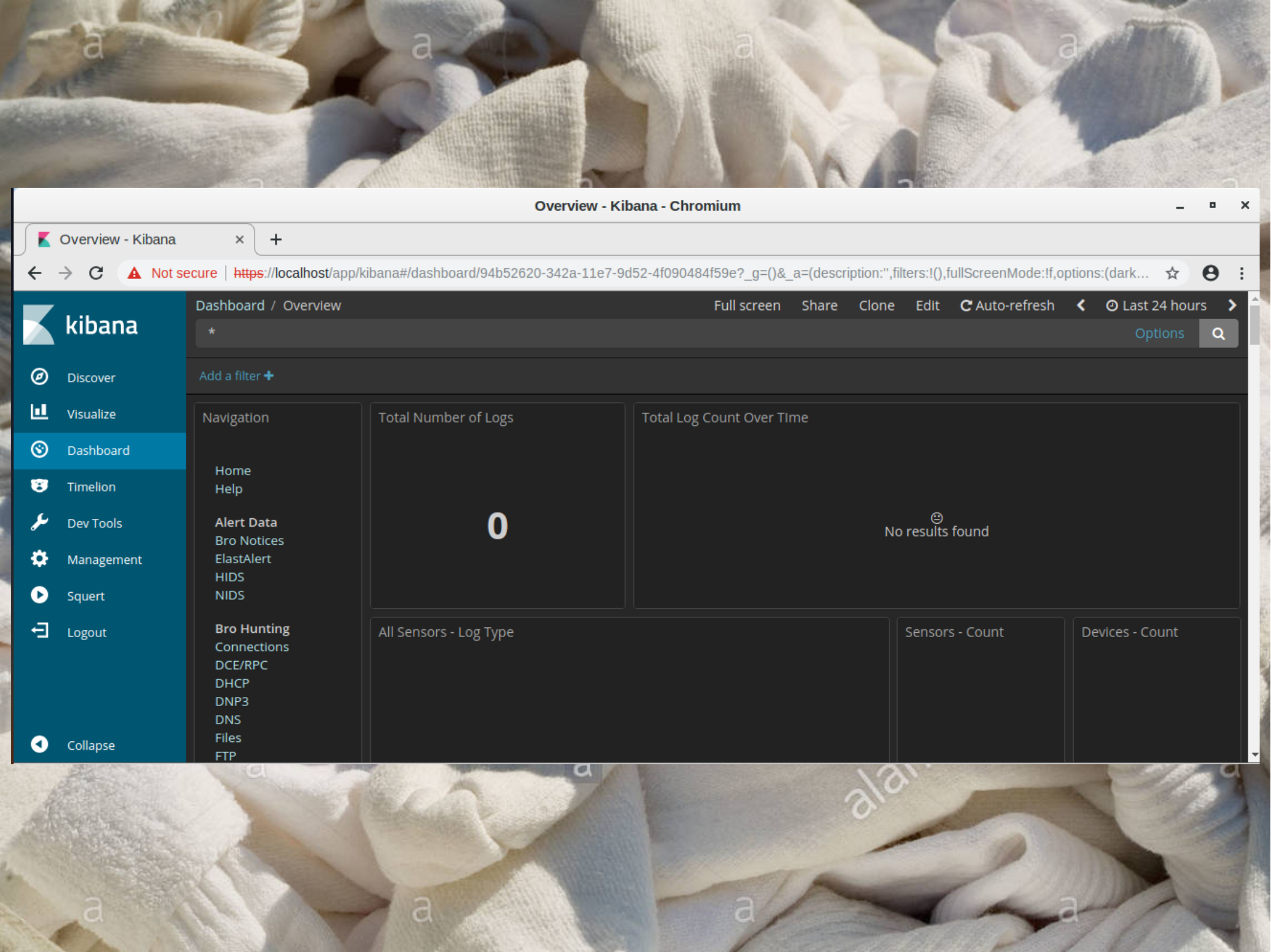

Security Onion Setup (security-onion)
Please note that the local ufw firewall
has been locked down to only allow connections
to port 22. If you need to connect over any
other port, then run "sudo so-allow".
OK

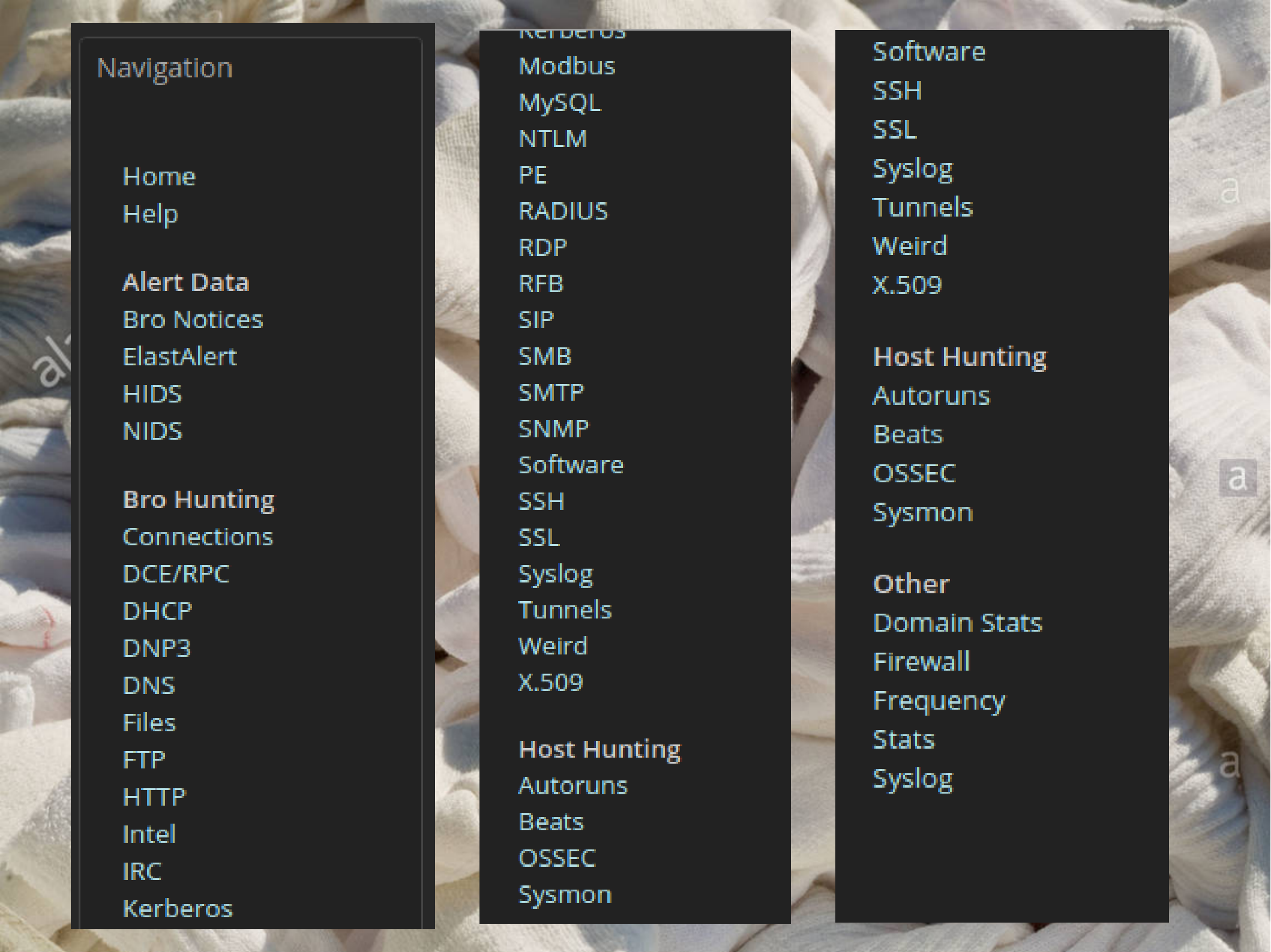

Security Onion Setup (security-onion)
If you have any questions or problems, please visit our website where you can find the following links:
FAQ
Wiki
Mailing Lists
IRC channel
and more!
https://securityonion.net
OK


Security Onion Setup (security-onion)
If you need commercial support or training, please see:
https://securityonionsolutions.com
OK


Applications
Places
Sat 18:51
home
Squert
Setup
Trash
Kibana
README
Sguil
Security Onion
1 / 4


Kibana


Overview - Kibana - Chromium
Overview - Kibana
Not secure
https://localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=()&_a=(description:'',filters:!(),fullScreenMode:!f,options:(dark...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Dashboard / Overview
Full screen
Share
Clone
Edit
Auto-refresh
Last 24 hours
*
Options
Add a filter +
Navigation
Home
Help
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS
Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
Total Number of Logs
0
Total Log Count Over TIme
No results found
All Sensors - Log Type
Sensors - Count
Devices - Count


Navigation
Home
Help
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS
Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
Weird
X.509
Host Hunting
Autoruns
Beats
OSSEC
Sysmon
Software
SSH
SSL
Syslog
Tunnels
Weird
X.509
Host Hunting
Autoruns
Beats
OSSEC
Sysmon
Other
Domain Stats
Firewall
Frequency
Stats
Syslog

kibana

0 hits

New Save Open Share Auto-refresh Last 24 hours

Search... (e.g. status:200 AND extension:PHP) Options

Add a filter +

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

:logstash-

Selected fields

? _source

Available fields

No results match your search criteria

Expand your time range

One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or there may not be any data at all in the currently selected time range. You can try opening the time picker and changing the time range to one which contains data.

Refine your query

The search bar at the top uses Elasticsearch's support for Lucene Query String syntax. Here are some examples of how you can search for web server logs that have been parsed into a few fields.

Find requests that contain the number 200, in any field	`200`
Find 200 in the status field	`status:200`
Find all status codes between 400-499	`status:[400 TO 499]`
Find status codes 400-499 with the extension php	`status:[400 TO 499] AND extension:PHP`
Find status codes 400-499 with the extension php or html	`status:[400 TO 499] AND (extension:php OR extension:html)`

kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

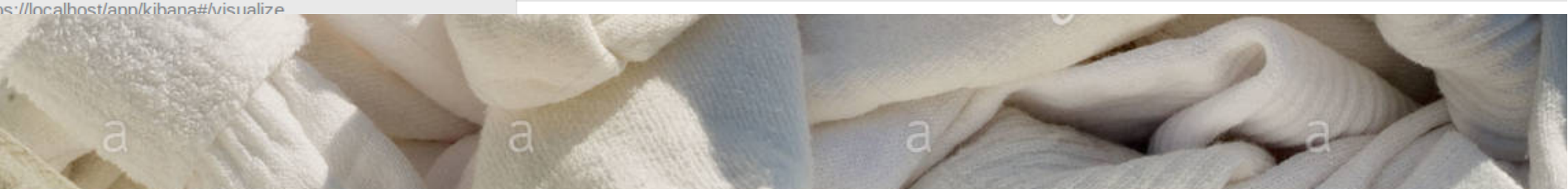
Visualize

Search...

1–20 of 386

Title	Type
All Sensors - Log Type	Data Table
Autoruns - Category	Vertical Bar
Autoruns - Company	Tag Cloud
Autoruns - Entry	Data Table
Autoruns - Hostname	Data Table
Autoruns - Hostname (Tag Cloud)	Tag Cloud
Autoruns - Launch String	Data Table
Autoruns - Log Count	42 Metric
Autoruns - Log Count Over Time	Line
Autoruns - Profile	Data Table
Autoruns - Signer	Data Table
Beats - Computer Names	Data Table

https://localhost/app/kibana#/visualize



kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

Collapse

New Add Save Delete Open Options Help Auto-refresh Last 24 hours

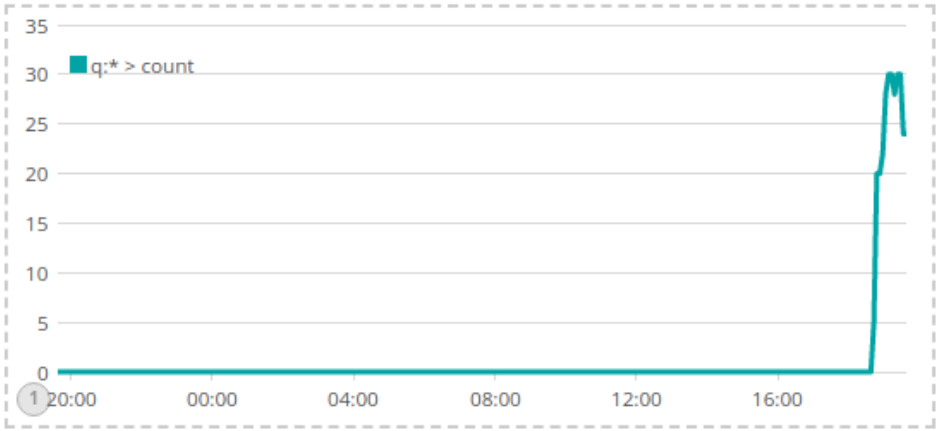
Welcome to **Timelion**!
Timelion is the clawing, gnashing, zebra killing, pluggable time series interface for *everything*. If your datastore can produce a time series, then you have all of the awesome power of Timelion at your disposal. Timelion lets you compare, combine, and combobulate datasets across multiple datasources with one easy-to-master expression syntax. This tutorial focuses on Elasticsearch, but you'll quickly discover that what you learn here applies to any datasource Timelion supports.
Ready to get started? Click **Next**. Want to skip the tutorial and view the docs? Jump to the function reference.

Don't show this again

Ne

.es(*)

auto




Squil

SGUIL-0.9.0 - Connected To localhost

ile Query Reports Sound: Off ServerName: localhost UserName: user UserID: 2 2018-10-27 19:46:34 GM

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	security-o...	1.1	2018-10-27 18:47:48	0.0.0.0		0.0.0.0			[OSSEC] File added to the system.
RT	1	security-o...	1.2	2018-10-27 18:48:10	0.0.0.0		0.0.0.0			[OSSEC] Integrity checksum changed.
RT	7	security-o...	1.3	2018-10-27 18:48:16	0.0.0.0		0.0.0.0			[OSSEC] New group added to the system
RT	7	security-o...	1.4	2018-10-27 18:48:16	0.0.0.0		0.0.0.0			[OSSEC] New user added to the system
RT	3	security-o...	1.17	2018-10-27 18:53:16	0.0.0.0		0.0.0.0			[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
RT	5	security-o...	1.18	2018-10-27 18:56:56	0.0.0.0		0.0.0.0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.c...
RT	2	security-o...	1.23	2018-10-27 19:34:22	0.0.0.0		0.0.0.0			[OSSEC] Web server 400 error code.
RT	43	security-o...	3.1	2018-10-27 19:41:19						SURICATA zero length padN option

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

☑ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ○ None ○ Src IP ◉ Dst IP

ERROR: Could not connect to whois.arin.net

☑ Show Packet Data ☑ Show Rule

alert ipv6 any any -> any any (msg:"SURICATA zero length padN option"; decode-event:ipv6.zero_len_padn;

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	0.0.0.0	0.0.0.0	0	0	0	0	0	0	0	0	0

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum

DATA	None .	None .

Search Packet Payload ○ Hex ◉ Text ☐ NoCase


Squert

EVENTS | SUMMARY | VIEWS

Filter

INTERVAL: 2018-10-27 00:00:00 -> 2018-10-27 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 100.0%

TOGGLE

queue only	on
grouping	on

SUMMARY

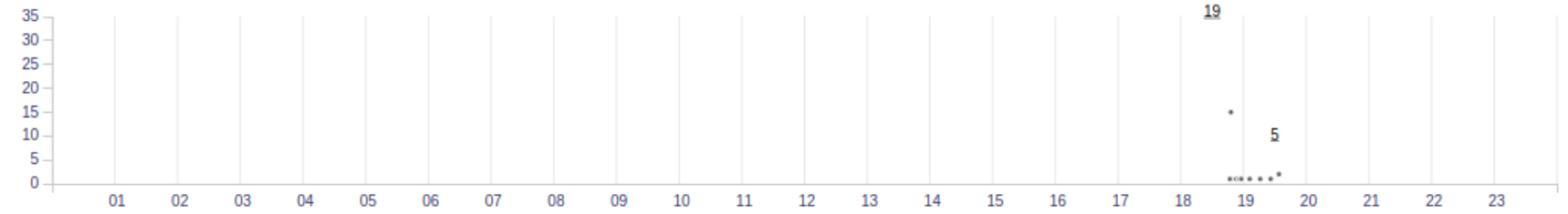
queued events	24
total events	24
total signatures	7

PRIORITY

high	-
medium	-
low	-
other	24 (100.0%)

CLASSIFICATION

compromised L1	-
compromised L2	-
attempted access	-
denial of service	-
policy violation	-
reconnaissance	-
malicious	-
no action req'd.	-
escalated event	-



QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
3	7	1	1	19:34:58	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0	**12.500%**
1	5	1	1	19:34:22	[OSSEC] Web server 400 error code.	31101	0	**4.167%**
4	7	1	1	19:26:57	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	**16.667%**
7	8	1	1	18:48:16	[OSSEC] New group added to the system	5901	0	**29.167%**
7	8	1	1	18:48:16	[OSSEC] New user added to the system	5902	0	**29.167%**
1	7	1	1	18:48:10	[OSSEC] Integrity checksum changed.	550	0	**4.167%**
1	5	1	1	18:47:48	[OSSEC] File added to the system.	554	0	**4.167%**

QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
3	7	1	1		19:34:58	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0	**12.500%**

Generator ID 10001. OSSEC rules can be found in /var/ossec/rules/.

file: **n/a:n/a**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
3		2018-10-27 19:34:58	0.0.0.0	-	*unknown (-)*	0.0.0.0	-	*unknown (-)*

	ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
	RT	2018-10-27 19:34:58	~~1.24~~	0.0.0.0	-	0.0.0.0	-	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
	RT	2018-10-27 18:58:58	~~1.19~~	0.0.0.0	-	0.0.0.0	-	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
	RT	2018-10-27 18:53:16	~~1.17~~	0.0.0.0	-	0.0.0.0	-	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).

1	5	1	1		19:34:22	[OSSEC] Web server 400 error code.	31101	0	4.167%
4	7	1	1		19:26:57	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please	111112	0	16.667%

EVENTS | SUMMARY | VIEWS

Filter

INTERVAL: 2018-10-27 00:00:00 -> 2018-10-27 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY:

TOP SIGNATURES (25 events)

viewing **7** of **7** results

COUNT	%TOTAL	#SRC	#DST	SIGNATURE	ID
7	**28.00%**	**1**	**1**	[OSSEC] New group added to the system	5901
7	**28.00%**	**1**	**1**	[OSSEC] New user added to the system	5902
5	**20.00%**	**1**	**1**	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112
3	**12.00%**	**1**	**1**	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533
1	**4.00%**	**1**	**1**	[OSSEC] File added to the system.	554
1	**4.00%**	**1**	**1**	[OSSEC] Web server 400 error code.	31101
1	**4.00%**	**1**	**1**	[OSSEC] Integrity checksum changed.	550

TOP SOURCE IPS

viewing **1** of **1** results

COUNT	%TOTAL	#SIG	#DST	IP	COUNTRY
25	**100.00%**	**7**	**1**	0.0.0.0	- (-)

TOP DESTINATION IPS

viewing **1** of **1** results

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
25	**100.00%**	**7**	**1**	0.0.0.0	- (-)

TOP SOURCE COUNTRIES

viewing **0** of **0** results

COUNT	%TOTAL	#SIG	#DST	COUNTRY	#IP
No result.					

TOP DESTINATION COUNTRIES

viewing **0** of **0** results

COUNT	%TOTAL	#SIG	#SRC	COUNTRY	#IP
No result.					

TOP SOURCE PORTS

TOP DESTINATION PORTS

EVENTS SUMMARY VIEWS

Filter

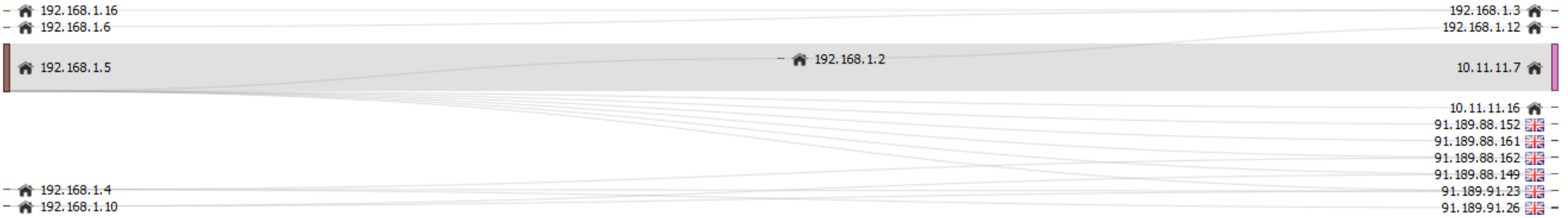
< 2017 Jan Feb Mar Apr May Jun Jul Aug Sep **Oct** Nov Dec 2019 >

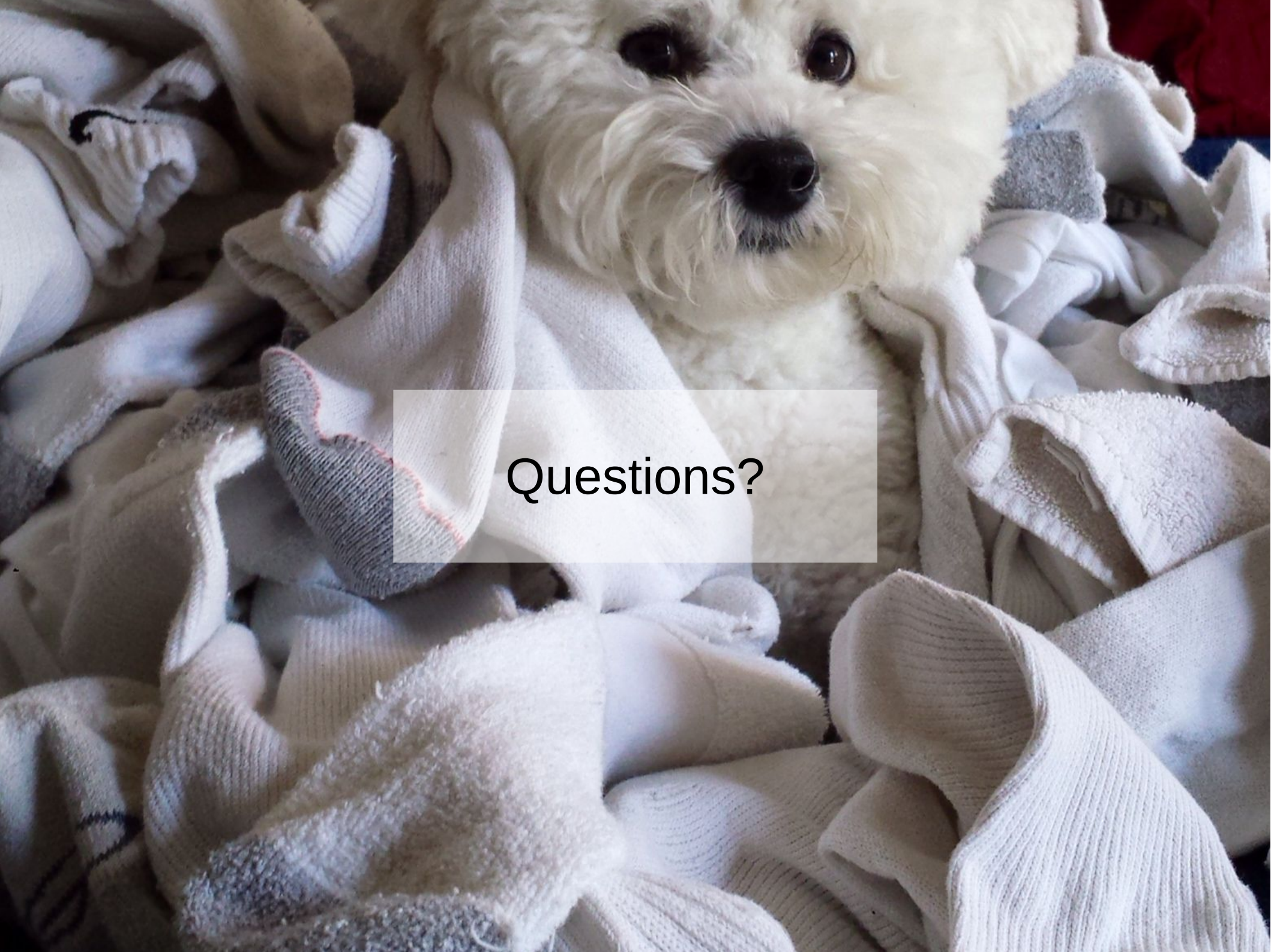
on01 Tue02 Wed03 Thu04 Fri05 **Sat06** **Sun07** Mon08 Tue09 Wed10 Thu11 Fri12 **Sat13** **Sun14** Mon15 Tue16 Wed17 Thu18 Fri19 **Sat20** **Sun21** **Mon22** Tue23 Wed24 Thu25 Fri26 **Sat27** **Sun28** Mon29 Tue30 Wed31

0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00

INTERVAL: 2018-10-22 00:00:00 -> 2018-10-22 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY:

view: IP SOURCE COUNTRY DESTINATION COUNTRY type: SANKEY DIAGRAM




Questions?