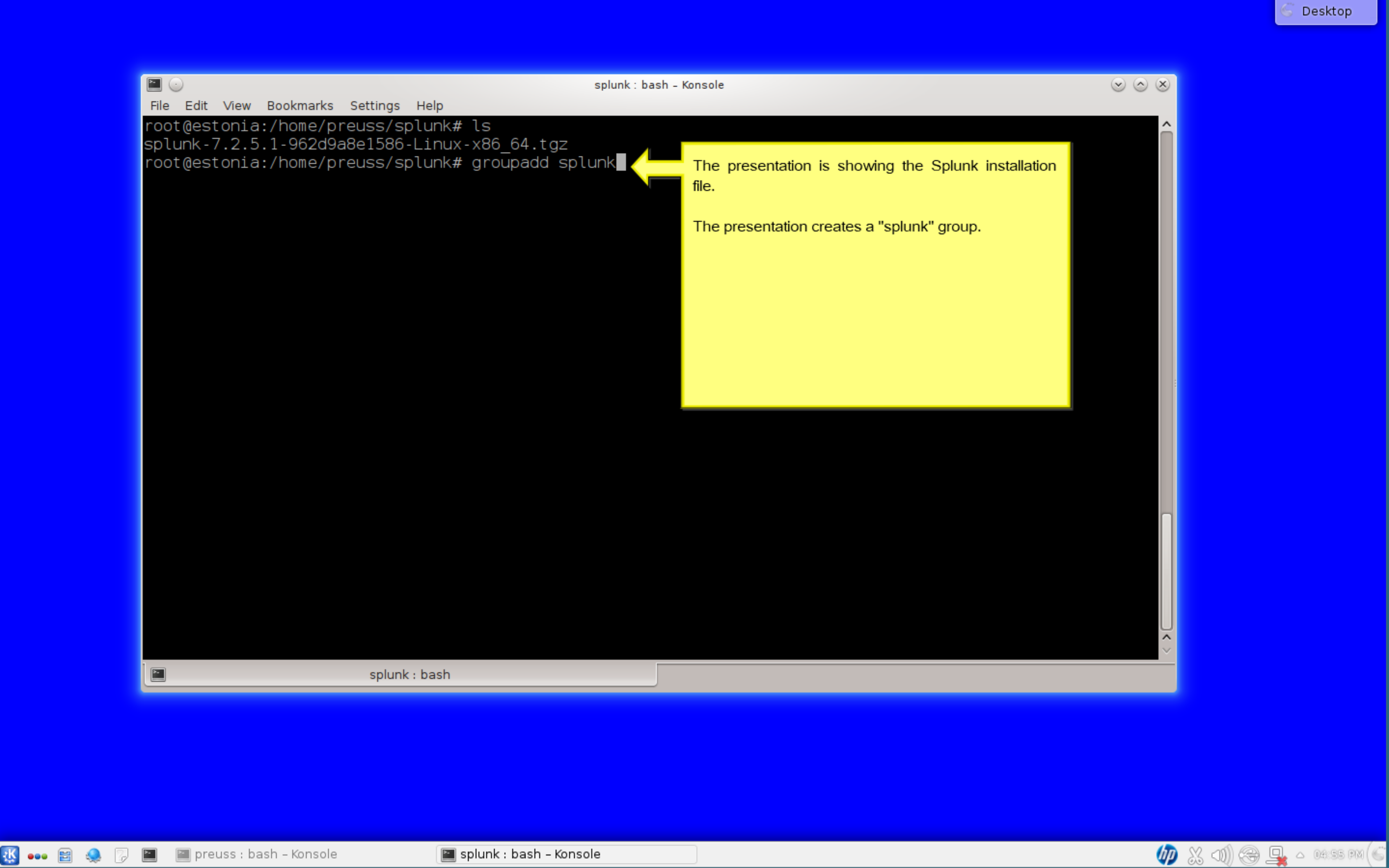
Splunk Installation Spring 2019

The presentation installs the free version of Splunk on Slackware 14.2.

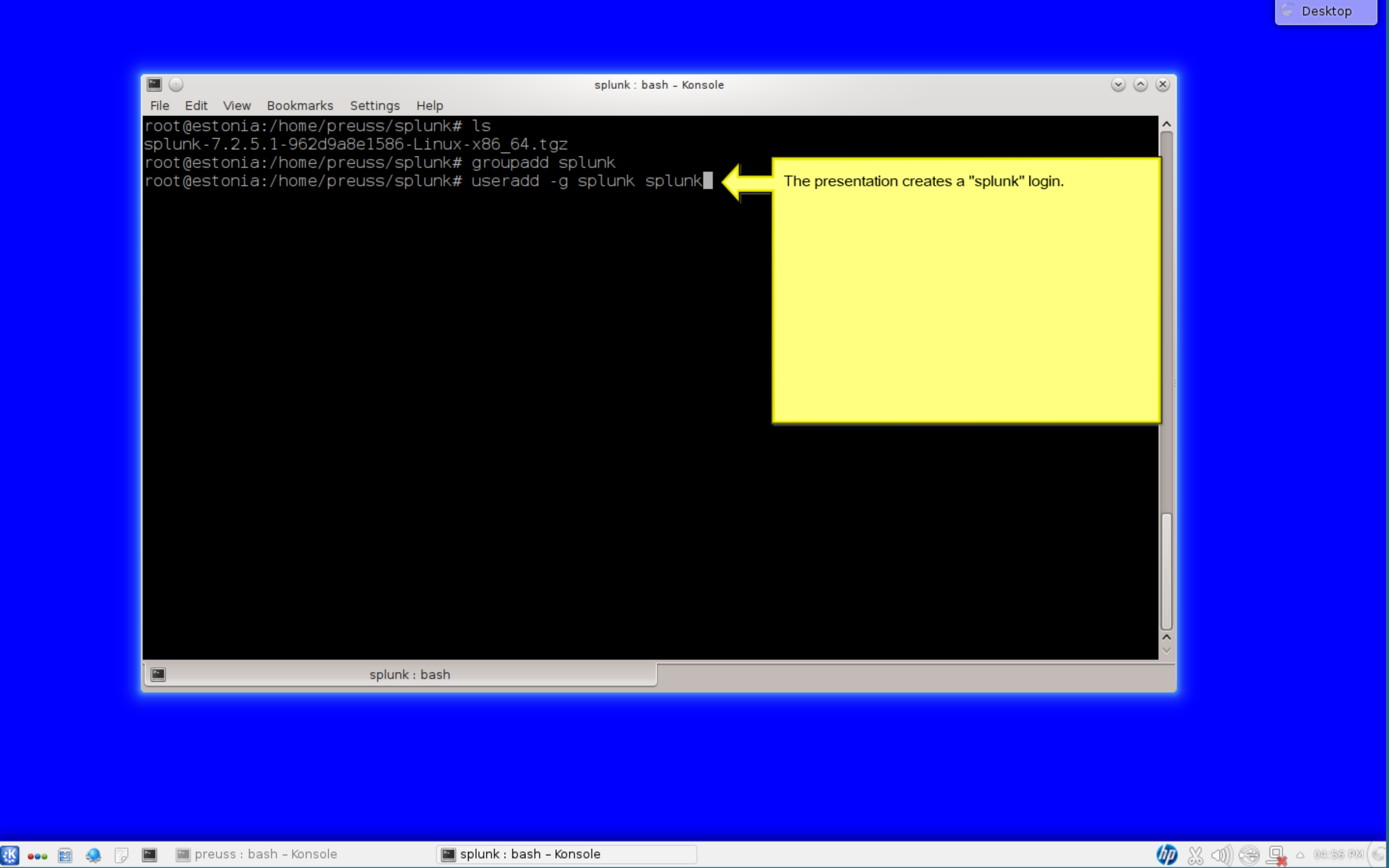
Preuss
4/26/2019



```
root@estonia:/home/preuss/splunk# ls
splunk-7.2.5.1-962d9a8e1586-Linux-x86_64.tgz
root@estonia:/home/preuss/splunk# groupadd splunk
```

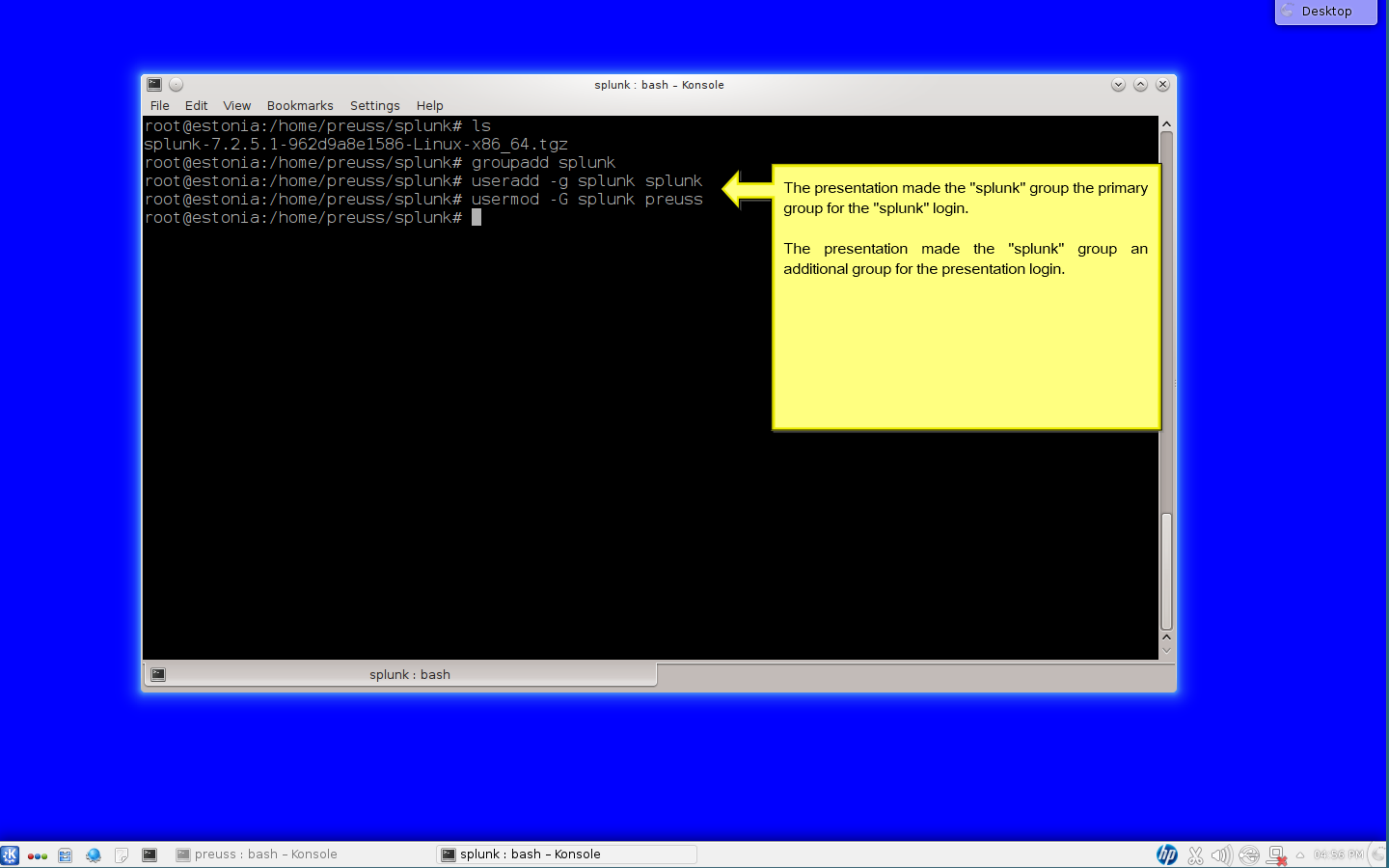
The presentation is showing the Splunk installation file.

The presentation creates a "splunk" group.



```
root@estonia:/home/preuss/splunk# ls
splunk-7.2.5.1-962d9a8e1586-Linux-x86_64.tgz
root@estonia:/home/preuss/splunk# groupadd splunk
root@estonia:/home/preuss/splunk# useradd -g splunk splunk
```

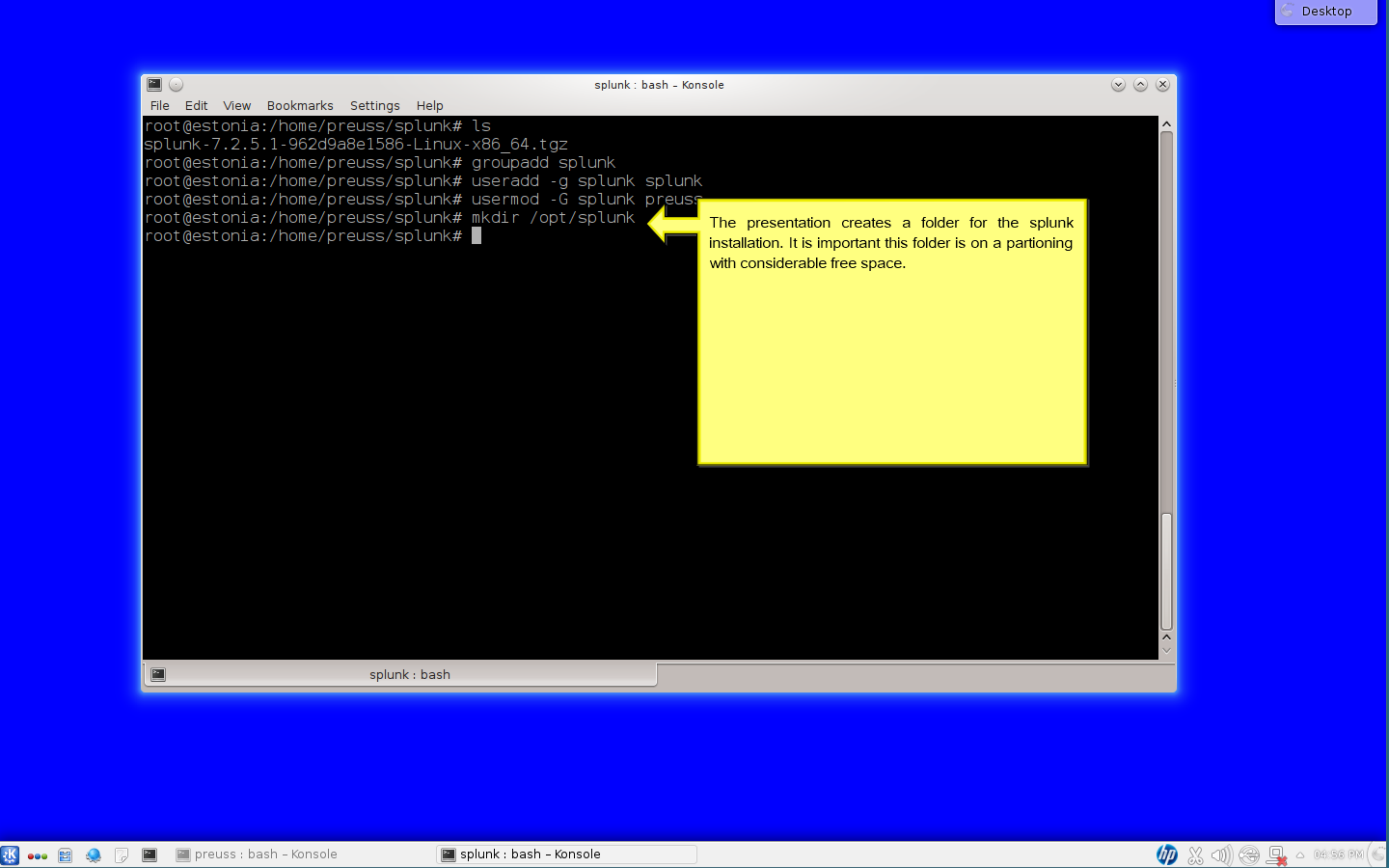
The presentation creates a "splunk" login.



```
root@estonia:/home/preuss/splunk# ls
splunk-7.2.5.1-962d9a8e1586-Linux-x86_64.tgz
root@estonia:/home/preuss/splunk# groupadd splunk
root@estonia:/home/preuss/splunk# useradd -g splunk splunk
root@estonia:/home/preuss/splunk# usermod -G splunk preuss
root@estonia:/home/preuss/splunk# 
```

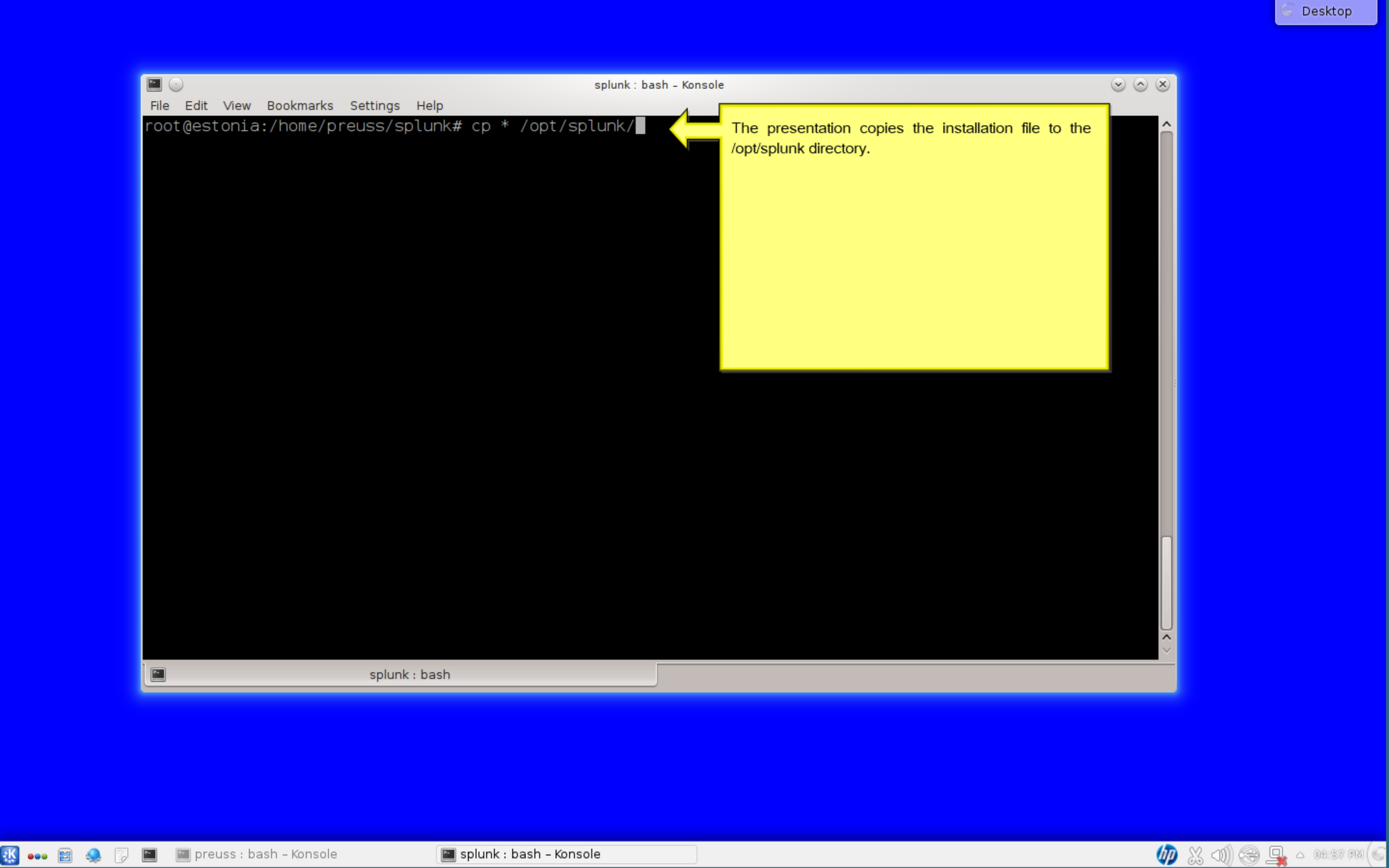
The presentation made the "splunk" group the primary group for the "splunk" login.

The presentation made the "splunk" group an additional group for the presentation login.



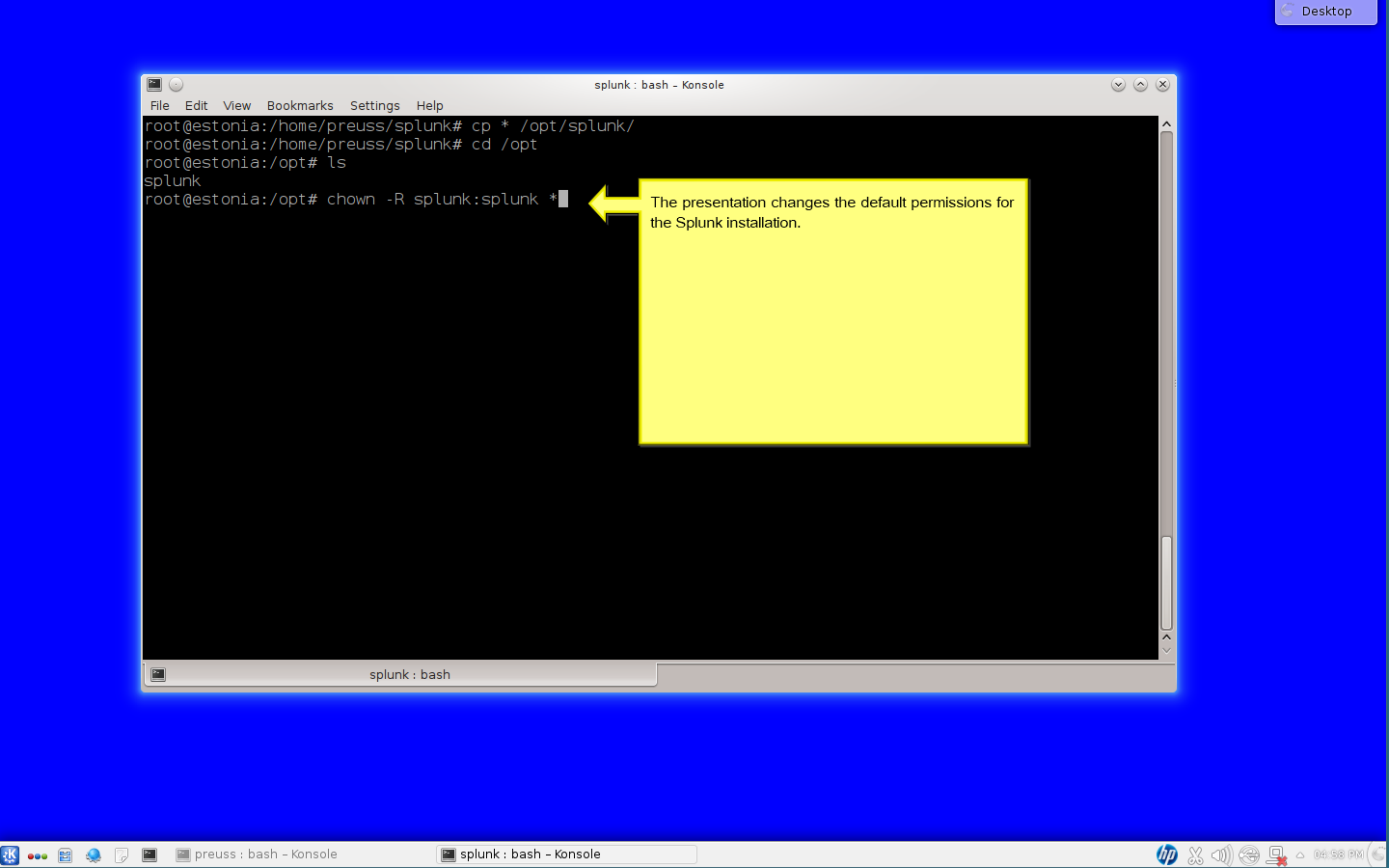
```
root@estonia:/home/preuss/splunk# ls
splunk-7.2.5.1-962d9a8e1586-Linux-x86_64.tgz
root@estonia:/home/preuss/splunk# groupadd splunk
root@estonia:/home/preuss/splunk# useradd -g splunk splunk
root@estonia:/home/preuss/splunk# usermod -G splunk preuss
root@estonia:/home/preuss/splunk# mkdir /opt/splunk
root@estonia:/home/preuss/splunk#
```

The presentation creates a folder for the splunk installation. It is important this folder is on a partioning with considerable free space.



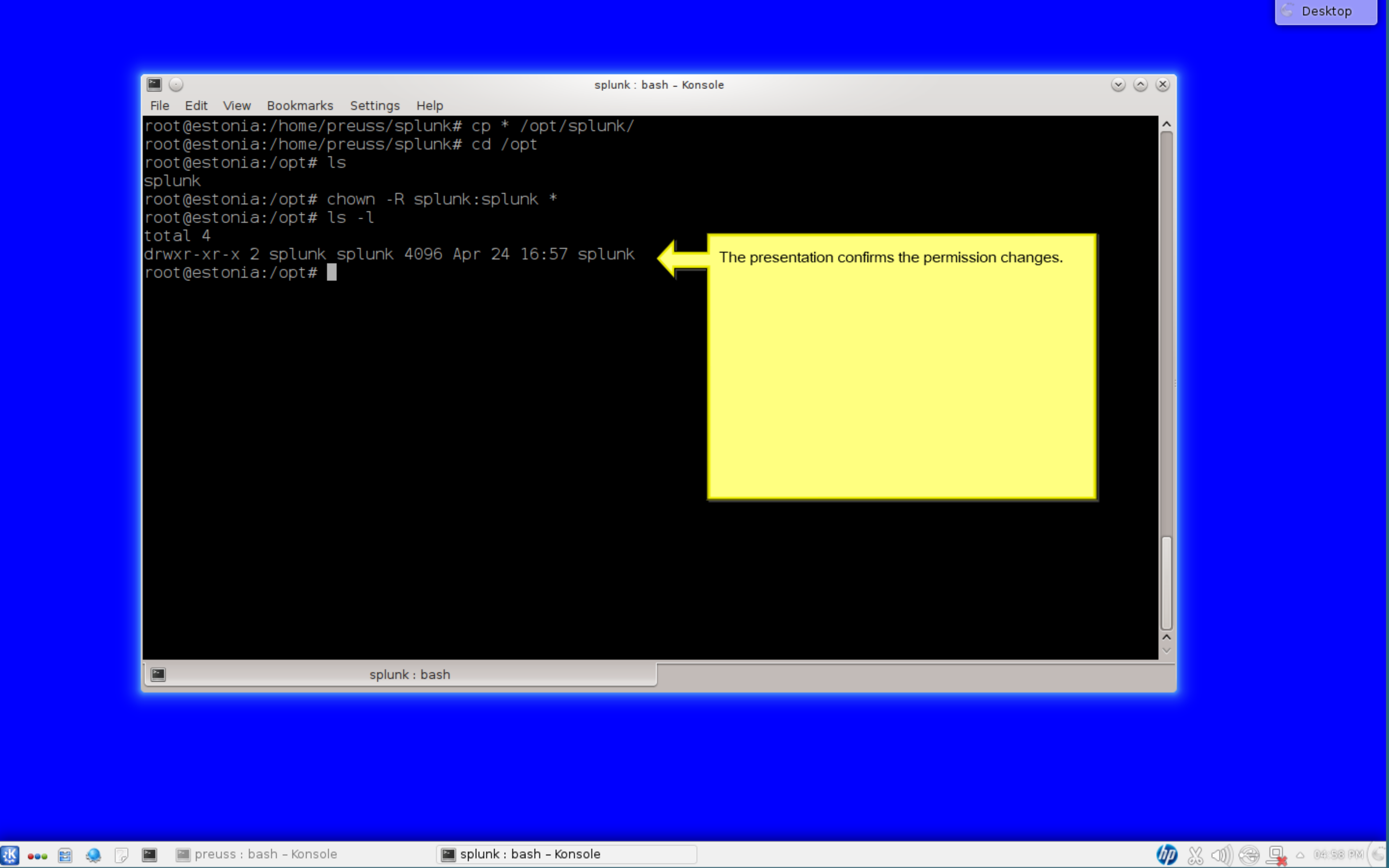
```
root@estonia:/home/preuss/splunk# cp * /opt/splunk/
```

The presentation copies the installation file to the /opt/splunk directory.



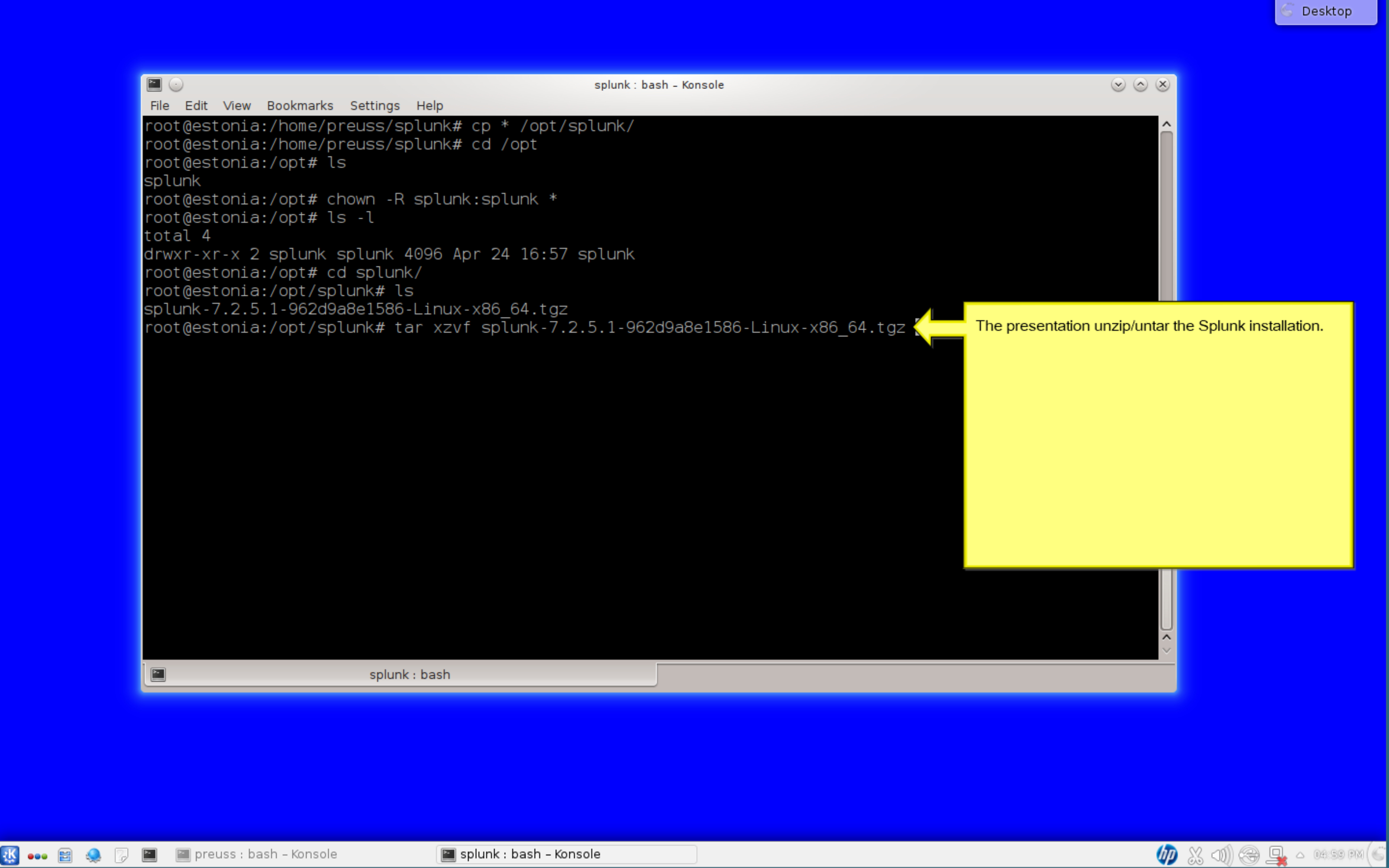
```
root@estonia:/home/preuss/splunk# cp * /opt/splunk/
root@estonia:/home/preuss/splunk# cd /opt
root@estonia:/opt# ls
splunk
root@estonia:/opt# chown -R splunk:splunk *
```

The presentation changes the default permissions for the Splunk installation.



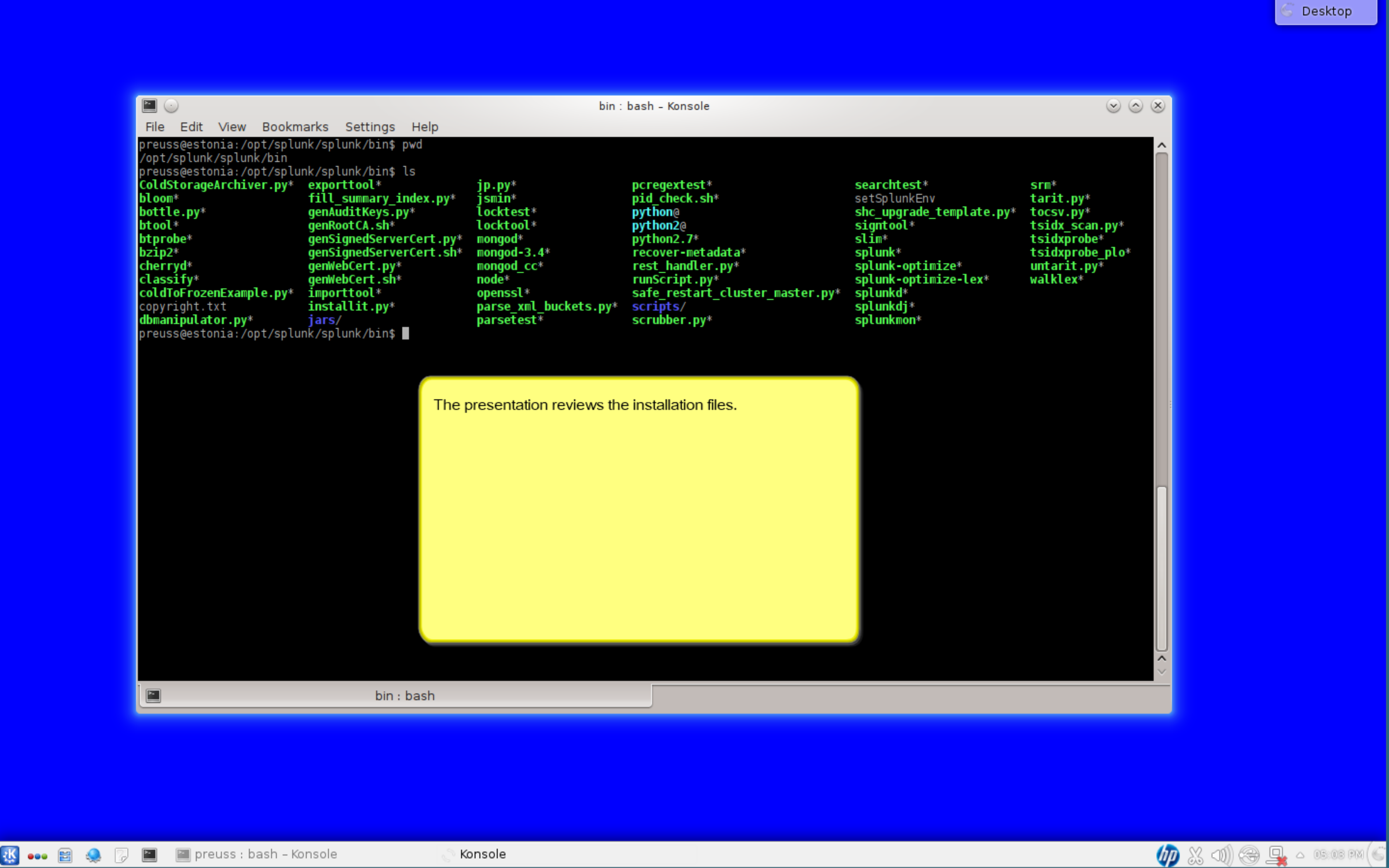
```
root@estonia:/home/preuss/splunk# cp * /opt/splunk/
root@estonia:/home/preuss/splunk# cd /opt
root@estonia:/opt# ls
splunk
root@estonia:/opt# chown -R splunk:splunk *
root@estonia:/opt# ls -l
total 4
drwxr-xr-x 2 splunk splunk 4096 Apr 24 16:57 splunk
root@estonia:/opt# 
```

The presentation confirms the permission changes.



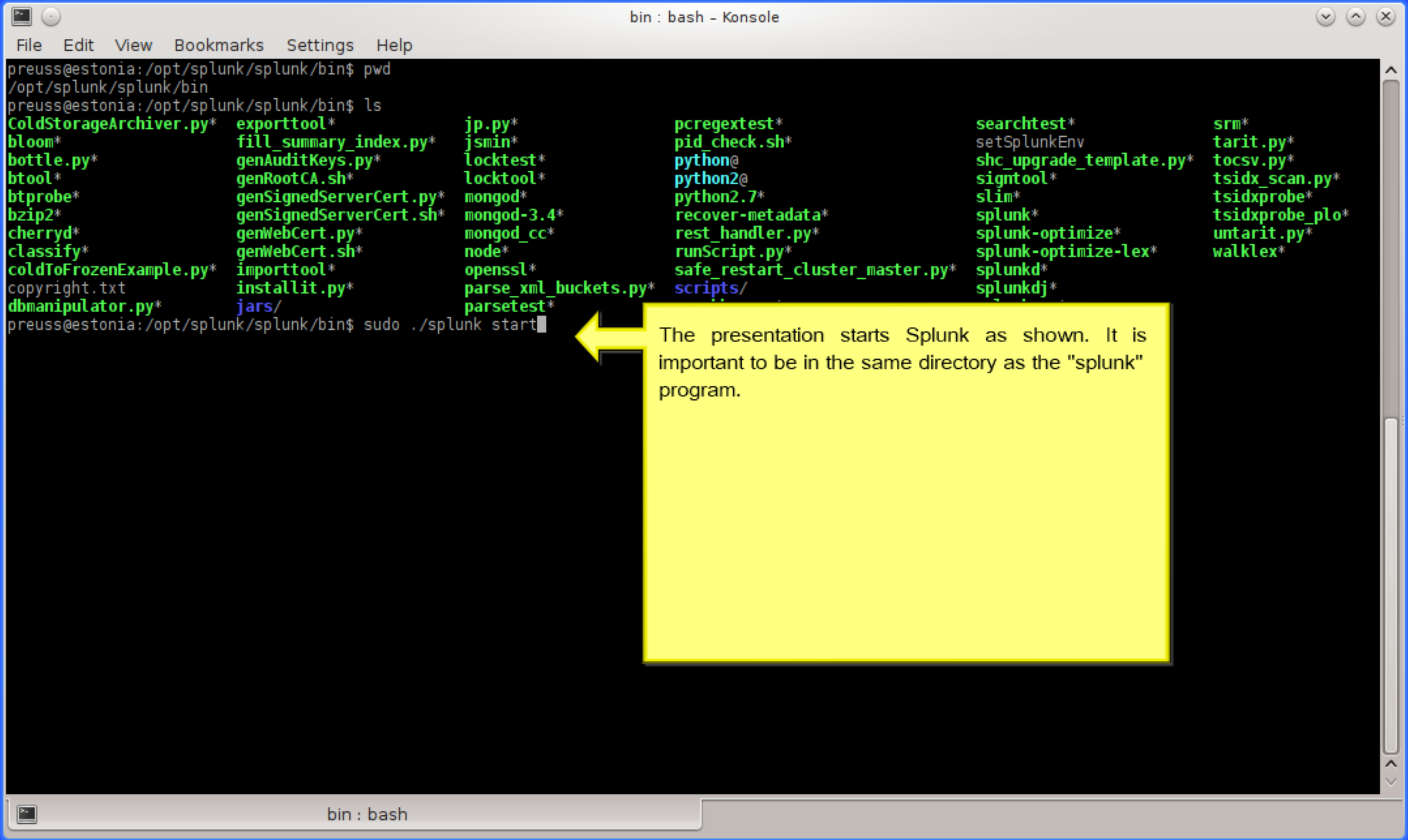
```
root@estonia:/home/preuss/splunk# cp * /opt/splunk/
root@estonia:/home/preuss/splunk# cd /opt
root@estonia:/opt# ls
splunk
root@estonia:/opt# chown -R splunk:splunk *
root@estonia:/opt# ls -l
total 4
drwxr-xr-x 2 splunk splunk 4096 Apr 24 16:57 splunk
root@estonia:/opt# cd splunk/
root@estonia:/opt/splunk# ls
splunk-7.2.5.1-962d9a8e1586-Linux-x86_64.tgz
root@estonia:/opt/splunk# tar xzvf splunk-7.2.5.1-962d9a8e1586-Linux-x86_64.tgz
```

The presentation unzip/untar the Splunk installation.



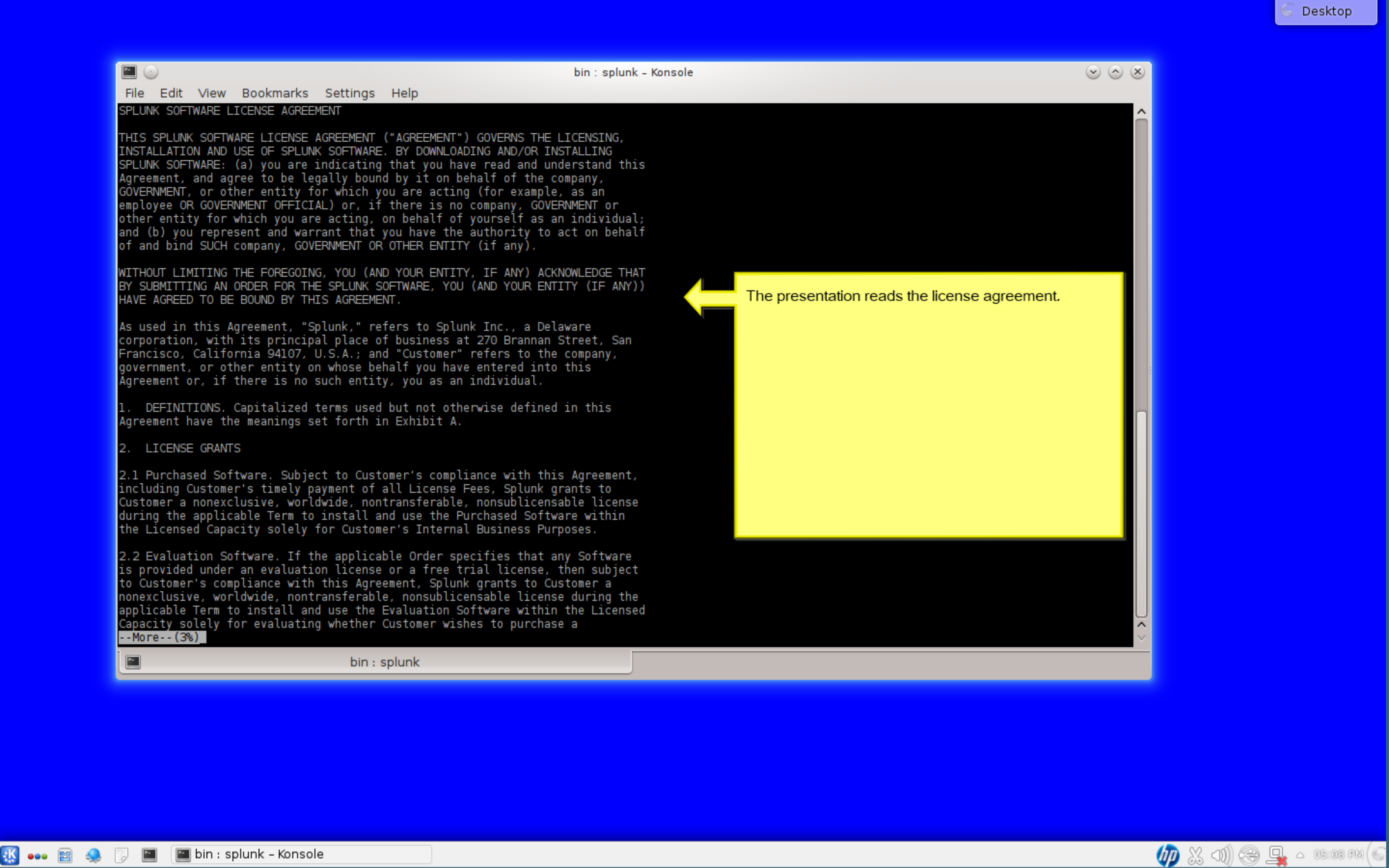
```
preuss@estonia:/opt/splunk/splunk/bin$ pwd
/opt/splunk/splunk/bin
preuss@estonia:/opt/splunk/splunk/bin$ ls
ColdStorageArchiver.py* exporttool*             jp.py*                pcregextest*                    searchtest*              srm*
bloom*                  fill_summary_index.py*  jsmin*                pid_check.sh*                   setSplunkEnv             tarit.py*
bottle.py*              genAuditKeys.py*        locktest*             python@                         shc_upgrade_template.py* tocsv.py*
btool*                  genRootCA.sh*           locktool*             python2@                        signtool*                tsidx_scan.py*
btprobe*                genSignedServerCert.py* mongod*               python2.7*                      slim*                    tsidxprobe*
bzip2*                  genSignedServerCert.sh* mongod-3.4*           recover-metadata*               splunk*                  tsidxprobe_plo*
cherryd*                genWebCert.py*          mongod_cc*            rest_handler.py*                splunk-optimize*         untarit.py*
classify*               genWebCert.sh*          node*                 runScript.py*                   splunk-optimize-lex*     walklex*
coldToFrozenExample.py* importtool*             openssl*              safe_restart_cluster_master.py* splunkd*
copyright.txt           installit.py*           parse_xml_buckets.py* scripts/                        splunkdj*
dbmanipulator.py*       jars/                   parsetest*            scrubber.py*                    splunkmon*
preuss@estonia:/opt/splunk/splunk/bin$ 
```

The presentation reviews the installation files.



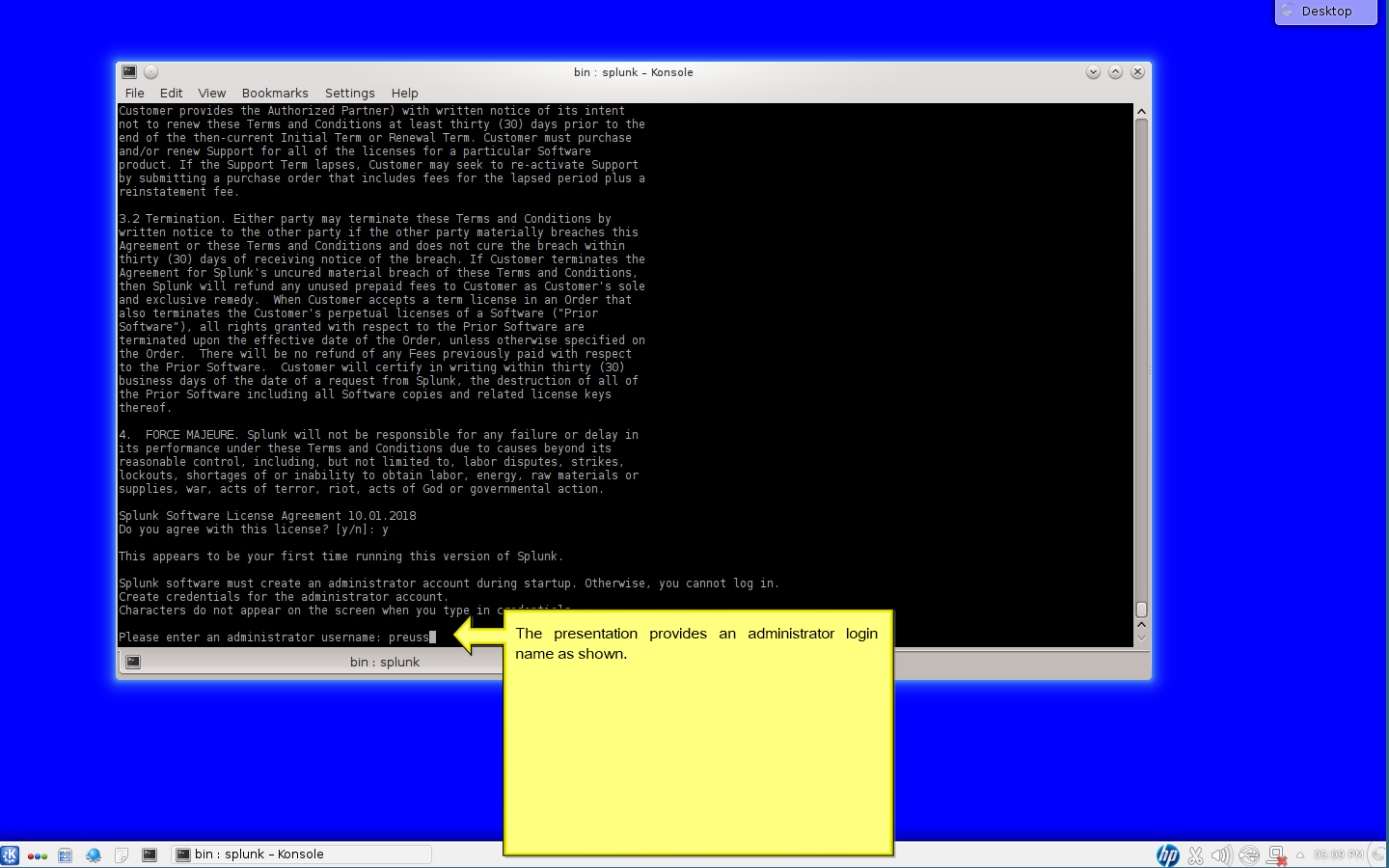
```
preuss@estonia:/opt/splunk/splunk/bin$ pwd
/opt/splunk/splunk/bin
preuss@estonia:/opt/splunk/splunk/bin$ ls
ColdStorageArchiver.py*  exporttool*              jp.py*                pcregextest*                     searchtest*                  srm*
bloom*                   fill_summary_index.py*   jsmin*                pid_check.sh*                    setSplunkEnv                 tarit.py*
bottle.py*               genAuditKeys.py*         locktest*             python@                          shc_upgrade_template.py*     tocsv.py*
btool*                   genRootCA.sh*            locktool*             python2@                         signtool*                    tsidx_scan.py*
btprobe*                 genSignedServerCert.py*  mongod*               python2.7*                       slim*                        tsidxprobe*
bzip2*                   genSignedServerCert.sh*  mongod-3.4*           recover-metadata*                splunk*                      tsidxprobe_plo*
cherryd*                 genWebCert.py*           mongod_cc*            rest_handler.py*                 splunk-optimize*             untarit.py*
classify*                genWebCert.sh*           node*                 runScript.py*                    splunk-optimize-lex*         walklex*
coldToFrozenExample.py*  importtool*              openssl*              safe_restart_cluster_master.py*  splunkd*
copyright.txt            installit.py*            parse_xml_buckets.py* scripts/                         splunkdj*
dbmanipulator.py*        jars/                    parsetest*
preuss@estonia:/opt/splunk/splunk/bin$ sudo ./splunk start
```

The presentation starts Splunk as shown. It is important to be in the same directory as the "splunk" program.



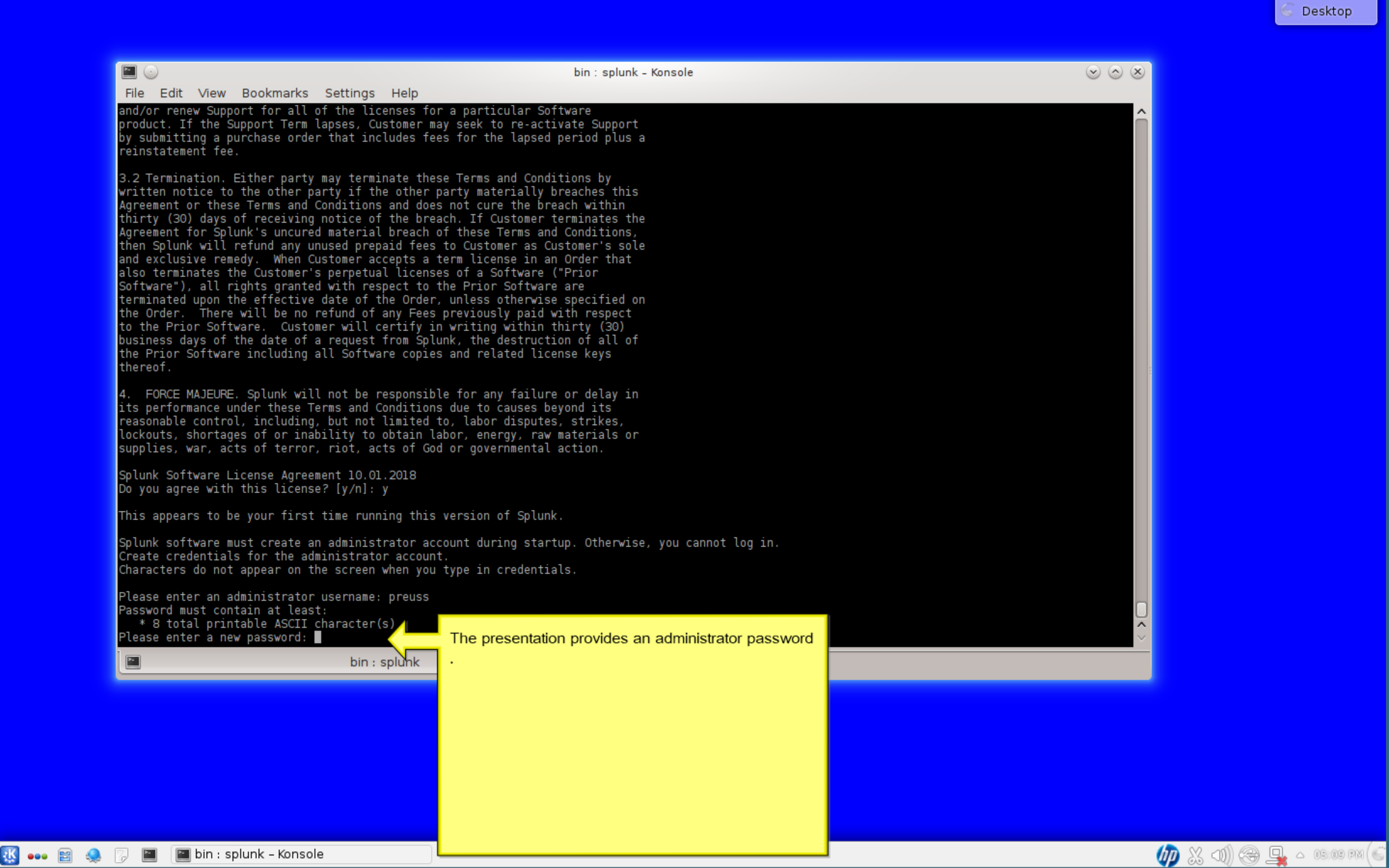
```
SPLUNK SOFTWARE LICENSE AGREEMENT

THIS SPLUNK SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERNS THE LICENSING,
INSTALLATION AND USE OF SPLUNK SOFTWARE. BY DOWNLOADING AND/OR INSTALLING
SPLUNK SOFTWARE: (a) you are indicating that you have read and understand this
Agreement, and agree to be legally bound by it on behalf of the company,
GOVERNMENT, or other entity for which you are acting (for example, as an
employee OR GOVERNMENT OFFICIAL) or, if there is no company, GOVERNMENT or
other entity for which you are acting, on behalf of yourself as an individual;
and (b) you represent and warrant that you have the authority to act on behalf
of and bind SUCH company, GOVERNMENT OR OTHER ENTITY (if any).

WITHOUT LIMITING THE FOREGOING, YOU (AND YOUR ENTITY, IF ANY) ACKNOWLEDGE THAT
BY SUBMITTING AN ORDER FOR THE SPLUNK SOFTWARE, YOU (AND YOUR ENTITY (IF ANY))
HAVE AGREED TO BE BOUND BY THIS AGREEMENT.

As used in this Agreement, "Splunk," refers to Splunk Inc., a Delaware
corporation, with its principal place of business at 270 Brannan Street, San
Francisco, California 94107, U.S.A.; and "Customer" refers to the company,
government, or other entity on whose behalf you have entered into this
Agreement or, if there is no such entity, you as an individual.

1.  DEFINITIONS. Capitalized terms used but not otherwise defined in this
Agreement have the meanings set forth in Exhibit A.

2.  LICENSE GRANTS

2.1 Purchased Software. Subject to Customer's compliance with this Agreement,
including Customer's timely payment of all License Fees, Splunk grants to
Customer a nonexclusive, worldwide, nontransferable, nonsublicensable license
during the applicable Term to install and use the Purchased Software within
the Licensed Capacity solely for Customer's Internal Business Purposes.

2.2 Evaluation Software. If the applicable Order specifies that any Software
is provided under an evaluation license or a free trial license, then subject
to Customer's compliance with this Agreement, Splunk grants to Customer a
nonexclusive, worldwide, nontransferable, nonsublicensable license during the
applicable Term to install and use the Evaluation Software within the Licensed
Capacity solely for evaluating whether Customer wishes to purchase a
--More--(3%)
```

The presentation reads the license agreement.



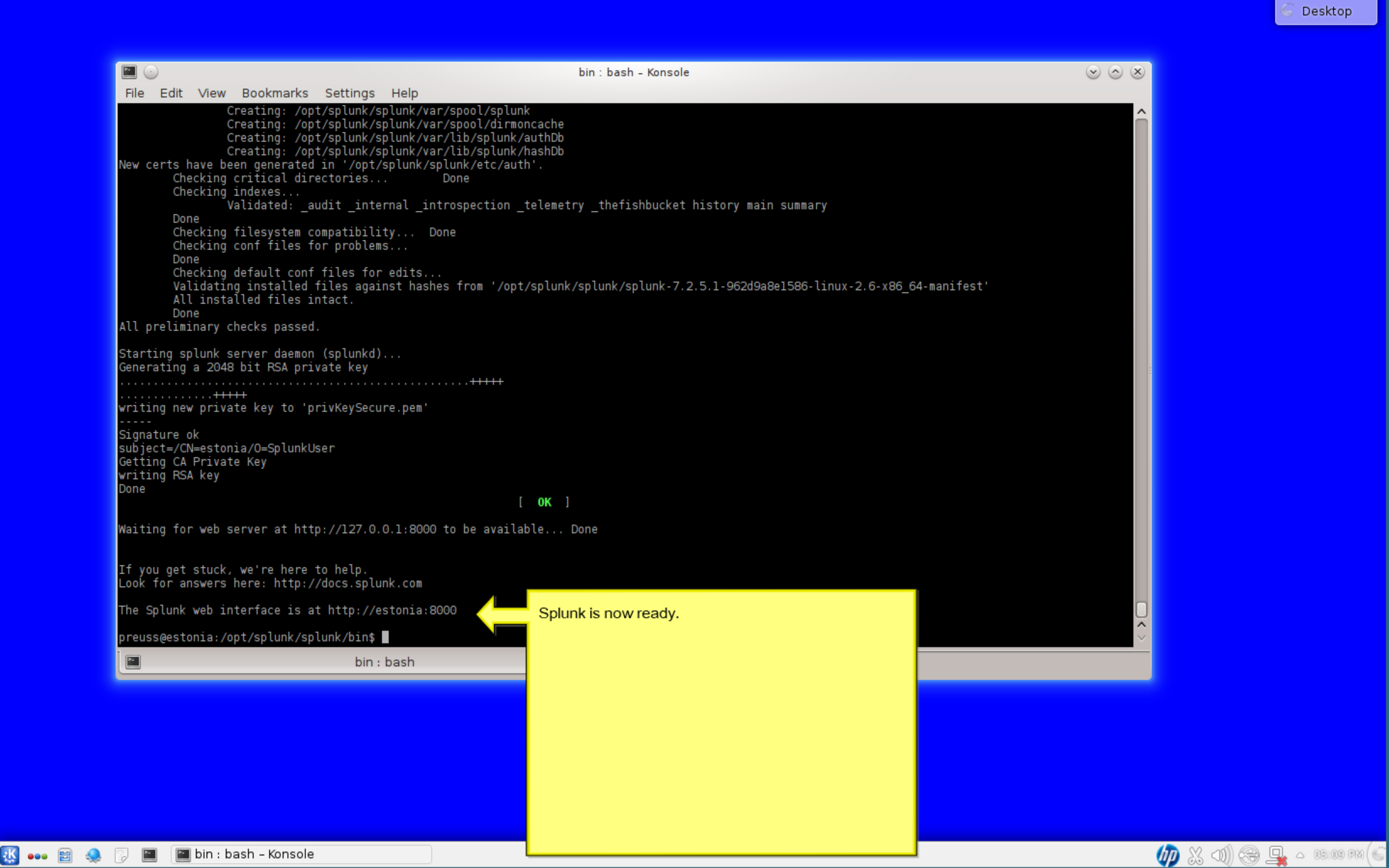
```
Customer provides the Authorized Partner) with written notice of its intent
not to renew these Terms and Conditions at least thirty (30) days prior to the
end of the then-current Initial Term or Renewal Term. Customer must purchase
and/or renew Support for all of the licenses for a particular Software
product. If the Support Term lapses, Customer may seek to re-activate Support
by submitting a purchase order that includes fees for the lapsed period plus a
reinstatement fee.

3.2 Termination. Either party may terminate these Terms and Conditions by
written notice to the other party if the other party materially breaches this
Agreement or these Terms and Conditions and does not cure the breach within
thirty (30) days of receiving notice of the breach. If Customer terminates the
Agreement for Splunk's uncured material breach of these Terms and Conditions,
then Splunk will refund any unused prepaid fees to Customer as Customer's sole
and exclusive remedy.  When Customer accepts a term license in an Order that
also terminates the Customer's perpetual licenses of a Software ("Prior
Software"), all rights granted with respect to the Prior Software are
terminated upon the effective date of the Order, unless otherwise specified on
the Order.  There will be no refund of any Fees previously paid with respect
to the Prior Software.  Customer will certify in writing within thirty (30)
business days of the date of a request from Splunk, the destruction of all of
the Prior Software including all Software copies and related license keys
thereof.

4.  FORCE MAJEURE. Splunk will not be responsible for any failure or delay in
its performance under these Terms and Conditions due to causes beyond its
reasonable control, including, but not limited to, labor disputes, strikes,
lockouts, shortages of or inability to obtain labor, energy, raw materials or
supplies, war, acts of terror, riot, acts of God or governmental action.

Splunk Software License Agreement 10.01.2018
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: preuss
```

The presentation provides an administrator login name as shown.



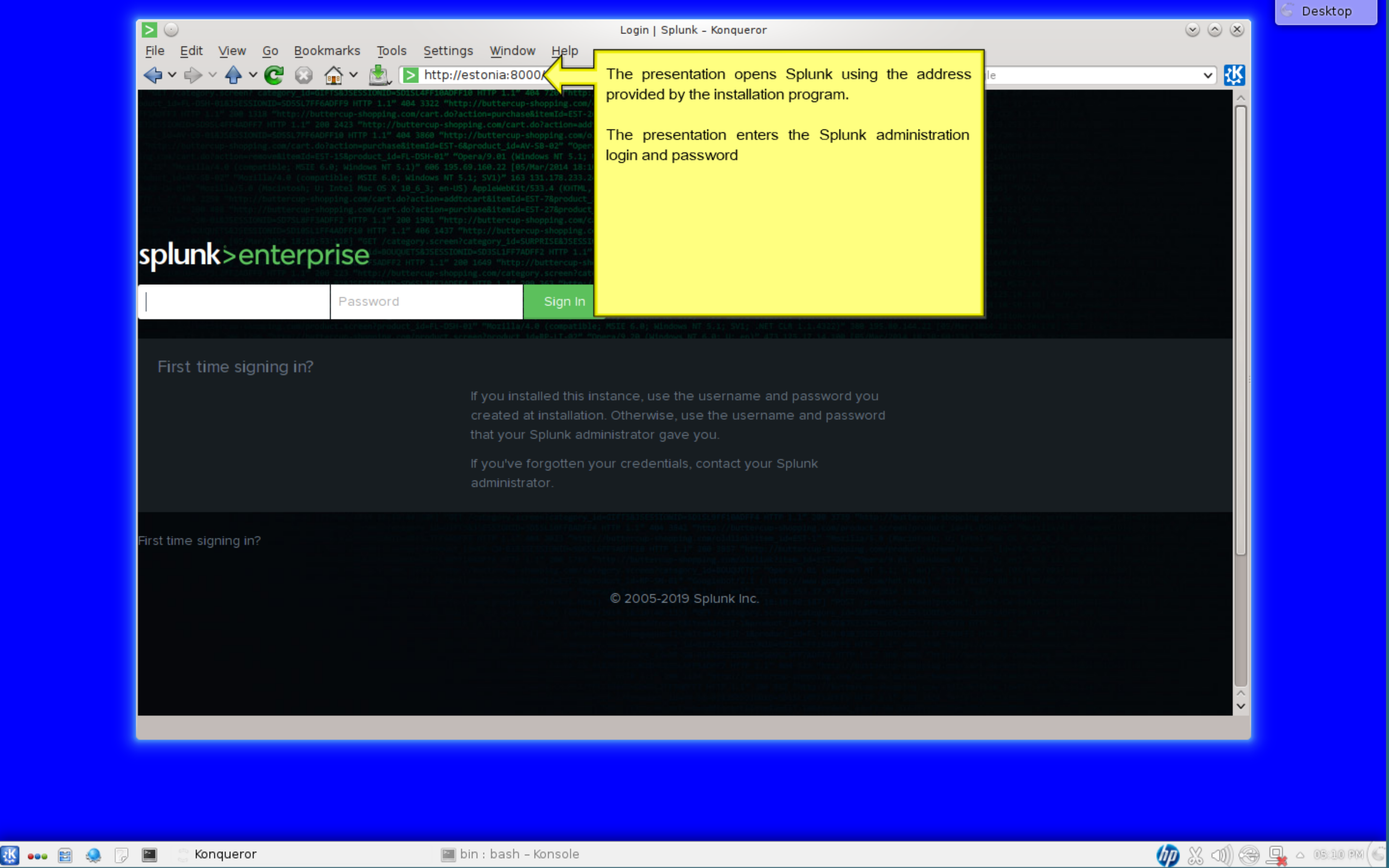
```
and/or renew Support for all of the licenses for a particular Software
product. If the Support Term lapses, Customer may seek to re-activate Support
by submitting a purchase order that includes fees for the lapsed period plus a
reinstatement fee.

3.2 Termination. Either party may terminate these Terms and Conditions by
written notice to the other party if the other party materially breaches this
Agreement or these Terms and Conditions and does not cure the breach within
thirty (30) days of receiving notice of the breach. If Customer terminates the
Agreement for Splunk's uncured material breach of these Terms and Conditions,
then Splunk will refund any unused prepaid fees to Customer as Customer's sole
and exclusive remedy.  When Customer accepts a term license in an Order that
also terminates the Customer's perpetual licenses of a Software ("Prior
Software"), all rights granted with respect to the Prior Software are
terminated upon the effective date of the Order, unless otherwise specified on
the Order.  There will be no refund of any Fees previously paid with respect
to the Prior Software.  Customer will certify in writing within thirty (30)
business days of the date of a request from Splunk, the destruction of all of
the Prior Software including all Software copies and related license keys
thereof.

4.  FORCE MAJEURE. Splunk will not be responsible for any failure or delay in
its performance under these Terms and Conditions due to causes beyond its
reasonable control, including, but not limited to, labor disputes, strikes,
lockouts, shortages of or inability to obtain labor, energy, raw materials or
supplies, war, acts of terror, riot, acts of God or governmental action.

Splunk Software License Agreement 10.01.2018
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: preuss
Password must contain at least:
   * 8 total printable ASCII character(s)
Please enter a new password: 
```

The presentation provides an administrator password
.



```
                Creating: /opt/splunk/splunk/var/spool/splunk
                Creating: /opt/splunk/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/splunk/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunk/splunk/etc/auth'.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspection _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk/splunk-7.2.5.1-962d9a8e1586-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a 2048 bit RSA private key
....................................................+++++
..............+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=estonia/O=SplunkUser
Getting CA Private Key
writing RSA key
Done
                                                            [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://estonia:8000

preuss@estonia:/opt/splunk/splunk/bin$ 
```

Splunk is now ready.



The presentation opens Splunk using the address provided by the installation program.

The presentation enters the Splunk administration login and password

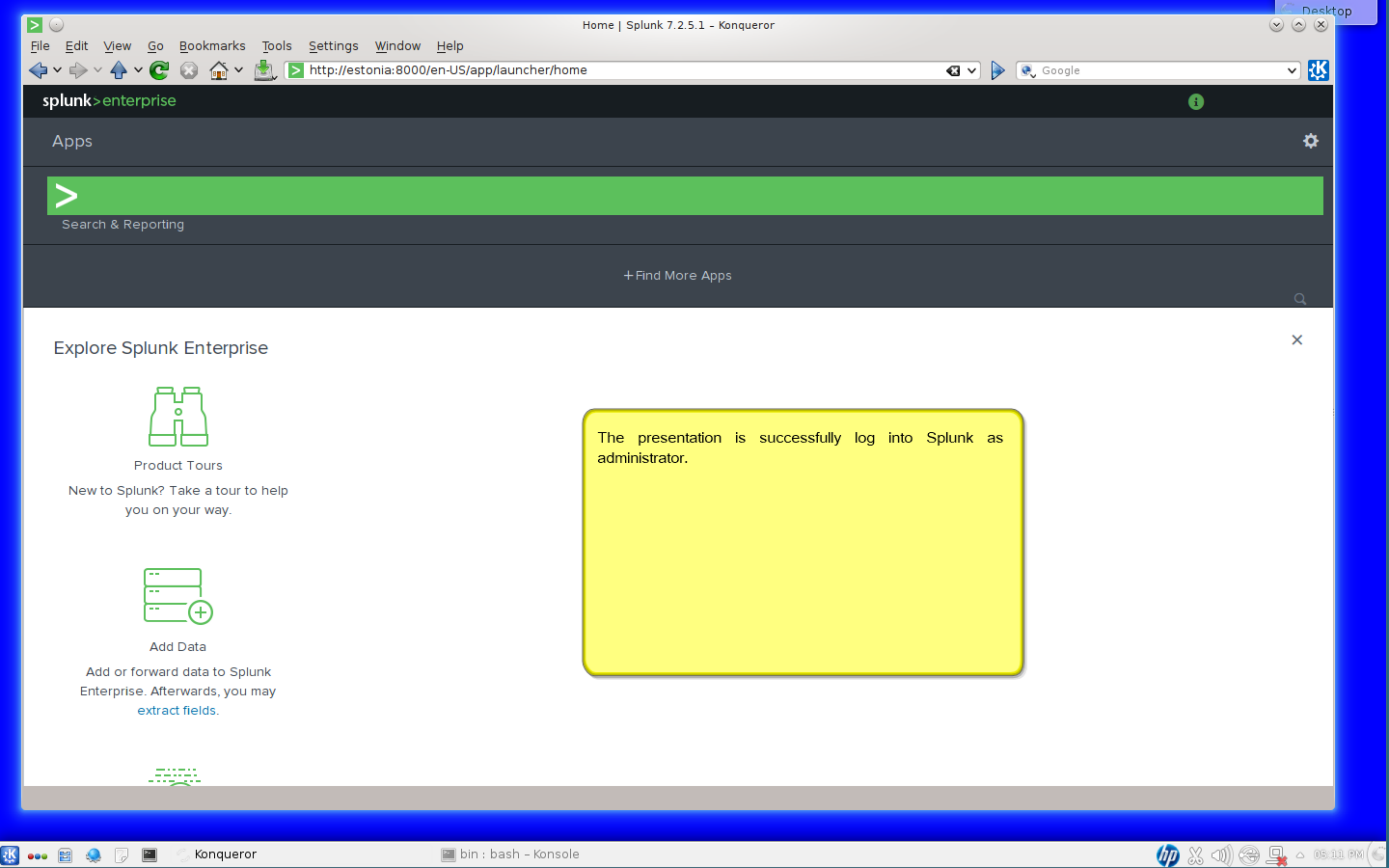
First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you.

If you've forgotten your credentials, contact your Splunk administrator.

First time signing in?

© 2005-2019 Splunk Inc.



Desktop
Home | Splunk 7.2.5.1 – Konqueror
File
Edit
View
Go
Bookmarks
Tools
Settings
Window
Help
Google
splunk>enterprise
Apps
Search & Reporting
+Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Konqueror
bin : bash – Konsole
05:11 PM

http://estonia:8000/en-US/app/launcher/home

The presentation is successfully log into Splunk as administrator.