Sécurité du Big Data
TP Hadoop & Kerberos

4e IABD

```
nadim@nadim:~$ hostnamectl set-hostname server.security-tp.com
nadim@nadim:~$
```

```
nadim@server:~$ cat /etc/hosts
127.0.0.1        localhost
127.0.1.1        nadim.myguest.virtualbox.org        nadim
127.0.0.1        client.security-tp.com
127.0.0.1        server.security-tp.com
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
┌───────────────── Configuring Kerberos Authentication ─────────────────┐
│ When users attempt to use Kerberos and specify a principal or user name without │
│ specifying what administrative Kerberos realm that principal belongs to, the system │
│ appends the default realm.  The default realm may also be used as the realm of a Kerberos │
│ service running on the local machine.  Often, the default realm is the uppercase version │
│ of the local DNS domain.                                                          │
│                                                                                   │
│ Default Kerberos version 5 realm:                                                 │
│                                                                                   │
│ SECURITY-TP.COM                                                                   │
│                                                                                   │
│                                    <Ok>                                           │
│                                                                                   │
└───────────────────────────────────────────────────────────────────────┘
```

```
┌───────────────── Configuring Kerberos Authentication ─────────────────┐
│ Enter the hostnames of Kerberos servers in the SECURITY-TP.COM Kerberos realm separated │
│ by spaces.                                                                        │
│                                                                                   │
│ Kerberos servers for your realm:                                                  │
│                                                                                   │
│ server.security-tp.com                                                            │
│                                   <Ok>                                            │
│                                                                                   │
└───────────────────────────────────────────────────────────────────────┘
```

```
Selecting previously unselected package krb5-admin-server.
Preparing to unpack .../9-krb5-admin-server_1.19.2-2_amd64.deb ...
Unpacking krb5-admin-server (1.19.2-2) ...
Setting up libgssrpc4:amd64 (1.19.2-2) ...
Setting up krb5-config (2.6+nmu1ubuntu1) ...
Setting up libkadm5clnt-mit12:amd64 (1.19.2-2) ...
Setting up libkdb5-10:amd64 (1.19.2-2) ...
Setting up libkadm5srv-mit12:amd64 (1.19.2-2) ...
Setting up krb5-user (1.19.2-2) ...
Setting up libverto-libevent1:amd64 (0.3.1-1ubuntu3) ...
Setting up libverto1:amd64 (0.3.1-1ubuntu3) ...
Setting up krb5-kdc (1.19.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/krb5-kdc.service →/
lib/systemd/syste
m/krb5-kdc.service.
Could not execute systemctl:  at /usr/bin/deb-systemd-invoke line 142.
Setting up krb5-admin-server (1.19.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/krb5-admin-server.se
rvice →/lib/syst
emd/system/krb5-admin-server.service.
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Processing triggers for man-db (2.10.2-1) ...
nadim@server:~$
```

```
remembered.  However, if you lose the
password and /etc/krb5kdc/stash,
you cannot decrypt your Kerberos datab
ase.
Loading random data
Initializing database '/var/lib/krb5kd
c/principal' for realm 'SECURITY-TP.CO
M',
master key name 'K/M@SECURITY-TP.COM'
You will be prompted for the database
Master Password.
It is important that you NOT FORGET th
is password.
Enter KDC database master key:
Re-enter KDC database master key to ve
rify:
```

```
Now that your realm is set up you may
wish to create an administrative
principal using the addprinc subcomman
d of the kadmin.local program.
Then, this principal can be added to /
etc/krb5kdc/kadm5.acl so that
you can use the kadmin program on othe
r computers.  Kerberos admin
principals usually belong to a single
user and end in /admin.  For
example, if jruser is a Kerberos admin
istrator, then in addition to
the normal jruser principal, a jruser/
admin principal should be
created.

Don't forget to set up DNS information
 so your clients can find your
KDC and admin servers.  Doing so is do
cumented in the administration
guide.
nadim@server:~$
```

```
      /etc/krb5kdc/kadm5.acl *
# This file Is the access control list >
# When this file is edited run service >
# One common way to set up Kerberos adm>
# ending in /admin  is given full admin>
# To enable this, uncomment the followi>
*/admin *
```

```
nadim@server:~$ systemctl status krb5-admin-server
● krb5-admin-server.service - Kerberos 5 Admin Server
     Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2022-11-30 11:59:34 WAT; 7s ago
   Main PID: 32657 (kadmind)
      Tasks: 1 (limit: 4625)
     Memory: 636.0K
        CPU: 41ms
     CGroup: /system.slice/krb5-admin-server.service
             └─32657 /usr/sbin/kadmind -nofork
```

```
nadim@server:~$ sudo kadmin.local
Authenticating as principal root/admin@SECURITY-TP.COM with password.
kadmin.local:  addprinc nadim
No policy specified for nadim@SECURITY-TP.COM; defaulting to no policy
Enter password for principal "nadim@SECURITY-TP.COM":
Re-enter password for principal "nadim@SECURITY-TP.COM":
Principal "nadim@SECURITY-TP.COM" created.
```

```
nadim@server:~$ kinit nadim
Password for nadim@SECURITY-TP.COM:
nadim@server:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: nadim@SECURITY-TP.COM

Valid starting       Expires              Service principal
30/11/2022 12:05:31  30/11/2022 22:05:31  krbtgt/SECURITY-TP.COM@SECURITY-TP.COM
        renew until 01/12/2022 12:05:27
```

```
Principal: nadim@SECURITY-TP.COM
Expiration date: [never]
Last password change: Wed Nov 30 11:57:53 WAT 2022
Password expiration date: [never]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Nov 30 11:57:53 WAT 2022 (root/admin@SECURITY-TP.COM)
Last successful authentication: Wed Nov 30 12:05:31 WAT 2022
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, aes256-cts-hmac-sha1-96
Key: vno 1, aes128-cts-hmac-sha1-96
MKey: vno 1
Attributes: REQUIRES_PRE_AUTH
Policy: [none]
```

nadim@server: ~

nadim@server: ~ 80x24

```
openjdk-11-jdk            openjdk-11-jre-headless
nadim@server:~$ sudo apt install openjdk-11-jdk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openjdk-11-jdk is already the newest version (11.0.17+8-1ubuntu2~22.04).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
nadim@server:~$ java -version
openjdk version "11.0.17" 2022-10-18
OpenJDK Runtime Environment (build 11.0.17+8-post-Ubuntu-1ubuntu222.04)
OpenJDK 64-Bit Server VM (build 11.0.17+8-post-Ubuntu-1ubuntu222.04, mixed mode,
 sharing)
nadim@server:~$ sudo adduser hadoop
Adding user `hadoop' ...
Adding new group `hadoop' (1001) ...
Adding new user `hadoop' (1001) with group `hadoop' ...
Creating home directory `/home/hadoop' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
```

```
 sharing)
nadim@server:~$ sudo adduser hadoop
Adding user `hadoop' ...
Adding new group `hadoop' (1001) ...
Adding new user `hadoop' (1001) with group `hadoop' ...
Creating home directory `/home/hadoop' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for hadoop
Enter the new value, or press ENTER for the default
        Full Name []: nadim
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
nadim@server:~$
```

```
hadoop@server:~$ ssh-keygen -t rsaa
unknown key type rsaa
hadoop@server:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/hadoop/.ssh/id_rsa):
Created directory '/home/hadoop/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hadoop/.ssh/id_rsa
Your public key has been saved in /home/hadoop/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:IBL6hWHoLKQlnxICpuA0YK9mHTkCWsYdi8E38+5R8XM hadoop@server.security-tp.com
The key's randomart image is:
+---[RSA 3072]----+
|BOB...           |
|#****.  .        |
|XB+B++.  o       |
|++*oo.... o E    |
|.=.. . .S o      |
|o    o           |
|    . .          |
|     .           |
|                 |
+----[SHA256]-----+
hadoop@server:~$
```

```
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:r2LkCVpkpkg7ym68W95yMyvvoERo0OBNoe978YtCn7M root@server.security-tp.com (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:ZfQIkuqNDIZyoie44o+dVwT//XqFM+d0QJWc8Gzwbq8 root@server.security-tp.com (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for ufw (0.36.1-4build1) ...
hadoop@server:~$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:ZfQIkuqNDIZyoie44o+dVwT//XqFM+d0QJWc8Gzwbq8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

19 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hadoop@server:~$
```

```
hadoop-3.3.4/share/doc/hadoop/hadoop-archives/images/bg.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-archives/images/newwindow.png
hadoop-3.3.4/share/doc/hadoop/hadoop-archives/images/h3.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/project-reports.html
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/dependency-analysis.html
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/css/
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/css/maven-base.css
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/css/print.css
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/css/maven-theme.css
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/css/site.css
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/breadcrumbs.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/apache-maven-project-2.png
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/maven-logo-2.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/collapsed.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/logo_maven.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/icon_warning_sml.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/logos/
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/logos/build-by-maven-black.png
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/logos/maven-feather.png
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/logos/build-by-maven-white.png
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/banner.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/h5.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/icon_error_sml.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/icon_success_sml.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/expanded.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/external.png
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/icon_info_sml.gif
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/logo_apache.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/bg.jpg
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/newwindow.png
hadoop-3.3.4/share/doc/hadoop/hadoop-hdfs-nfs/images/h3.jpg
hadoop@server:~$ mv hadoop-3.3.4 hadoop
hadoop@server:~$
```
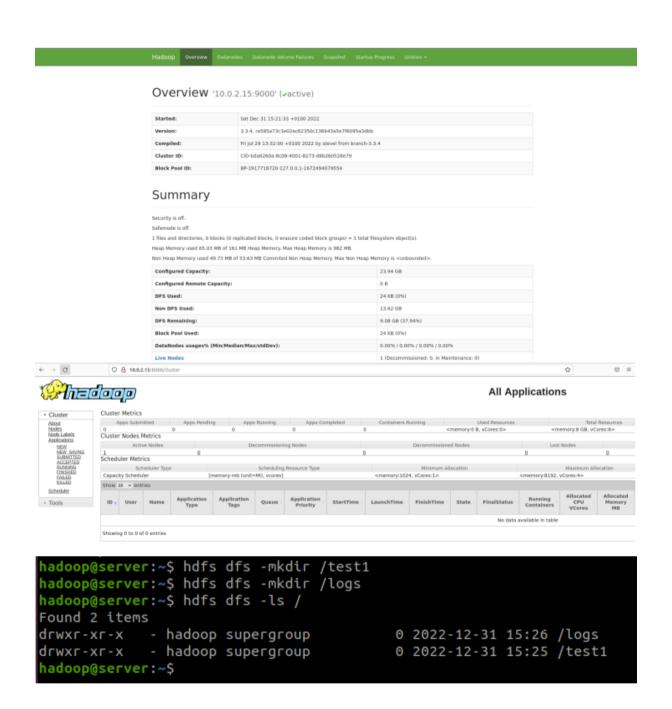
```
hadoop@server:~$ nano ~/.bashrc
hadoop@server:~$ source ~/.bashrc
hadoop@server:~$
```

```
  GNU nano 6.2                          /home/hadoop/hadoop/etc/hadoop/core-site.xml
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
<!--
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License. See accompanying LICENSE file.
-->

<!-- Put site-specific property overrides in this file. -->

<configuration>
        <property>
                <name>fs.defaultFS</name>
                <value>hdfs://hadoop.tecadmin.com:9000</value>
        </property>
</configuration>


                                        [ Read 24 lines ]
^G Help        ^O Write Out    ^W Where Is    ^K Cut        ^T Execute    ^C Location    M-U Undo
^X Exit        ^R Read File    ^\ Replace     ^U Paste      ^J Justify    ^/ Go To Line  M-E Redo
```

```
  GNU nano 6.2                          /home/hadoop/hadoop/etc/hadoop/yarn-site.xml
<?xml version="1.0"?>
<!--
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License. See accompanying LICENSE file.
-->
<configuration>
        <property>
                <name>yarn.nodemanager.aux-services</name>
                <value>mapreduce_shuffle</value>
        </property>
<!-- Site specific YARN configuration properties -->

</configuration>


                                        [ Wrote 22 lines ]
^G Help        ^O Write Out    ^W Where Is    ^K Cut        ^T Execute    ^C Location    M-U Undo
^X Exit        ^R Read File    ^\ Replace     ^U Paste      ^J Justify    ^/ Go To Line  M-E Redo
```

```
2022-12-31 14:20:01,233 INFO namenode.FSDirectory: XAttrs enabled? true
2022-12-31 14:20:01,233 INFO namenode.NameNode: Caching file names occurring more than 10 times
2022-12-31 14:20:01,237 INFO snapshot.SnapshotManager: Loaded config captureOpenFiles: false, skipCaptureAcce
meOnlyChange: false, snapshotDiffAllowSnapRootDescendant: true, maxSnapshotLimit: 65536
2022-12-31 14:20:01,239 INFO snapshot.SnapshotManager: SkipList is disabled
2022-12-31 14:20:01,242 INFO util.GSet: Computing capacity for map cachedBlocks
2022-12-31 14:20:01,242 INFO util.GSet: VM type       = 64-bit
2022-12-31 14:20:01,243 INFO util.GSet: 0.25% max memory 982 MB = 2.5 MB
2022-12-31 14:20:01,243 INFO util.GSet: capacity      = 2^18 = 262144 entries
2022-12-31 14:20:01,251 INFO metrics.TopMetrics: NNTop conf: dfs.namenode.top.window.num.buckets = 10
2022-12-31 14:20:01,251 INFO metrics.TopMetrics: NNTop conf: dfs.namenode.top.num.users = 10
2022-12-31 14:20:01,252 INFO metrics.TopMetrics: NNTop conf: dfs.namenode.top.windows.minutes = 1,5,25
2022-12-31 14:20:01,273 INFO namenode.FSNamesystem: Retry cache on namenode is enabled
2022-12-31 14:20:01,274 INFO namenode.FSNamesystem: Retry cache will use 0.03 of total heap and retry cache
 expiry time is 600000 millis
2022-12-31 14:20:01,276 INFO util.GSet: Computing capacity for map NameNodeRetryCache
2022-12-31 14:20:01,276 INFO util.GSet: VM type       = 64-bit
2022-12-31 14:20:01,277 INFO util.GSet: 0.029999999329447746% max memory 982 MB = 301.7 KB
2022-12-31 14:20:01,277 INFO util.GSet: capacity      = 2^15 = 32768 entries
2022-12-31 14:20:01,345 INFO namenode.FSImage: Allocated new BlockPoolId: BP-809035661-127.0.0.1-167249280131
2022-12-31 14:20:01,378 INFO common.Storage: Storage directory /home/hadoop/hadoopdata/hdfs/namenode has been
cessfully formatted.
2022-12-31 14:20:01,506 INFO namenode.FSImageFormatProtobuf: Saving image file /home/hadoop/hadoopdata/hdfs/n
ode/current/fsimage.ckpt_0000000000000000000 using no compression
2022-12-31 14:20:01,652 INFO namenode.FSImageFormatProtobuf: Image file /home/hadoop/hadoopdata/hdfs/namenode
rent/fsimage.ckpt_0000000000000000000 of size 401 bytes saved in 0 seconds .
2022-12-31 14:20:01,671 INFO namenode.NNStorageRetentionManager: Going to retain 1 images with txid >= 0
2022-12-31 14:20:01,696 INFO namenode.FSNamesystem: Stopping services started for active state
2022-12-31 14:20:01,700 INFO namenode.FSNamesystem: Stopping services started for standby state
2022-12-31 14:20:01,748 INFO namenode.FSImage: FSImageSaver clean checkpoint: txid=0 when meet shutdown.
2022-12-31 14:20:01,763 INFO namenode.NameNode: SHUTDOWN_MSG:
/************************************************************
SHUTDOWN_MSG: Shutting down NameNode at server.security-tp.com/127.0.0.1
************************************************************/
hadoop@server:~$
```

```
hadoop@server:~$ start-dfs.sh
Starting namenodes on [hadoop.tecadmin.com]
hadoop.tecadmin.com: ssh: connect to host hadoop.tecadmin.com port 22: Connection timed out
Starting datanodes
Starting secondary namenodes [server.security-tp.com]
server.security-tp.com: Warning: Permanently added 'server.security-tp.com' (ED25519) to the list of known hos
hadoop@server:~$ start-yarn.sh
Starting resourcemanager
Starting nodemanagers
hadoop@server:~$
```

```
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for dbus (1.12.20-2ubuntu4.1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
hadoop@server:~$ firewall-cmd --permanent --add-port=9870/tcp
Authorization failed.
    Make sure polkit agent is running or run the application as superuser.
hadoop@server:~$ sudo firewall-cmd --permanent --add-port=9870/tcp
success
hadoop@server:~$ sudo firewall-cmd --permanent --add-port=8088/tcp
success
hadoop@server:~$
```

```
hadoop@server:~$ sudo firewall-cmd --reload
success
```

```
hadoop@server:~$ jps
35248 ResourceManager
35024 SecondaryNameNode
35927 NameNode
35385 NodeManager
36095 DataNode
36383 Jps
hadoop@server:~$
```

Overview '10.0.2.15:9000' (✓active)

Started:	Sat Dec 31 15:21:33 +0100 2022
Version:	3.3.4, ra585a73c3e02ac62350c136643a5e7f6095a3dbb
Compiled:	Fri Jul 29 13:32:00 +0100 2022 by stevel from branch-3.3.4
Cluster ID:	CID-bda6260a-8c08-4001-8273-d8b260528e79
Block Pool ID:	BP-1917718720-127.0.0.1-1672494079554

Summary

Security is off.

Safemode is off.

1 files and directories, 0 blocks (0 replicated blocks, 0 erasure coded block groups) = 1 total filesystem object(s).

Heap Memory used 65.03 MB of 161 MB Heap Memory. Max Heap Memory is 982 MB.

Non Heap Memory used 49.73 MB of 53.63 MB Commited Non Heap Memory. Max Non Heap Memory is <unbounded>.

Configured Capacity:	23.94 GB
Configured Remote Capacity:	0 B
DFS Used:	24 KB (0%)
Non DFS Used:	13.62 GB
DFS Remaining:	9.08 GB (37.94%)
Block Pool Used:	24 KB (0%)
DataNodes usages% (Min/Median/Max/stdDev):	0.00% / 0.00% / 0.00% / 0.00%
Live Nodes	1 (Decommissioned: 0, In Maintenance: 0)


```
hadoop@server:~$ hdfs dfs -mkdir /test1
hadoop@server:~$ hdfs dfs -mkdir /logs
hadoop@server:~$ hdfs dfs -ls /
Found 2 items
drwxr-xr-x   - hadoop supergroup          0 2022-12-31 15:26 /logs
drwxr-xr-x   - hadoop supergroup          0 2022-12-31 15:25 /test1
hadoop@server:~$
```

ETAPE 4: Configurer un domaine Kerberos valide (KDC)

```
nadim@server:~$ systemctl status krb5-kdc
● krb5-kdc.service - Kerberos 5 Key Distribution Center
     Loaded: loaded (/lib/systemd/system/krb5-kdc.service; enabled; vendor pres>
     Active: active (running) since Sun 2023-02-19 18:59:56 WAT; 25min ago
   Main PID: 734 (krb5kdc)
      Tasks: 1 (limit: 4625)
     Memory: 1.6M
        CPU: 121ms
     CGroup: /system.slice/krb5-kdc.service
             └─734 /usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid

Warning: some journal files were not opened due to insufficient permissions.

nadim@server:~$ systemctl status krb5-admin-server
● krb5-admin-server.service - Kerberos 5 Admin Server
     Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; ve>
     Active: active (running) since Sun 2023-02-19 18:59:55 WAT; 26min ago
   Main PID: 666 (kadmind)
      Tasks: 1 (limit: 4625)
     Memory: 3.0M
        CPU: 117ms
     CGroup: /system.slice/krb5-admin-server.service
             └─666 /usr/sbin/kadmind -nofork
```

ETAPE 5: Connecter le serveur Hadoop à votre domaine Kerberos

```
                              hadoop@server: ~ 101x55
  GNU nano 6.2              /home/hadoop/hadoop/etc/hadoop/core-site.xml
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
<!--
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License. See accompanying LICENSE file.
-->

<!-- Put site-specific property overrides in this file. -->

<configuration>
        <property>
                <name>fs.defaultFS</name>
                <value>hdfs://10.0.2.15:9000</value>
        </property>
        <property>
                <name>hadoop.security.authentication</name>
                <value>kerberos</value>
        </property>
        <property>
                <name>hadoop.security.authorization</name>
                <value>true</value>
        </property>
</configuration>
```

```
  GNU nano 6.2                 /home/hadoop/hadoop/etc/hadoop/hadoop-env.sh *
# prefer any Xms setting in their respective _OPT variable.
# There is no default; the JVM will autoscale based upon machine
# memory size.
# export HADOOP_HEAPSIZE_MIN=

# Enable extra debugging of Hadoop's JAAS binding, used to set up
# Kerberos security.
# export HADOOP_JAAS_DEBUG=true

# Extra Java runtime options for all Hadoop commands. We don't support
# IPv6 yet/still, so by default the preference is set to IPv4.
# export HADOOP_OPTS="-Djava.net.preferIPv4Stack=true"
# For Kerberos debugging, an extended option set logs more information
# export HADOOP_OPTS="-Djava.net.preferIPv4Stack=true -Dsun.security.krb5.debug=true -Dsun.security.>
export HADOOP_OPTS="$HADOOP_OPTS -Djava.security.auth.login.config=/path/to/hadoop/conf/hadoop-jaas.>

# Some parts of the shell code may do special things dependent upon
# the operating system.  We have to set this here. See the next
# section as to why....
export HADOOP_OS_TYPE=${HADOOP_OS_TYPE:-$(uname -s)}

# Extra Java runtime options for some Hadoop commands
# and clients (i.e., hdfs dfs -blah).  These get appended to HADOOP_OPTS for

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo
```

```
hadoop@server:~$ sudo kadmin.local
Authenticating as principal root/admin@SECURITY-TP.COM with password.
kadmin.local:   addprinc -randkey hadoop/server.security-tp.com@SECURITY-TP.COM
No policy specified for hadoop/server.security-tp.com@SECURITY-TP.COM; defaulting to no policy
Principal "hadoop/server.security-tp.com@SECURITY-TP.COM" created.
kadmin.local:   xst -k /path/to/hadoop.keytab hadoop/server.security-tp.com@SECURITY-TP.COM
kadmin.local: Key table file '/path/to/hadoop.keytab' not found while adding key to keytab
kadmin.local:   xst -k /home/hadoop/hadoop/etc/hadoop/hadoop.keytab hadoop/server.security-tp.com@SECU
RITY-TP.COM
Entry for principal hadoop/server.security-tp.com@SECURITY-TP.COM with kvno 3, encryption type aes256
-cts-hmac-sha1-96 added to keytab WRFILE:/home/hadoop/hadoop/etc/hadoop/hadoop.keytab.
Entry for principal hadoop/server.security-tp.com@SECURITY-TP.COM with kvno 3, encryption type aes128
-cts-hmac-sha1-96 added to keytab WRFILE:/home/hadoop/hadoop/etc/hadoop/hadoop.keytab.
```

```
hadoop@server:~$ stop-all.sh
WARNING: Stopping all Apache Hadoop daemons as hadoop in 10 seconds.
WARNING: Use CTRL-C to abort.
Stopping namenodes on [10.0.2.15]
Stopping datanodes
Stopping secondary namenodes [server.security-tp.com]
Stopping nodemanagers
Stopping resourcemanager
```

ETAPE 6: Créer plusieurs utilisateurs dans le domaine Kerberos, et mettre en place des droits différents sur Hadoop

```
hadoop@server:~$ sudo kadmin.local -q "addprinc user1"
Authenticating as principal root/admin@SECURITY-TP.COM with password.
No policy specified for user1@SECURITY-TP.COM; defaulting to no policy
Enter password for principal "user1@SECURITY-TP.COM":
Re-enter password for principal "user1@SECURITY-TP.COM":
Principal "user1@SECURITY-TP.COM" created.
hadoop@server:~$ sudo kadmin.local -q "addprinc user2"
Authenticating as principal root/admin@SECURITY-TP.COM with password.
No policy specified for user2@SECURITY-TP.COM; defaulting to no policy
Enter password for principal "user2@SECURITY-TP.COM":
Re-enter password for principal "user2@SECURITY-TP.COM":
Principal "user2@SECURITY-TP.COM" created.
hadoop@server:~$ sudo kadmin.local -q "addprinc user3"
Authenticating as principal root/admin@SECURITY-TP.COM with password.
No policy specified for user3@SECURITY-TP.COM; defaulting to no policy
Enter password for principal "user3@SECURITY-TP.COM":
Re-enter password for principal "user3@SECURITY-TP.COM":
Principal "user3@SECURITY-TP.COM" created.
```

```
hadoop@server:~$ hdfs dfs -setfacl -m user:user1:rwx /test
hadoop@server:~$ hdfs dfs -setfacl -x user:user2 /test
```

ETAPE 7: Vérifier que la liaison fonctionne correctement et retourner un cas simple : hadoop fs -ls

```
hadoop@server:~$ hdfs dfs -getfacl /test
# file: /test
# owner: hadoop
# group: supergroup
user::rwx
user:user1:rwx
group::r-x
mask::rwx
other::r-x
```

```
hadoop@server:~$ hadoop fs -ls /
Found 1 items
drwxrwxr-x+   - hadoop supergroup          0 2023-02-19 22:01 /test
```

PARTIE BONUS : Schéma de l'architecture