NC STATE UNIVERSITY Computer Science

Insights to Hadoop Security Threats

Presenter:
Anwesha Das
Peipei Wang

Outline

- Attacks
  - DOS attack - Rate Limiting
  - Impersonation
- Implementation
  - Sandbox HDP version 2.1
  - Cluster Set-up
  - Kerberos Security Setup
- Insights
- Conclusion

Motivation

User Reviews In Bug Repository

Make NameNode resilient to DoS attacks (malicious or otherwise)
defective applications cause havoc on the NameNode, for e.g. by doing 100k+ 'listStatus' on very large directories (60k files) etc
It seems there are a number of DoS scenarios to worry about:

RPC flooding (as you noted above)
Malformed packets (it's probably not too hard to find a spot where you can make the NN allocate way too much memory and crash some important thread)
Open socket limit exhaustion - what if a client just opened thousands of connections to the NN's RPC ports without actually sending commands? At some point you'll hit the ulimit -n
lots of others

solutions- 1: Any type of rate-limiting should be either optional or configurable on per-application basis. rate-limiting——QoS reservation
2.apps within trusted network that does not need to be paranoid about this——ignore this problem

3. focus on detection of such attacks and counter acts with, say, iptables filtering to cut off an intruder or an honest fool.———detection

Motivation

HADOOP-9194—duplicated with HDFS-945------2.1.0-beta(fixed)----2.0.2-alpha(affected)
Hadoop performance is QoS (Quality of Service)
RPC Support for QoS
----HDFS has a separate port for "service" IPC, allows you do to port-based QOS (see HDFS-599)
Dos attack on server communication ports: hdfs, name node, datanode…(what is a secure port??)
HADOOP-9640-------Enable optional RPC-level priority to combat congestion and make request latencies more consistent.
RPC Congestion Control with FairCallQueue
replacing the FIFO call queue with a Fair Call Queue

Attacks

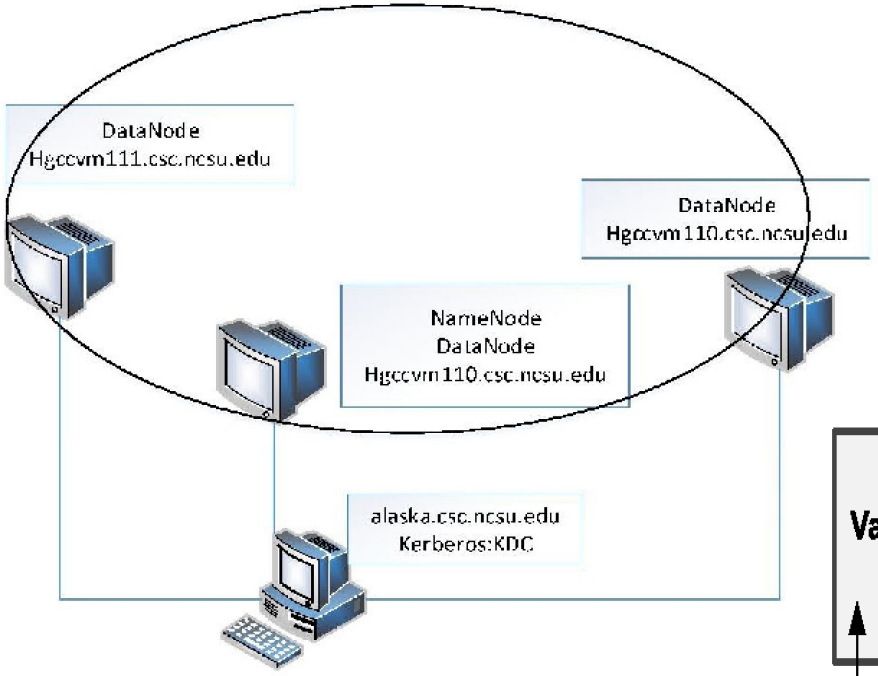
- DOS attack - Rate Limit
  - RPC Congestion Failure
- Impersonation
  - How to impersonate?
  - Figured out a way, could not evaluate it
  - HDFS access

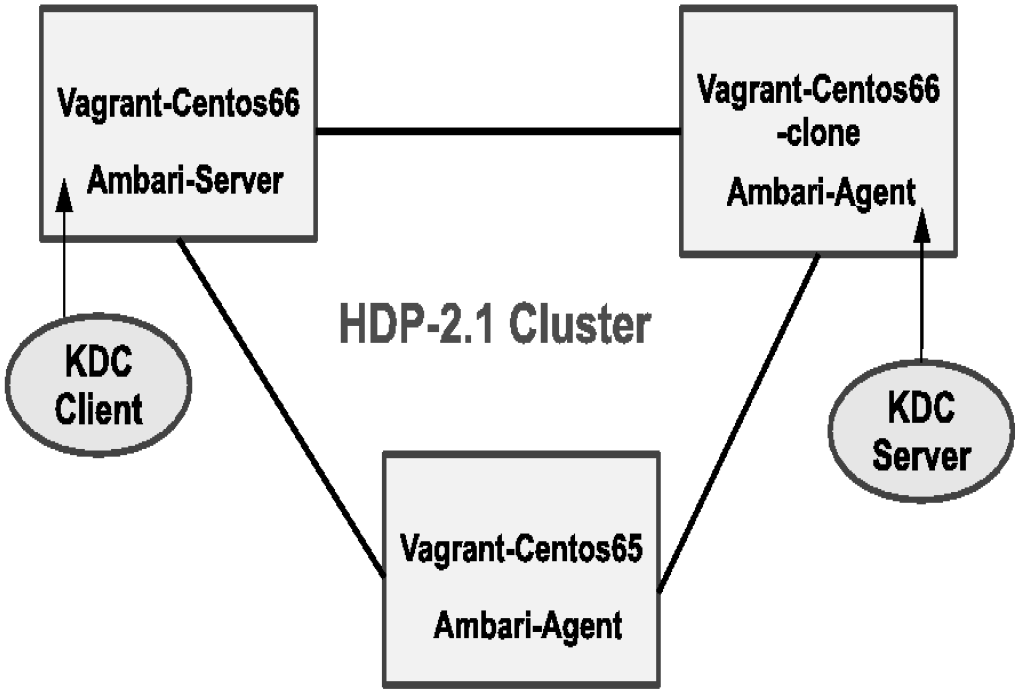
Implementation

- Sandbox HDP-2.1 - Provider *HortonWorks*
  - Cluster setup of 3 VM on virtual-box
  - CentOS Installed
  - Ambari Configuration
  - Kerberos Enabled Cluster

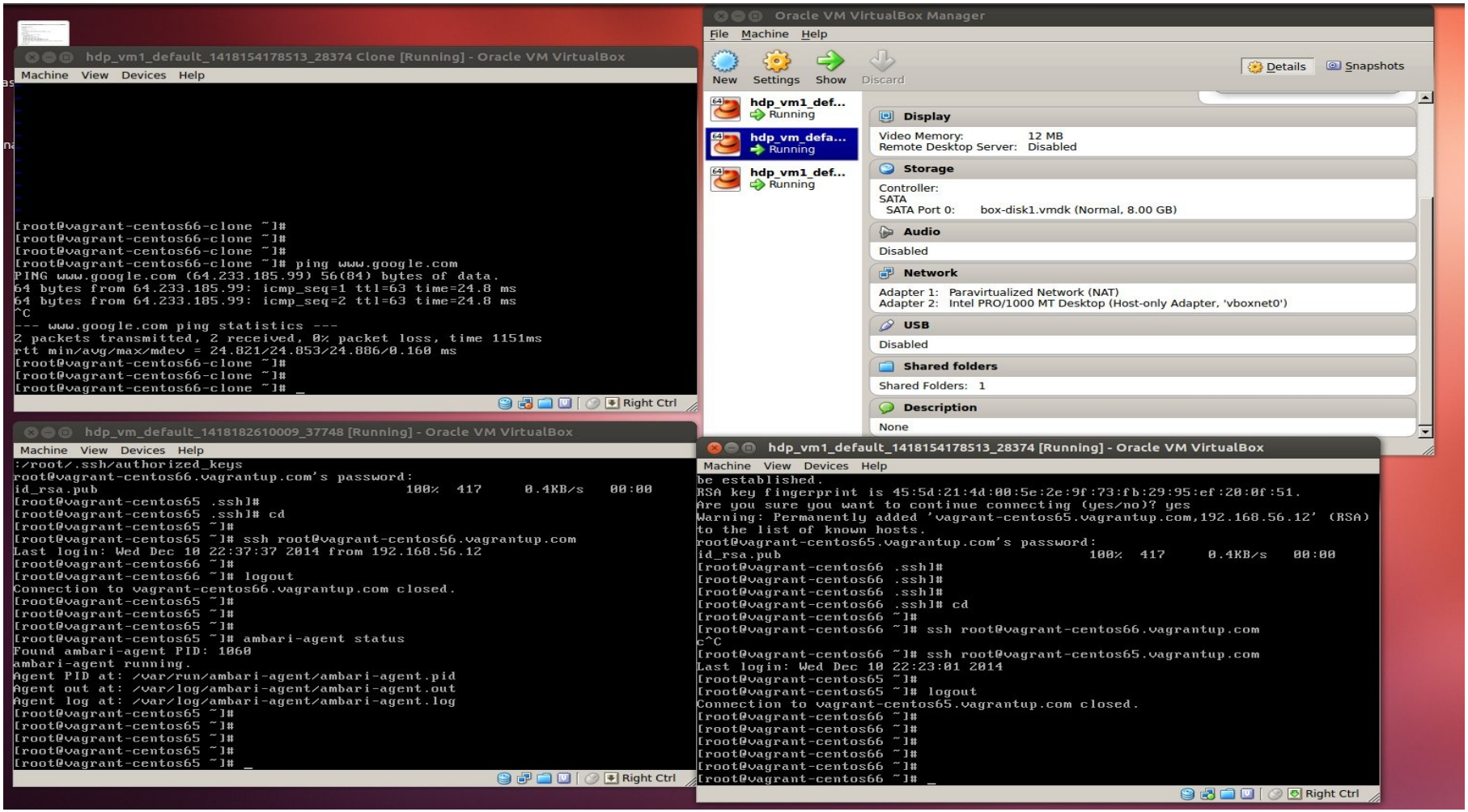
- Hadoop-2.5.0, Hadoop-1.2.1
  - 3 Hgcc nodes, 2 VMs each
  - Ubuntu 10.04
  - Separate KDC node

Setup


DataNode
Hgccvm111.csc.ncsu.edu
DataNode
Hgccvm110.csc.ncsu.edu
NameNode
DataNode
Hgccvm110.csc.ncsu.edu
alaska.csc.ncsu.edu
Kerberos:KDC


Vagrant-Centos66
Ambari-Server
Vagrant-Centos66
-clone
Ambari-Agent
HDP-2.1 Cluster
KDC
Client
KDC
Server
Vagrant-Centos65
Ambari-Agent

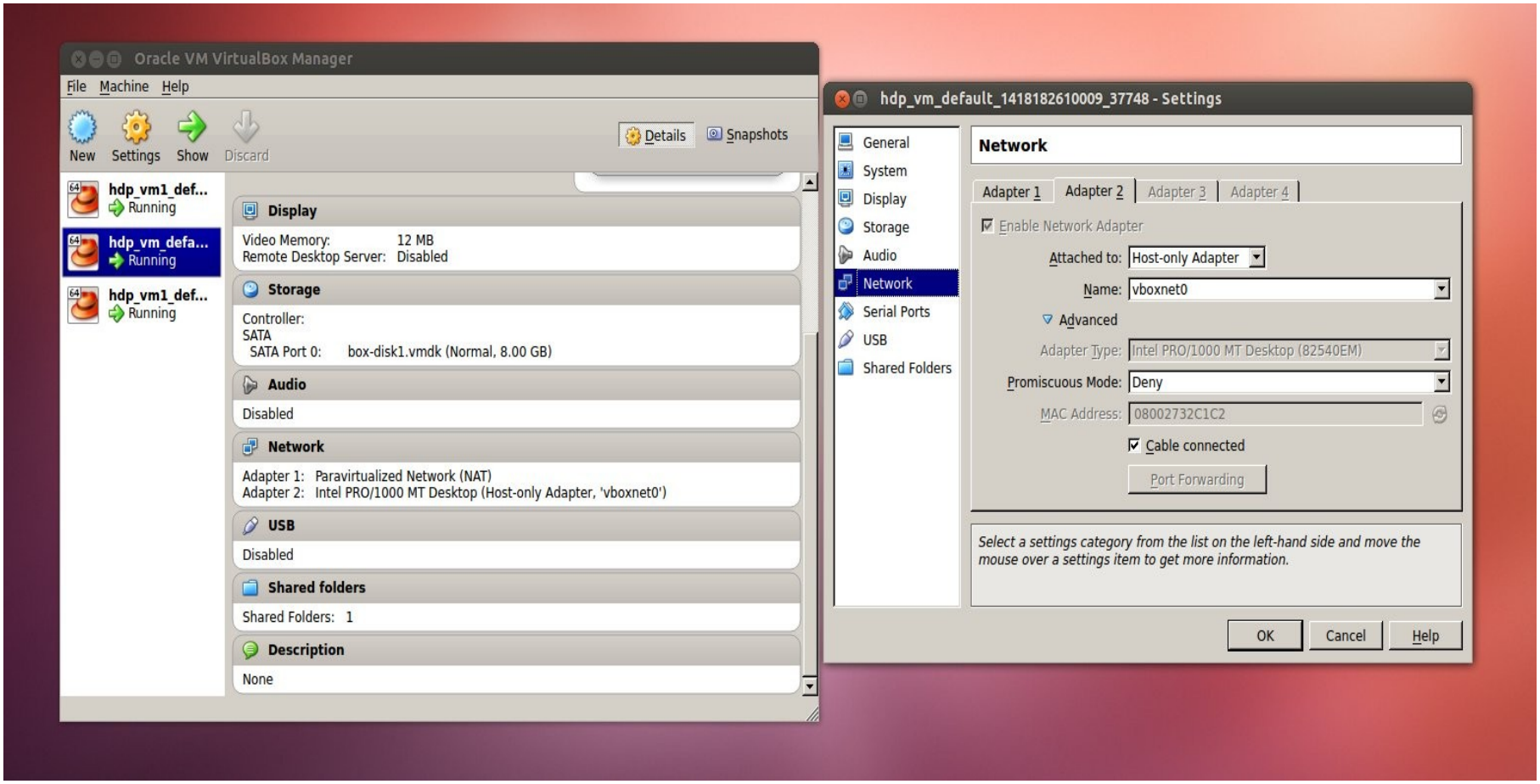
Sandbox


hdp_vm1_default_1418154178513_28374 Clone [Running] - Oracle VM VirtualBox
Machine View Devices Help
[root@vagrant-centos66-clone ~]#
[root@vagrant-centos66-clone ~]#
[root@vagrant-centos66-clone ~]#
[root@vagrant-centos66-clone ~]# ping www.google.com
PING www.google.com (64.233.185.99) 56(84) bytes of data.
64 bytes from 64.233.185.99: icmp_seq=1 ttl=63 time=24.8 ms
64 bytes from 64.233.185.99: icmp_seq=2 ttl=63 time=24.8 ms
^C
--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1151ms
rtt min/avg/max/mdev = 24.821/24.853/24.886/0.160 ms
[root@vagrant-centos66-clone ~]#
[root@vagrant-centos66-clone ~]#
[root@vagrant-centos66-clone ~]#
Right Ctrl
Oracle VM VirtualBox Manager
File Machine Help
New Settings Show Discard
Details Snapshots
hdp_vm1_def... Running
hdp_vm_defa... Running
hdp_vm1_def... Running
Display
Video Memory: 12 MB
Remote Desktop Server: Disabled
Storage
Controller: SATA
SATA Port 0: box-disk1.vmdk (Normal, 8.00 GB)
Audio
Disabled
Network
Adapter 1: Paravirtualized Network (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')
USB
Disabled
Shared folders
Shared Folders: 1
Description
None
hdp_vm_default_1418182610009_37748 [Running] - Oracle VM VirtualBox
Machine View Devices Help
:/root/.ssh/authorized_keys
root@vagrant-centos66.vagrantup.com's password:
id_rsa.pub 100% 417 0.4KB/s 00:00
[root@vagrant-centos65 .ssh]#
[root@vagrant-centos65 .ssh]# cd
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]# ssh root@vagrant-centos66.vagrantup.com
Last login: Wed Dec 10 22:37:37 2014 from 192.168.56.12
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]# logout
Connection to vagrant-centos66.vagrantup.com closed.
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]# ambari-agent status
Found ambari-agent PID: 1060
ambari-agent running.
Agent PID at: /var/run/ambari-agent/ambari-agent.pid
Agent out at: /var/log/ambari-agent/ambari-agent.out
Agent log at: /var/log/ambari-agent/ambari-agent.log
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]#
Right Ctrl
hdp_vm1_default_1418154178513_28374 [Running] - Oracle VM VirtualBox
Machine View Devices Help
be established.
RSA key fingerprint is 45:5d:21:4d:00:5e:2e:9f:73:fb:29:95:ef:20:0f:51.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'vagrant-centos65.vagrantup.com,192.168.56.12' (RSA)
to the list of known hosts.
root@vagrant-centos65.vagrantup.com's password:
id_rsa.pub 100% 417 0.4KB/s 00:00
[root@vagrant-centos66 .ssh]#
[root@vagrant-centos66 .ssh]#
[root@vagrant-centos66 .ssh]#
[root@vagrant-centos66 .ssh]# cd
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]# ssh root@vagrant-centos66.vagrantup.com
c^C
[root@vagrant-centos66 ~]# ssh root@vagrant-centos65.vagrantup.com
Last login: Wed Dec 10 22:23:01 2014
[root@vagrant-centos65 ~]#
[root@vagrant-centos65 ~]# logout
Connection to vagrant-centos65.vagrantup.com closed.
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]#
[root@vagrant-centos66 ~]#
Right Ctrl

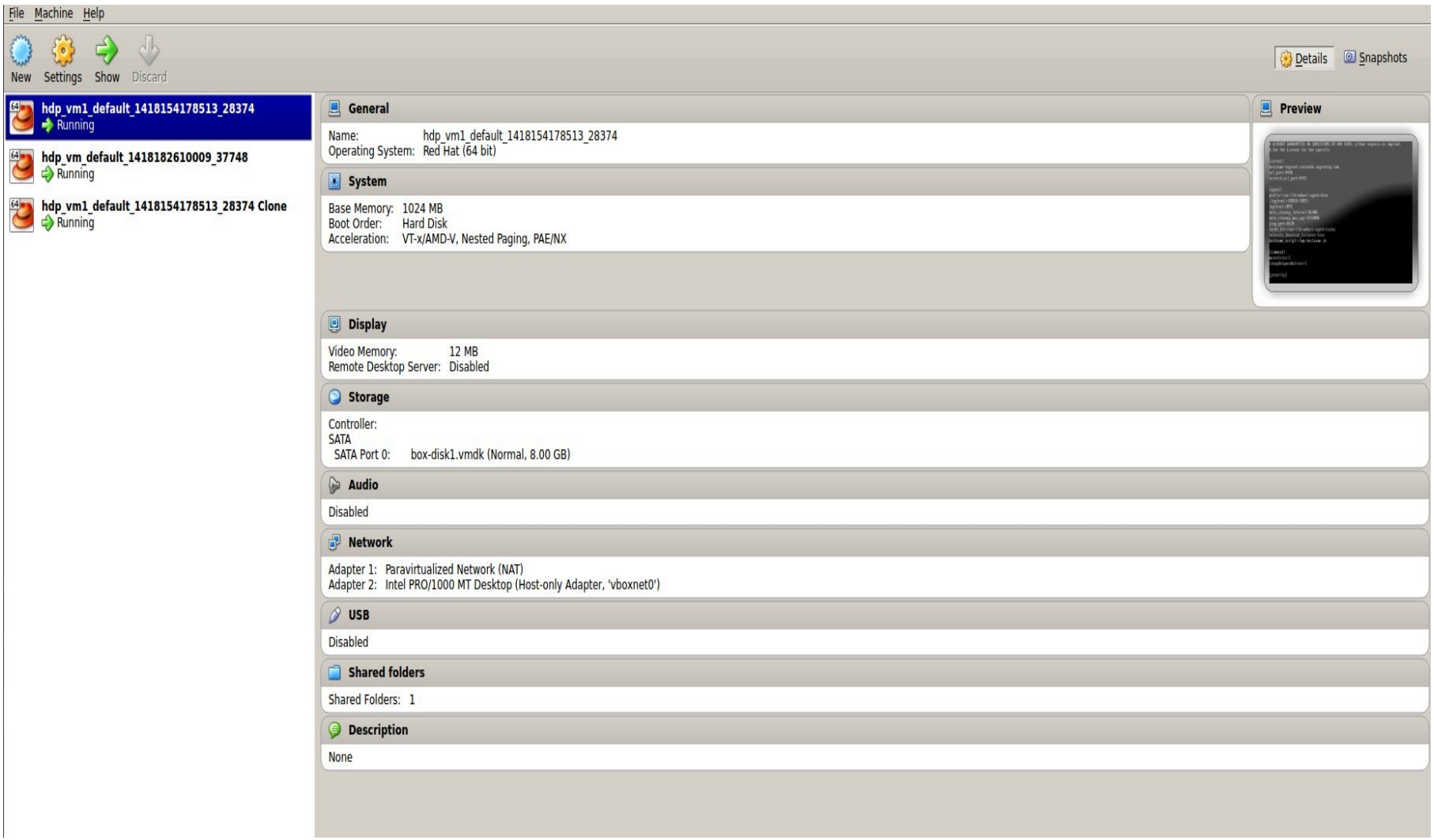
Sandbox

```
[server]
hostname=vagrant-centos66.vagrantup.com
url_port=8440
secured_url_port=8441

[agent]
prefix=/var/lib/ambari-agent/data
;loglevel=(DEBUG/INFO)
loglevel=INFO
data_cleanup_interval=86400
data_cleanup_max_age=2592000
ping_port=8670
cache_dir=/var/lib/ambari-agent/cache
tolerate_download_failures=true
hostname_script=/tmp/hostname.sh

[command]
maxretries=2
sleepBetweenRetries=1

[security]
```

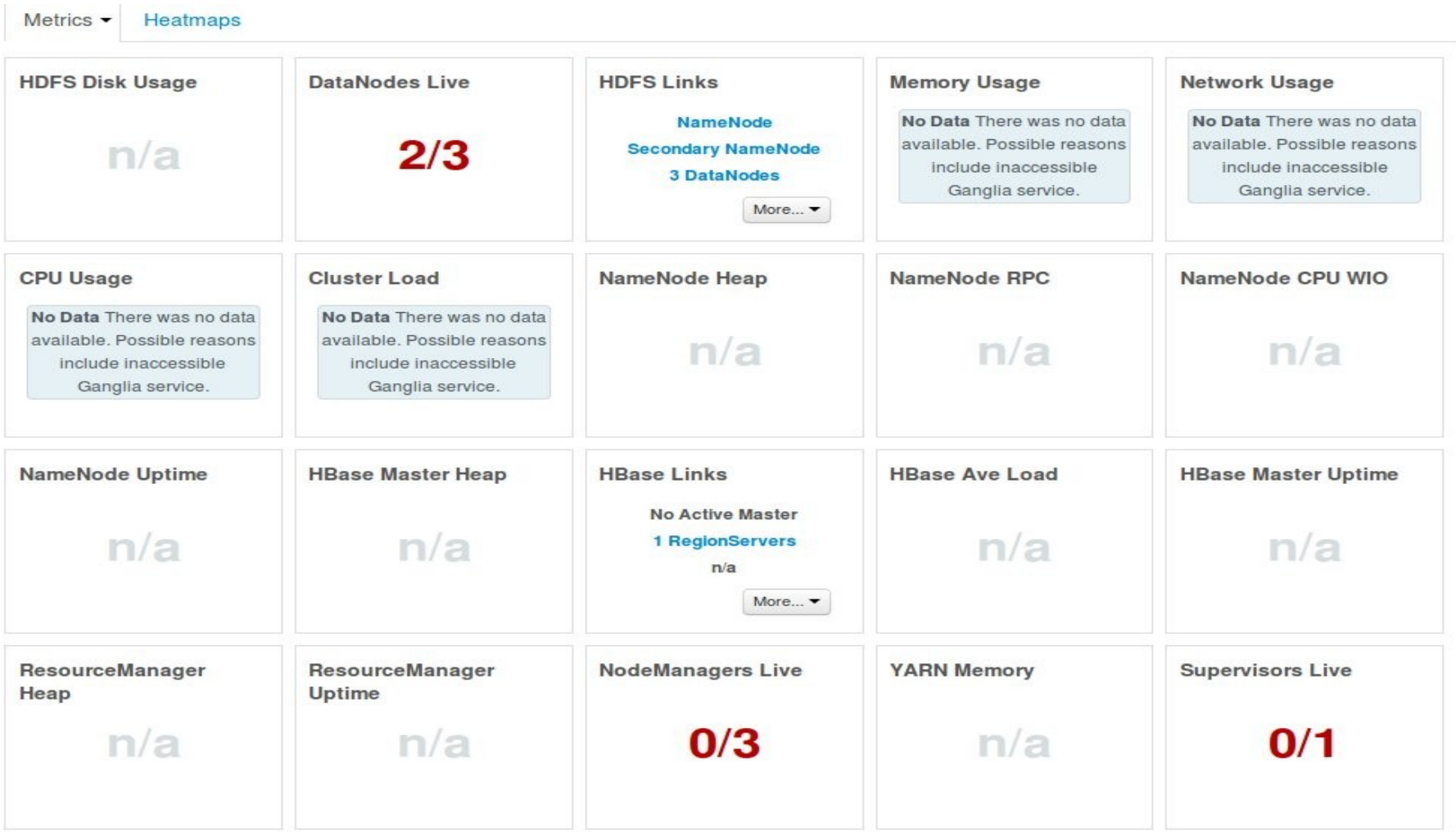
Sandbox


Oracle VM VirtualBox Manager
File Machine Help
New Settings Show Discard
Details Snapshots
hdp_vm1_def... Running
hdp_vm_defa... Running
hdp_vm1_def... Running
Display
Video Memory: 12 MB
Remote Desktop Server: Disabled
Storage
Controller: SATA
SATA Port 0: box-disk1.vmdk (Normal, 8.00 GB)
Audio
Disabled
Network
Adapter 1: Paravirtualized Network (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')
USB
Disabled
Shared folders
Shared Folders: 1
Description
None
hdp_vm_default_1418182610009_37748 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Network
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to: Host-only Adapter
Name: vboxnet0
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 08002732C1C2
Cable connected
Port Forwarding
Select a settings category from the list on the left-hand side and move the mouse over a settings item to get more information.
OK Cancel Help

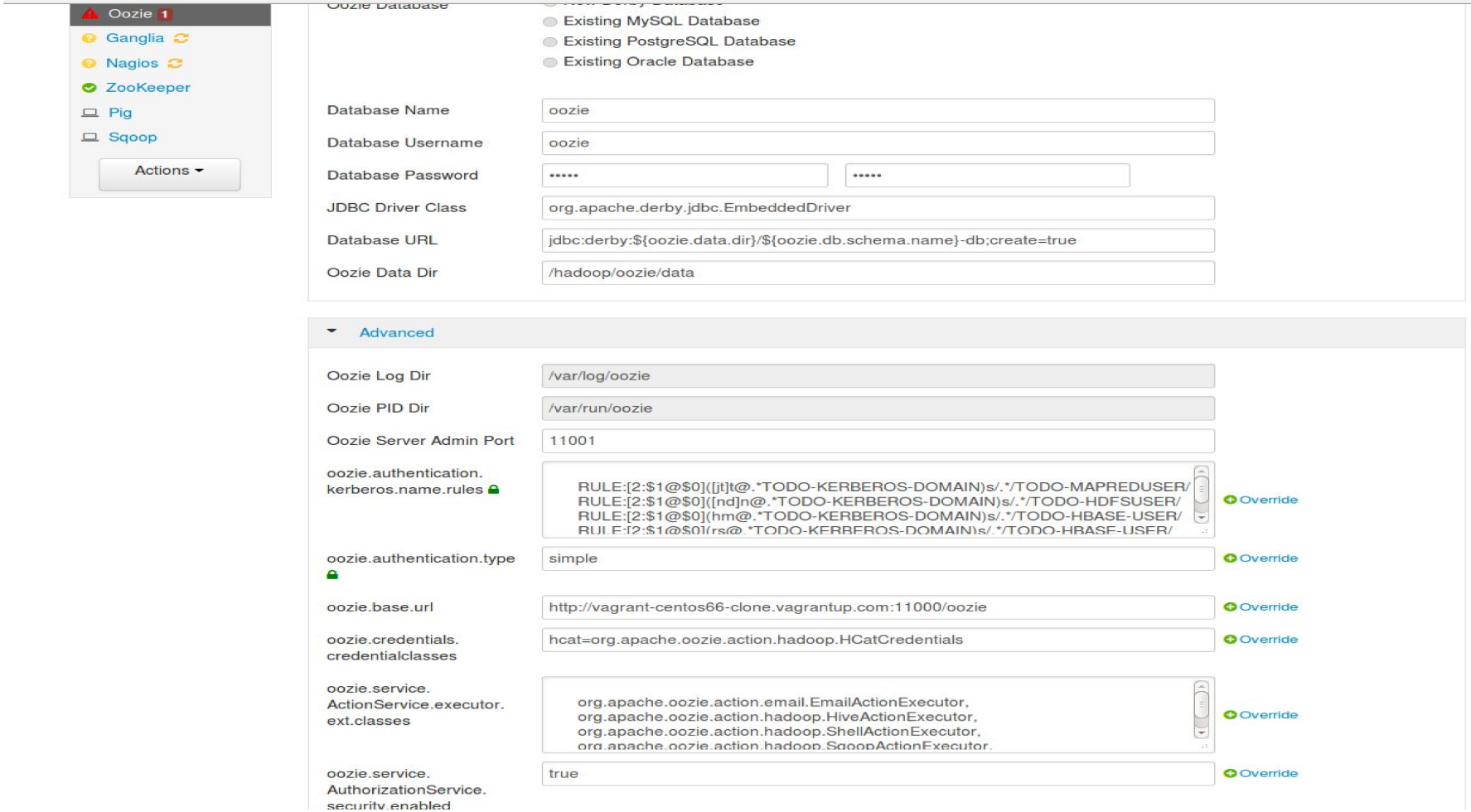
Sandbox


File Machine Help
New Settings Show Discard
Details Snapshots
hdp_vm1_default_1418154178513_28374
Running
hdp_vm_default_1418182610009_37748
Running
hdp_vm1_default_1418154178513_28374 Clone
Running
General
Name: hdp_vm1_default_1418154178513_28374
Operating System: Red Hat (64 bit)
Preview
System
Base Memory: 1024 MB
Boot Order: Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX
Display
Video Memory: 12 MB
Remote Desktop Server: Disabled
Storage
Controller:
SATA
SATA Port 0: box-disk1.vmdk (Normal, 8.00 GB)
Audio
Disabled
Network
Adapter 1: Paravirtualized Network (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')
USB
Disabled
Shared folders
Shared Folders: 1
Description
None

Sandbox Ambari



Security/Oozie



Rate Limiting

-rw-r--r--	peipei	supergroup	12.72 KB	3	128 MB	69998
-rw-r--r--	peipei	supergroup	12.72 KB	3	128 MB	69999
-rw-r--r--	peipei	supergroup	12.72 KB	3	128 MB	7
-rw-r--r--	peipei	supergroup	12.72 KB	3	128 MB	70
-rw-r--r--	peipei	supergroup	12.72 KB	3	128 MB	700

- 70000 files created for RPC Congestion
- Commands used: dfs -lsr, fsck
- 10 rounds, 13 secs, 12 secs respectively
- Failure in both Hadoop-1.2.1, Hadoop-2.5.0

Kerberos Tests

- 2 Tests made:
- Hadoop client without kerberos to access HDFS. HDFS recognized this illegal operation in its output messages.

peipei@ubuntu10045:~/hadoop-2.5.0/bin$ ./hadoop dfs -ls hdfs://10.76.2.127:9000/
DEPRECATED: Use of this script to execute hdfs command is deprecated.
Instead use the hdfs command for it.

14/12/01 16:25:31 WARN util.KerberosName: Kerberos krb5 configuration not found, setting default realm to empty
ls: Authorization (hadoop.security.authorization) is enabled but authentication (hadoop.security.authentication) is configured as simple. Please configure another method like kerberos or digest.

Kerberos Tests

- Client access in a Hadoop cluster with a kerberos enabled Datanode which is not predefined in Hadoop cluster. Hadoop does not allow nodes to join Hadoop cluster randomly. It requires the user principals to be added before joining it:

```
2014-12-01 18:40:29,887 INFO
org.apache.hadoop.ipc.Server: IPC Server listener on
9000: readAndProcess threw exception
org.apache.hadoop.security.AccessControlException:
Connection from 152.14.92.184:53152 for protocol
org.apache.hadoop.hdfs.server.protocol.DatanodeProtocol
is unauthorized for user peipei/peipei-optiplex-
9010@HADOOP.DOMAIN (auth:KERBEROS) from client
152.14.92.184. Count of bytes read: 0
```

Kerberos Pain

- Problems in creating Kerberos principal Database
  - Program hangs in “Loading Random Data”
- Fully Qualified Domain Names(FQDN) needed for kerberos authentication
- Kerberos enabled DataNodes needs to be started with root and jsvc
- Slow running hadoop cluster
  - KDC and hadoop cluster under different subnet
  - Lumpy Kerberos Authentication??

Hard to start secure datanode

DataNode

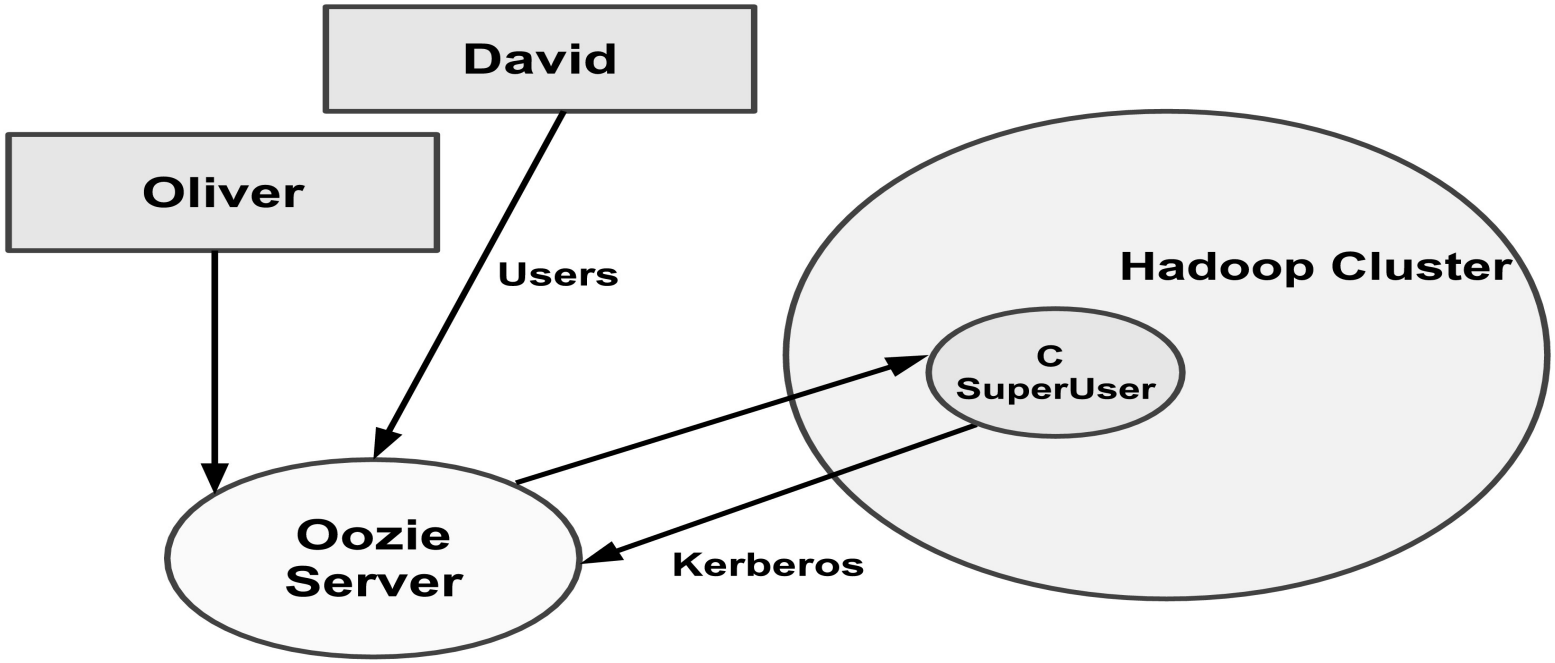
Configuration for `conf/hdfs-site.xml`

Parameter	Value	Notes
dfs.datanode.data.dir.perm	700	
dfs.datanode.address	*0.0.0.0:1004*	Secure DataNode must use privileged port in order to assure that the server was started securely. This means that the server must be started via jsvc.
dfs.datanode.http.address	*0.0.0.0:1006*	Secure DataNode must use privileged port in order to assure that the server was started securely. This means that the server must be started via jsvc.
dfs.datanode.https.address	*0.0.0.0:50470*	
dfs.datanode.keytab.file	*/etc/security/keytab/dn.service.keytab*	Kerberos keytab file for the DataNode.
dfs.datanode.kerberos.principal	dn/_HOST@REALM.TLD	Kerberos principal name for the DataNode.
dfs.datanode.kerberos.https.principal	host/_HOST@REALM.TLD	HTTPS Kerberos principal name for the DataNode.
dfs.encrypt.data.transfer	*false*	set to `true` when using data encryption

- Use root privilege and jsvc to start secure data node
- Jsvc – separate installation needed, absent in jdk

Oozie

Oozie Impersonation



Conclusions

- Kerberos – fit for simple authentication
- Kerberos – Painful Deployment

- Third party vendor – easier deployment
- Degraded performance in a Virtualized cluster
- Oozie Impersonation
- Commercial Product HDP or Hadoop specific tightly coupled authentication better choice than Kerberos like third party software

- Sandbox or Hadoop native cluster ?? Sandbox

Thank you