Followed the steps to get access to Dev and stage Linux servers:

1. Log service desk ticket for AD creation under cca-audit account

* Username should be followed as firstname.lastname [suprija.sirikonda]

1. Service desk ticket  to add created user  to norgenrdsstg.ccaintranet.com
2. Service desk ticket for Access to the AD groups for new User for below groups

* entdev\_developers\_dev
* shell\_hdp\_access\_dev
* shell\_hdp\_access\_stg
* rdp\_norgenrdsstg
* rdp\_tsdev2
* users\_analyticsdev

With these groups will get access to below servers:

* norgenhdpdev01
* norgenhdpdev02
* norgenhdpdev04
* norgenhdpstg02

1. dzdo access to svcdwsexecute on  norgenhdpdev01,norgenhdpdev02

**Export and import enterprise Root certificates:**

🡪Certificate needs to be exported and imported on the system where these scripts are running.

Steps to be followed:

1. Enterprise Root Certificate Export Steps:

* Click on Start -> Run in windows machine and then type mmc
* Go to File -> Add/Remove Snap-in
* Select “Certificates” on the left column and click on “Add” button
* Select “Computer account” and click on “OK” button
* Click “Trusted Root Certificate Authorities” - > “Certificates” on the

left column

* Find the certificate with both “Issued To” and “Issued By” of “Connolly Enterprise Root CA 2009-11” and with “Expiration Date” of “10/18/2030”
* Right click on it and select “All Tasks” -> “Export”
* Click “Next”
* Select “DER encoded binary X.509 (.CER) and click on “Next”
* Click “Browse” to pick a path to save the certificate and then click on “Next”
* Click “Finish”

Then we should see message as "The export was Successful"

2. Enterprise Root Certificate Import Steps:

Prerequisite: enterprise root certificate is exported and saved.

* Steps to Validate the root certificate content:

Ensure that the Java keytool can parse the certificate and display its content with below command

keytool -v -printcert -file "C:\Certificates\Connolly Enterprise Root CA 2009-11.cer"

In Ubuntu:

* Copied the .cer file to Desktop.
* Import the root certificate into the JVM trust store:

The Java certificate store location depends on your Java installation, e.g. to /usr/lib/jvm/java-8-oracle/;

for -alias pick some unique name for the certificate in the store with below command

keytool -importcert -alias cotiviti -keystore "/usr/lib/jvm/java-8-oracle/jre/lib/security/cacerts" -storepass changeit -file "/home/suprija/desktop/Connolly Enterprise Root CA 2009-11.cer"

(the default password for the CA store is changeit)

The keytool will prompt you for confirmation, enter yes to complete the operation.

* Verify that the root certificate has been imported:

(To do that list the trust store content and filter for the certificate alias (name) with grep)

Command: keytool -keystore "/usr/lib/jvm/java-8-oracle/jre/lib/security/cacerts" -storepass changeit -list |grep cotiviti

* You will now be able to make secure SSL/TLS connections to servers which have a certificate signed by the CA which we just imported.

Note: This is one-time activity on a machine, not required to do these steps for every execution

**Generate keytab:**

In dev01,

cd /opt/abinitio/bin

ksh configure\_user\_dev.ksh (Run the script)

In dev02,

kinit <your name>@CCAINTRANET.COM -k -t /home/<your name>/<your name>.keytab

(Java Kerberos Client doc)