ECA – Linux Development Desktop Build - Ansible Build

|  |
| --- |
|  |
| * Version: 0.9 (Draft) * INTERNAL |
|  |

|  |  |
| --- | --- |
| Document control | |
|  |  |
|  |  |
| |  |  | | --- | --- | | **Author** | Steven Eyre | | **Owner** | Andrew Raison | | **Approved by** | Paul Gabriel | | **Approval date** |  | | **Effective from** |  | | **Next review date** |  | | **Source location** |  | | **Audience** | IT department | | |

|  |  |
| --- | --- |
| Change history | |
|  |  |
|  |  |
| |  |  |  |  | | --- | --- | --- | --- | | Version | Date | Amended by | Details | | 0.1 | 25/11/2019 | Steven Eyre | First draft | | 0.5 | 15/01/2020 | Steven Eyre | Updates for changed disk layout/sizing | | 0.7 | 03/02/2020 | Steven Eyre | Corrected screenshots + added placeholders for Firewall screenshots. | | 0.8 | 20/02/2020 | Steven Eyre | Updated network configuration | | 0.9 | 24/02/2020 | Steven Eyre | Added ECA Active Directory | | |

Contents

[Introduction 3](#_Toc33706566)

[Overview 3](#_Toc33706567)

[Purpose/Scope 3](#_Toc33706568)

[Procedure 4](#_Toc33706569)

[Description 4](#_Toc33706570)

[Assumptions 4](#_Toc33706571)

[Centos Install Pre-Requisites 4](#_Toc33706572)

[Server Build 5](#_Toc33706573)

[Hyper-V – Create VM 5](#_Toc33706574)

[SOFTWARE 15](#_Toc33706575)

[DISK LAYOUT 17](#_Toc33706576)

[Linux Install, System, INSTALLATION DESTINATION *sda / 32 GiB free* 18](#_Toc33706577)

[Select the / partition – and change its size down to 17.1 Gib 21](#_Toc33706578)

[Now add the additional mountpoints as below using the + symbol at bottom of the Layout 23](#_Toc33706579)

[/home – 9GB 23](#_Toc33706580)

[/etc/ECA - 1.5G 24](#_Toc33706581)

[Final Layout should look same as below 25](#_Toc33706582)

[NETWORK 27](#_Toc33706583)

[Linux Install, Network and Hostname 28](#_Toc33706584)

[ANSIBLE PLAYBOOK 36](#_Toc33706585)

[What is Ansible ? 36](#_Toc33706586)

[ADD SSH KEY FROM SPACEWALK SERVER 36](#_Toc33706587)

[On the Spacewalk Server 36](#_Toc33706588)

[On the Target/newly built Server 36](#_Toc33706589)

[TEST SSH WORKS FROM SPACEWALK SERVER TO TARGET SERVER 38](#_Toc33706590)

[TEMPORARILY ENABLE INTERNET ACCESS FOR NEW BUILT SERVER(S) 38](#_Toc33706591)

[RUN ANSIBLE-PLAYBOOK FROM SPACEWALK SERVER TO TARGET SERVER 38](#_Toc33706592)

[ACTIVE-DIRECTORY 43](#_Toc33706593)

[On the Target host 43](#_Toc33706594)

[PATCH SERVER 46](#_Toc33706595)

[USEFUL LINKS 47](#_Toc33706596)

[CENTOS (Operating System) 47](#_Toc33706597)

[SPACEWALK (OS Provisioning/Patching) 47](#_Toc33706598)

[ANSIBLE (Configuration Management software) 47](#_Toc33706599)

|  |  |
| --- | --- |
| Introduction | |
|  |  |
|  |  |
| Overview ECA brought in-house the StarRate development environment. This necessitates several Linux Servers (Both Desktop/Gnome and management servers be built. Previously builds were by hand/knowledge specific to Starrate  This document covers an semi-automated build to ECA/industry standards on ECA hardware. Purpose/Scope Step by Step build procedure for Linux Desktop using Ansible playbooks for final configuration | |

|  |
| --- |
| Procedure |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Description ***Centos*** *is an open source Linux distribution* [*https://www.centos.org/*](https://www.centos.org/) *. It is derived from* [*Red Hat Enterprise Linyx (RHEL)*](https://www.centos.org/)  *sources.*  Since March 2004, CentOS Linux has been a community-supported distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with RHEL. We mainly change packages to remove upstream vendor branding and artwork. CentOS Linux is no-cost and [free to redistribute](https://www.centos.org/legal). Assumptions While this document covers the build/maintenance procedures – below assumptions are made:   1. A broad understanding of IT standards/methodologies. 2. Basic Linux administration skills. 3. Familiarity with ECA procedure and standards.  Centos Install Pre-Requisites **[URL]** [**https://github.com/spacewalkproject/spacewalk/wiki/HowToInstall**](https://github.com/spacewalkproject/spacewalk/wiki/HowToInstall)  **SERVER SPECS**   * Hyper V VM * 1-2CPU * 2GB RAM minimum, 6GB recommended * 32GB Disk for OS/Root * Centos 7.8 DVD/ISO (*or later iteration if available*)   + **[URL]** [**Centos Download**](https://www.centos.org/download/) * Make sure your underlying OS is fully up-to-date (build from DVD should suffice)   **FIREWALL/PORTS**   * Outbound open ports 80, 443   **SOFTWARE REPOSITORIES**  Check re DVD and OS   |  |  | | --- | --- | | **repo id** | **Repo name** | | centos\_7\_patch | Centos\_7\_Patch | |  |  |  |  |  | | --- | --- | | Server Build | | |  |  | |  |  |  Hyper-V – Create VM Each server requires a new VM creating on the HyperV platform **(lnvh7.eca-international.local)**.  **Remote Desktop to the server:**    **Server Manager**  **Windows Start (Bottom Left)–> Server Manager**    **Server Manager, Tools, Hyper-V Manager**    **Hyper-V Manager**  1st Check that enough CPU/RAM/Storage are available on the **lnvh7.eca-international.local** host.  **N.B.** Recommend that you 1st check with management if this is the target Hyper-V host before creating any new instances.    **Hyper-V Manager, New, Virtual Machine(Top Right Panel Actions)**    **New, Virtual Machine Wizard, VM Name and Location of VM Store**    Specify Name of Machine  Change Virtual Machine Store/Location to be **D:\** (a folder with VM name is created where data files are stored)  **New, Virtual Machine Wizard, Specify Generation 2**    **New, Virtual Machine Wizard, Specify Generation**  6Gb Ram = 6144MB    **New, Virtual Machine Wizard, Configure Networking**  Virtual Guests    **New, Virtual Machine Wizard, Connect Virtual Hard Disk**  **Disk = 32GB**    **New, Virtual Machine Wizard, Installation Options**  Install Source/DVD/ISO (Downloaded from Centos Mirrors)  DVD/ISO images are held here **d:\CENTOS\_IMAGES**    **New, Virtual Machine Wizard, Summary**    **Hyper-V – VM, Settings, Security (updates before booting !!!)**  Select VM you just created) Right Click, Settings, Security Tab  Update to be **Microsoft UEFI Certificate Authority, click apply.**    **Hyper-V – VM, Settings, Connect**    **Hyper-V – VM, Settings, Connect (cont’d)**    **Click on Start**  **Linux Install**  Click in window, and user Arrow keys to move/highlight **Install Centos**    **Linux Install, Lang & Keyboard**  Select **English (United Kingdom)** from Right hand Panel, **Select Continue**.    **Note Timezone/Keyboard are now updated to be GB** SOFTWARE   **Select - SOFTWARE, INSTALLATION SOURCE,**  **See next page**  **SOFTWARE SELECTION, Base Environment, Gnome Desktop, Done (Top Left Hand Corner)**    **Select Done** DISK LAYOUTLinux Install, System, INSTALLATION DESTINATION *sda / 32 GiB free* Select 32GB/SDA device (should only be 1 x disk)  **Select Other Storage Options, Select *I will Configure partitioning***    **See next page.**  We then need to re-layout the partition as we want to make 2 x additional Filesystems (legacy they had 1 x FS) But going forward we want them configure 3 x FS.  / # 17.1GB  /home # 9.0GB  /etc/ECA # 1.5GB  **Select Done**  **Next screen will then let you layout the Filesystems as required**  **Leave Partitioning Scheme as LVM**    **Select “Click here to create them automatically”**    **We then need to modify/free space to add the extra FS**  **See next page.** Select the / partition – and change its size down to 17.1 Gib   **See next page**  **Once size has been changed – click on any other partition so the Available Space updates**    **See next page.** Now add the additional mountpoints as below using the + symbol at bottom of the Layout/home – 9GB   **Click “Add mount point”** /etc/ECA - 1.5G   **Click “Add mount point”** Final Layout should look same as below   **Select Done**  **Summary of changes/Accept Changes**   NETWORK **Linux Install, Exclamation Marks cleared from sections as you have populated them.**   Linux Install, Network and Hostname Update Host Name (bottom Left, Apply)    **Configure (bottom Right)**    **Select IPv4 Settings (on row where Ethernet is underlined in blue text)**    **Change:**  **Method: Manual**  (Check with network admin for the IP/Subnet you have been provided)  **Address: IP Address, Netmask, Default Route**  **DNS Servers: 192.168.33.3, 192.168.33.6, 192.168.130.2**  **Search Domains: eca-international.local, domain01.starrate-intranet.co.uk**  **Addresses**  **Get IP/Netmask/Subnet (N.B)**    **Save,**  **Enable Ethernet**    **IP 192.168.130.67/24**  **GW 192.168.130.1**  **Linux Install, begin Installation (Root Password, Add “admin” user)**  Select Begin Installation (Bottom Right)    **Linux Install, root Password, User Creation (“admin” user)**    **Select Root Password**    **Enter desired root passwd, Select Done Top Left**  **Select User Creation**    `  Current admin password is weak – so you will have to **Click Done twice**  Allow 10-15 mins while Instance will is provisioned:    **Reboot**  Once instance has bene built – the screen will show as below    **N.B. Ignore the US keyboard at the top – this is a quirk of the installer, GB keyboard is set/will be default on the installed server.** |

|  |
| --- |
| ANSIBLE PLAYBOOKWhat is Ansible ? <https://www.ansible.com/>  **Ansible** is a configuration management/automation tool. It works on the premise that you describe what the end state should be. The state/tasks which are evaluated/actioned are based upon idempotency (i.e. they will not run if nothing is to be changed) ADD SSH KEY FROM SPACEWALK SERVER Bit of chicken and Egg here ….. To register the server with Spacewalk – you have to have the software installed – and its doesn’t come on the DVD.  So we are going to add the **ssh** key to enable the Spacewalk server to do all the configuration management for us. On the Spacewalk Server |
|  |

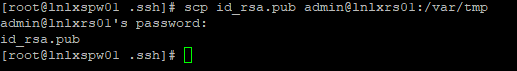
1. Login as your account.
2. # sudo su - # su to root using the sudo mechanism
3. # pwd # Present Working Directory – should be /root



1. # cd .ssh # Change Directory (cd) to .ssh
2. # pwd # Check path is **/root/.ssh**

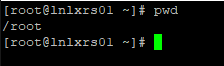


1. # scp id\_rsa.pub admin@target\_hostname:/var/tmp ***# where admin is the account you created at install***

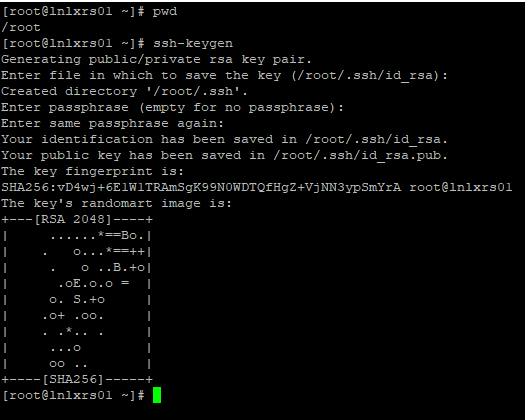


### On the Target/newly built Server

1. Login as the **user you created on install** (I’ve used **admin** in the worked example)
2. # sudo su - # su to root using the sudo mechanism
3. # pwd # Present Working Directory – should be /root



1. # ssh-keygen # This will generate the Public/Private keypair for the root user

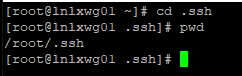


1. Accept defaults for path (/root/.ssh/id\_rsa)
2. Hit Enter, Enter when prompted for passphrase.
3. It then creates the key pair in /root/.ssh/
4. Change directory (cd) to /root/.ssh

**[CMD]**

# cd .ssh

# pwd # **P**resent **W**orking **D**irectory



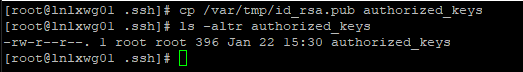
PWD = /root/.ssh path

1. Copy /var/tmp/id\_rsa.pub authorized\_keys

[CMD]

# cp /var/tmp/id\_rsa.pub authorized\_keys

# ls -altr authorized\_keys



### TEST SSH WORKS FROM SPACEWALK SERVER TO TARGET SERVER

1. On Spacewalk server:

**[CMD]**

# ssh ***target\_server*** date # Where ***target\_server*** is IP/hostname of new server



If you get a message like the above – it’s just letting you know that the IP has been added to a file called known\_hosts under the /root/.ssh directory.

### TEMPORARILY ENABLE INTERNET ACCESS FOR NEW BUILT SERVER(S)

1. Enable internet access for the newly built server (temporarily)

**Add hostname to temporary internet enabled rule**

**FIREWALL STEPS REQUIRED**

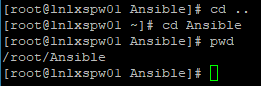
### RUN ANSIBLE-PLAYBOOK FROM SPACEWALK SERVER TO TARGET SERVER

1. As **root account** on **lnlxspw01**

**[CMD]**

# cd /root/Ansible # Change Directory to PATH

# pwd # Check PWD is what we expect



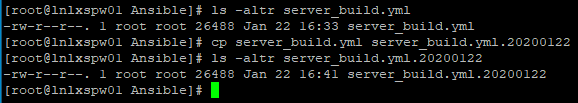
1. List and then create a backup of the **cp** file

**[CMD]**

# ls -altr master\_server\_build.yml

# cp master\_server\_build.yml server\_build.yml.BACKUP.YYYYMMDD

# ls -altr master\_server\_build.yml.BACKUP.YYYYMMDD



1. Ansible has its own hosts configuration file /etc/ansible/hosts – hostname must appear in here before it can be used within ansible (file lives on lnlxspw01)

**[CMD]**

**# cat /etc/ansible/hosts # cat is short for concat**

Eyeball the output of the file and ensure the hostname of the new server is within the file

To add hostname to the file do the following:

**[CMD]**

# echo ***hostname*** >> /etc/ansible/hosts # >> means append hostname to file.

1. Update the **master\_server\_build.yml** file with target server(s) hostname



So this would run against the lnlxwg01 server if called by ansible. The hosts entry can be single/lists, or groups as they are entered in /etc/ansible/hosts.

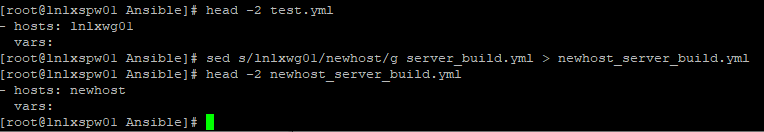
For ease we will just use hostname lists in our playbooks

**[CMD]**

# pwd

# head -2 master\_server\_build.yml # Check what hostname is in file/to be replaced

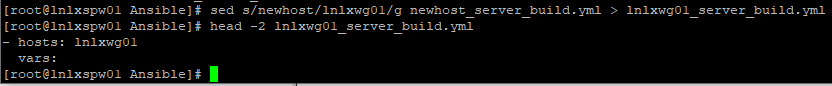
# sed s/lnlxwg01/**newhost/g master\_server\_build.yml > newhos\_server\_build.yml # Change hostname and create a new file for that target host**



1. Check new file has correct hostname

**[CMD]**

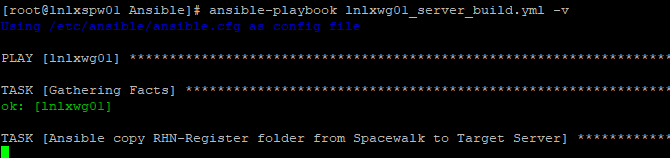
**# head -2 newhost\_server\_build.yml**



1. Execute the ansible playbook against the target host

**[CMD]**

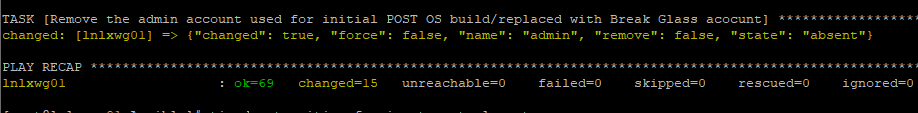
**# ansible-playbook lnlxwg01\_server\_build.yml -v**



This runs for approx. 5-10 mins

1. Successful complete …… 😊

Up Successful completion you will see a summary like below:



Ansible generates a report

1. A failed playbook !!
   1. **Firstly – don’t panic !!**
   2. The playbook will exit/stop running (as typically an action/task is an upstream dependency for others. (If you have more than one target host, and only one of them fails – the playbook will continue to run on the one with no other with no errors)
   3. Where it has failed – it will try and display a usable error message as to why it failed
   4. Often this is a simple case of remediating whatever the issue is – and then re-running the playbook from the spacewalk server again

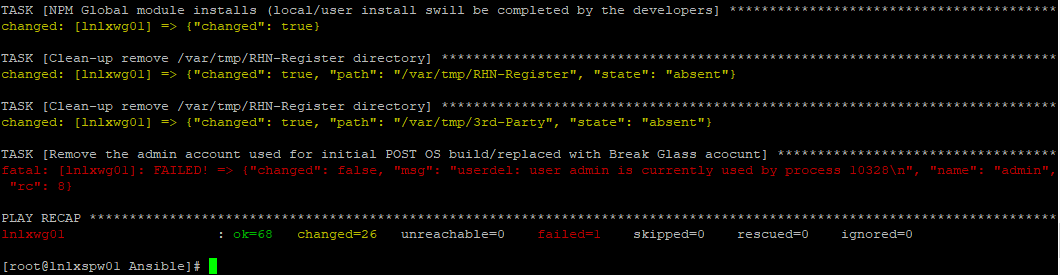
e.g.

Below is output from a playbook run – where final step is we remove the Admin account on the target server (audit/compliance reasons)

In this instance the error shows why is can’t remove the user:

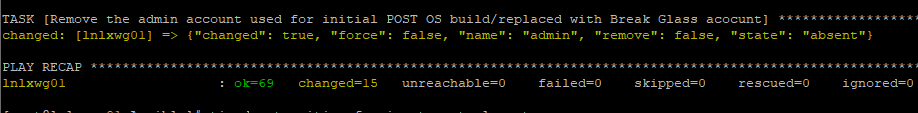
**Fatal: [lnlxwg01]: FAILED => !”change”; false, “msg”; “userdel: user admin is currently used by process 123456”**

I’d say this is pretty clear **(highlighted text)** in short it can’t remove a user which has running processes. In this instance I had logged in as that user on the console, and forgotten to logout – hence running/open processes.



.

To remediate the issue – I logged out from the console session, and re-ran the playbook from the spacewalk server – and it completed successfully.



The summary shows how many **TASKS** were **OK** how many **TASKS** resulted in a **CHANGED,** and of failed/skipped/ignored.

N.B. It is quite often to have tasks which will always result in a change, this does not mean they have updated something – but for example where we copy across ECA specific config files, restart services etc – this will always be flagged as a **change**, rather than just **OK.**

|  |
| --- |
| ACTIVE-DIRECTORY **ECA** use Active Directory for Single-Sign-on/password complexity compliance etc. On the Target host |
|  |

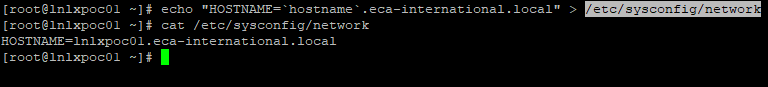
1. Login as your account.
2. # sudo su - # su to root using the sudo mechanism
3. # pwd # Present Working Directory – should be /root



1. Add ***hostname.eca-international.local*** to /etc/sysconfig/network file

**[CMD] # echo "HOSTNAME=`hostname`.eca-international.local" > /etc/sysconfig/network**

**# cat /etc/sysconfig/network**



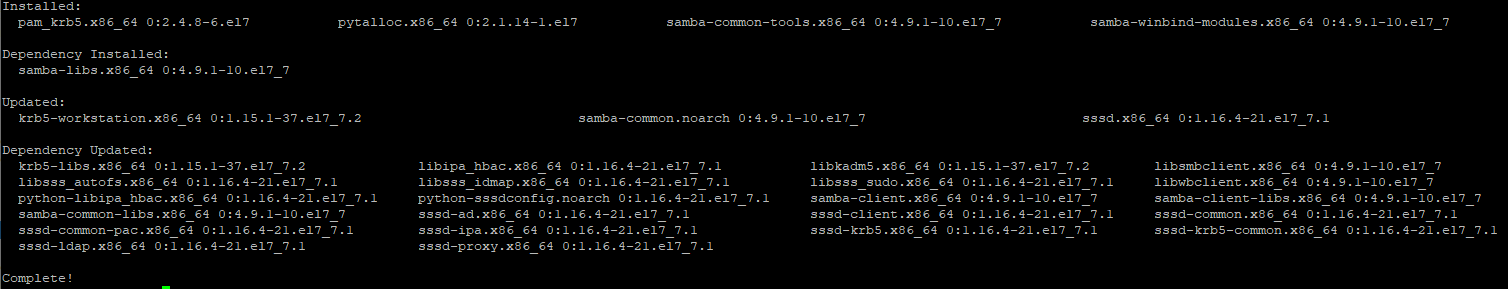
1. Restart both network and NetworkManager system services

**[CMD] # systemctl restart network NetworkManager**



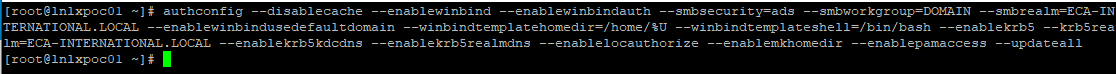
1. YUM – install required packages (System uses Kerberos/Samba and winbind for AD authentication)

**[CMD] # yum -y install authconfig krb5-workstation pam\_krb5 samba-common oddjob-mkhomedir libselinux-python realmd oddjob sssd adcli samba-common-tools pytalloc samba-winbind-modules**



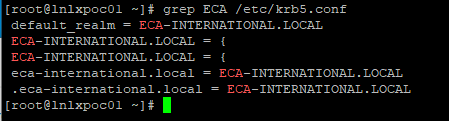
1. Configure the AD DOMAIN/Kerberos/PAM authentication.

**[CMD] # authconfig --disablecache --enablewinbind --enablewinbindauth --smbsecurity=ads --smbworkgroup=DOMAIN --smbrealm=ECA-INTERNATIONAL.LOCAL --enablewinbindusedefaultdomain --winbindtemplatehomedir=/home/%U --winbindtemplateshell=/bin/bash --enablekrb5 --krb5realm=ECA-INTERNATIONAL.LOCAL --enablekrb5kdcdns --enablekrb5realmdns --enablelocauthorize --enablemkhomedir --enablepamaccess –updateall**



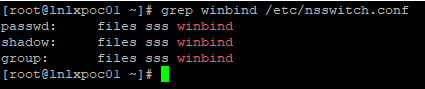
1. Ensure **default\_realm = ECA-INTERNATIONAL.LOCAL** is **UPPERCASE** in **/etc/krb5.conf**

**[CMD] # grep ECA /etc/krb5.conf**



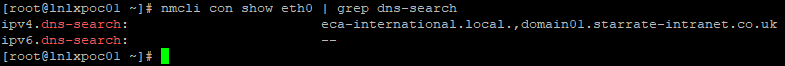
1. Ensure **winbind** is **listed** for **passwd authentication** in the **/etc/nsswitch.conf**

**[CMD] # grep winbind /etc/nsswitch.conf**



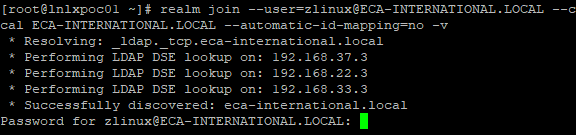
1. Check DNS name search contains both AD domains (eca-international.local & domain01.starrate-intranet.co.uk)

**[CMD] # nmcli con show eth0 | grep dns-search**

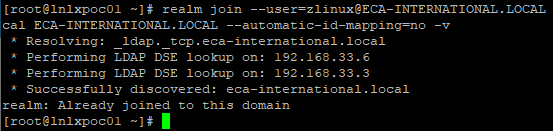


1. Add/bind the host to the **ECA.INTERNATIONAL.LOCAL** AD realm

**[CMD] # realm join --user=zlinux@ECA-INTERNATIONAL.LOCAL --computer-ou=OU=Linux,OU=Servers,OU=London,DC=eca-international,DC=local ECA-INTERNATIONAL.LOCAL --automatic-id-mapping=no -v**



**N.B.**If you get message saying server is already joined to the domain – as below – do a **realm leave**



**[CMD] # realm leave**

**And re-run the realm join command**

**This uses a username and password for initial 1 x authentication**

**User:** [**zlinux@ECA-INTERNATIONAL.LOCAL**](mailto:zlinux@ECA-INTERNATIONAL.LOCAL)

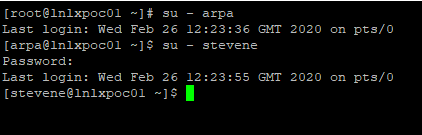
**Password: Get it form the Secure passwd Vault (blanked out in screenshot below)**

A screenshot of a cell phone

Description automatically generated

1. Check AD authentication is working !!
   1. Login as your account, and when prompted use AD password
   2. Su to an account other than yours and then **su – your\_account** (you will be prompted for your passwd)

Example of su’ing to another account and then to my account (Asked for my AD password)



# PATCH SERVER

Please see the Separate Document **ECALinuxPatchProcedure**

# USEFUL LINKS

## CENTOS (Operating System)

CentOS Linux is a community-supported distribution derived from sources freely provided to the public on [**Red Hat**](ftp://ftp.redhat.com/pub/redhat/linux/enterprise/) or [**CentOS git**](https://git.centos.org/) for Red Hat Enterprise Linux (RHEL).

As such, CentOS Linux aims to be functionally compatible with RHEL. The CentOS Project mainly changes packages to remove upstream vendor branding and artwork. CentOS Linux is no-cost and free to redistribute.

<https://www.centos.org/>

ECA have used Centos 7.7 (1908 iso image) Centos 8.0 was GA, but deemed to new/likely to need more maintenance than the more mature Centos 7.

## SPACEWALK (OS Provisioning/Patching)

<https://spacewalkproject.github.io/> # Main Project Page

<https://github.com/spacewalkproject/spacewalk/wiki/UserDocs> # Wiki Docs Page

## ANSIBLE (Configuration Management software)

GOAL-ORIENTED, NOT SCRIPTED

<https://www.ansible.com/>

<https://www.ansible.com/overview/how-ansible-works>