Infrastructure Identity, SSH, and Ansible Connectivity Setup

This project documents the end-to-end configuration and validation of identity management, secure SSH access, and Ansible automation readiness across a multi-host Linux environment.

The work begins with enrolling a stage web server into a FreeIPA domain, establishing centralized authentication, authorization, and certificate trust. System services such as SSSD, Kerberos, LDAP, and SSH are configured and validated to ensure domain users can authenticate, receive correct group memberships, and escalate privileges via sudo policies.

To support secure automation, SSH key-based authentication is implemented using modern cryptography (ED25519 and RSA where required). Host key mismatches and stale trust entries are identified and resolved by cleaning and rebuilding known_hosts data, followed by re-establishing trusted connections between managed nodes and the Ansible control host.

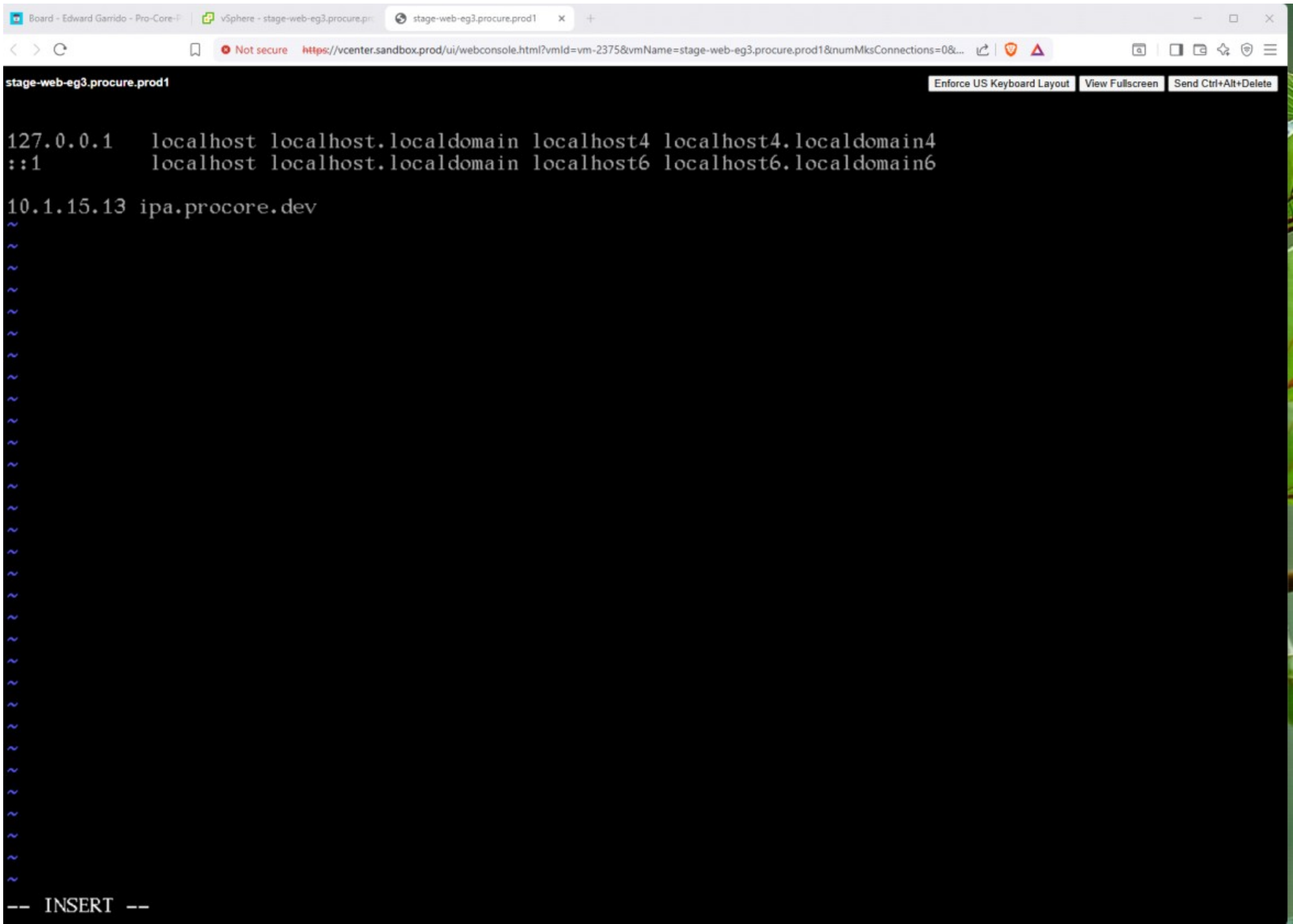
Static hostname resolution is configured via /etc/hosts where necessary to ensure reliable connectivity in controlled environments. SSH daemon settings are reviewed to confirm a hardened baseline aligned with enterprise standards.

Finally, Ansible inventory configuration and connectivity are verified using the ansible -m ping module. Initial connection failures are troubleshot and resolved, resulting in successful communication across development, performance, and stage web hosts. This confirms the environment is fully prepared for repeatable, secure automation workflows.

Security & Sanitization Notice

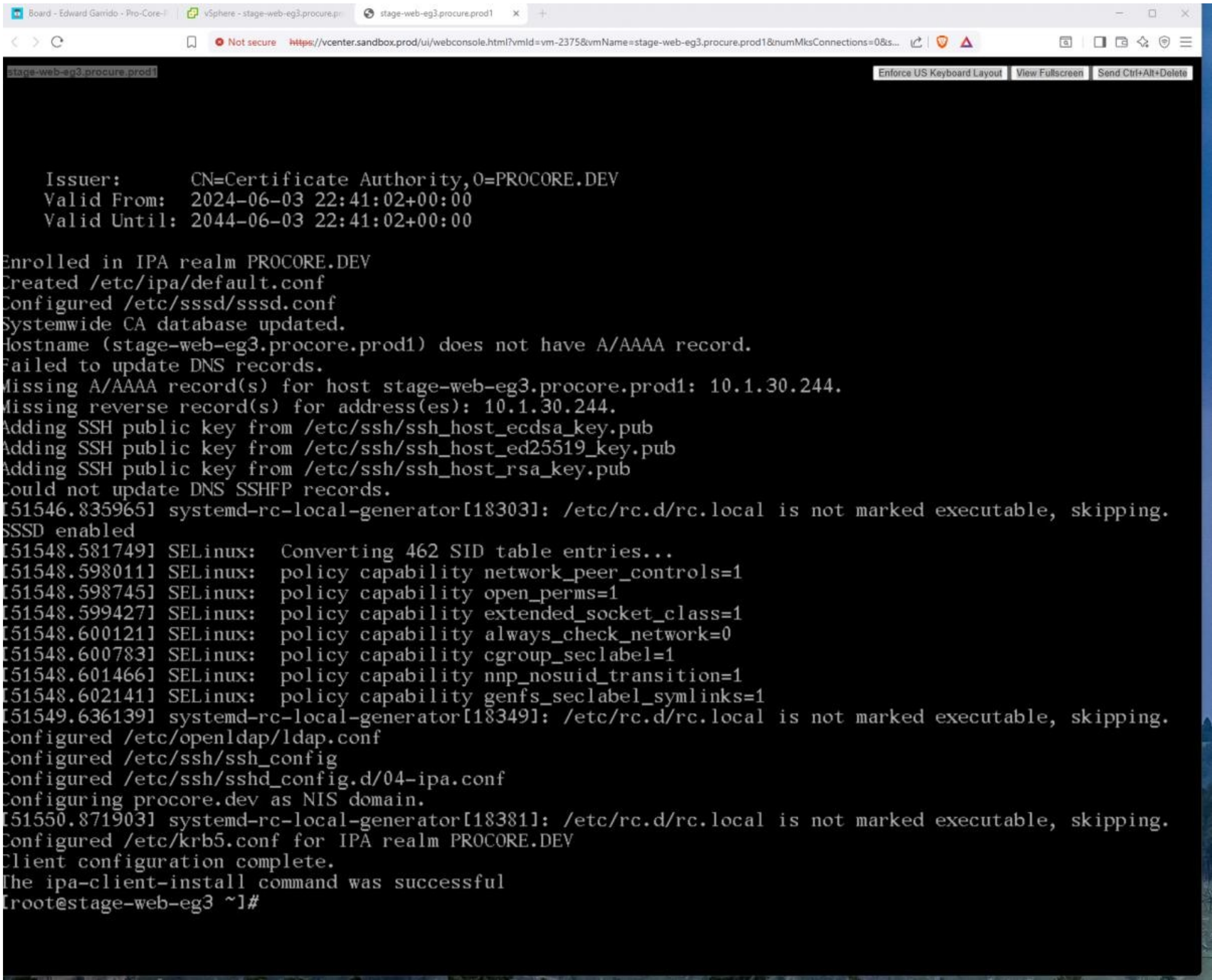
All IP addresses, hostnames, usernames, domain names, timestamps, and environment-specific identifiers shown in screenshots, command output, and configuration files have been sanitized or obfuscated. No production credentials, real infrastructure identifiers, or sensitive data are exposed in this repository.

Vim is open on stage-web-eg3.procore.prod1 (via the vSphere web console) editing the /etc/hosts file. It shows the default localhost entries (127.0.0.1 and ::1) along with a custom hostname mapping (10.1.15.13 ipa.procore.dev). The editor is currently in -- INSERT -- mode. All IP addresses shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-P
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

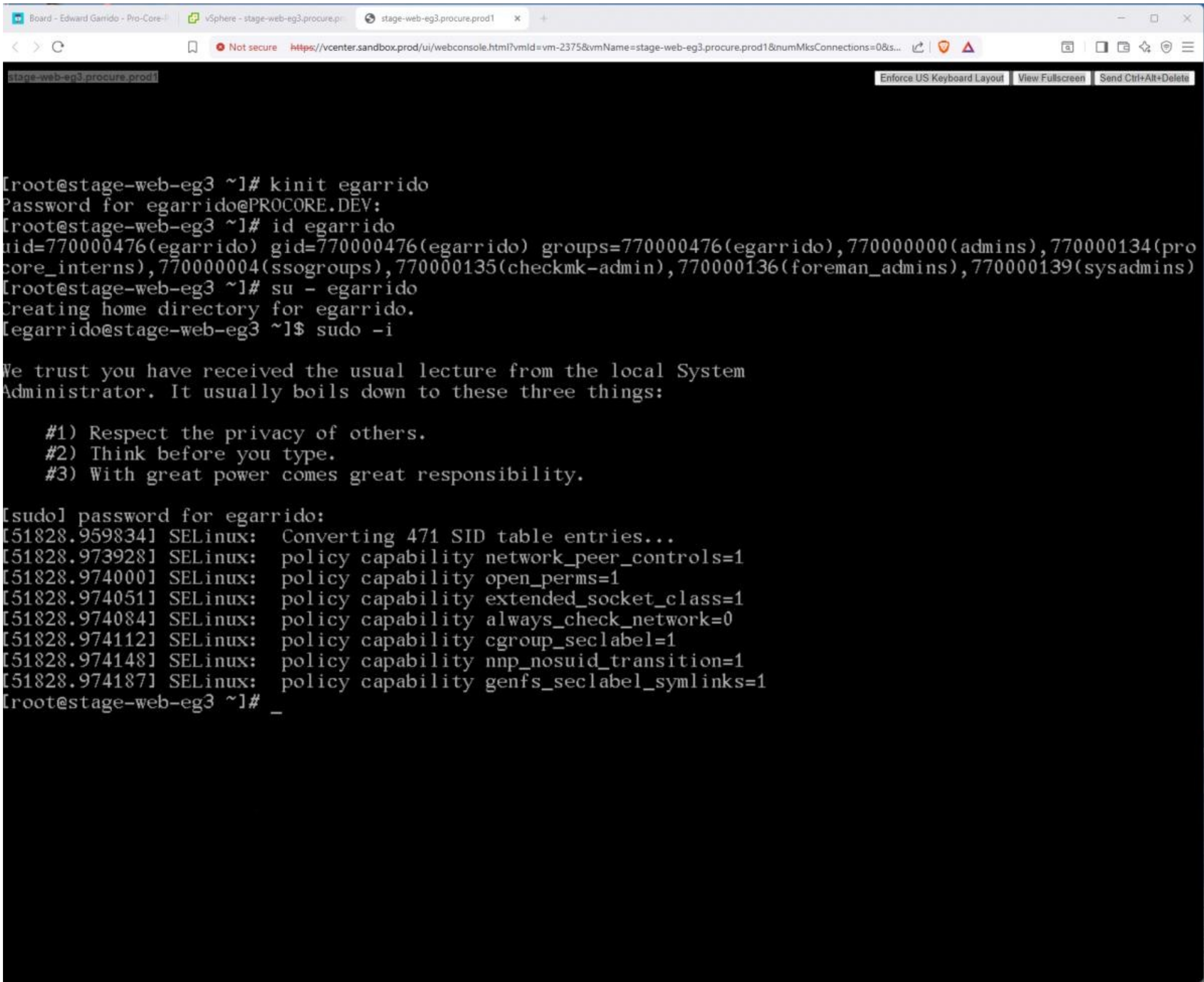
```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

10.1.15.13 ipa.procore.dev
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

The terminal output shows a successful FreeIPA client enrollment for stage-web-eg3.procore.prod1 into the PROCORE.DEV realm. During the process, system configuration files were created or updated (SSSD, Kerberos, SSH, LDAP), CA certificates were installed, and SSH host keys were registered. DNS updates attempted during enrollment reported missing forward and reverse records, but this did not prevent the client installation from completing successfully. SELinux policies were initialized, and the process завершед with confirmation that ipa-client-install ran successfully. All IP addresses shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&s...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

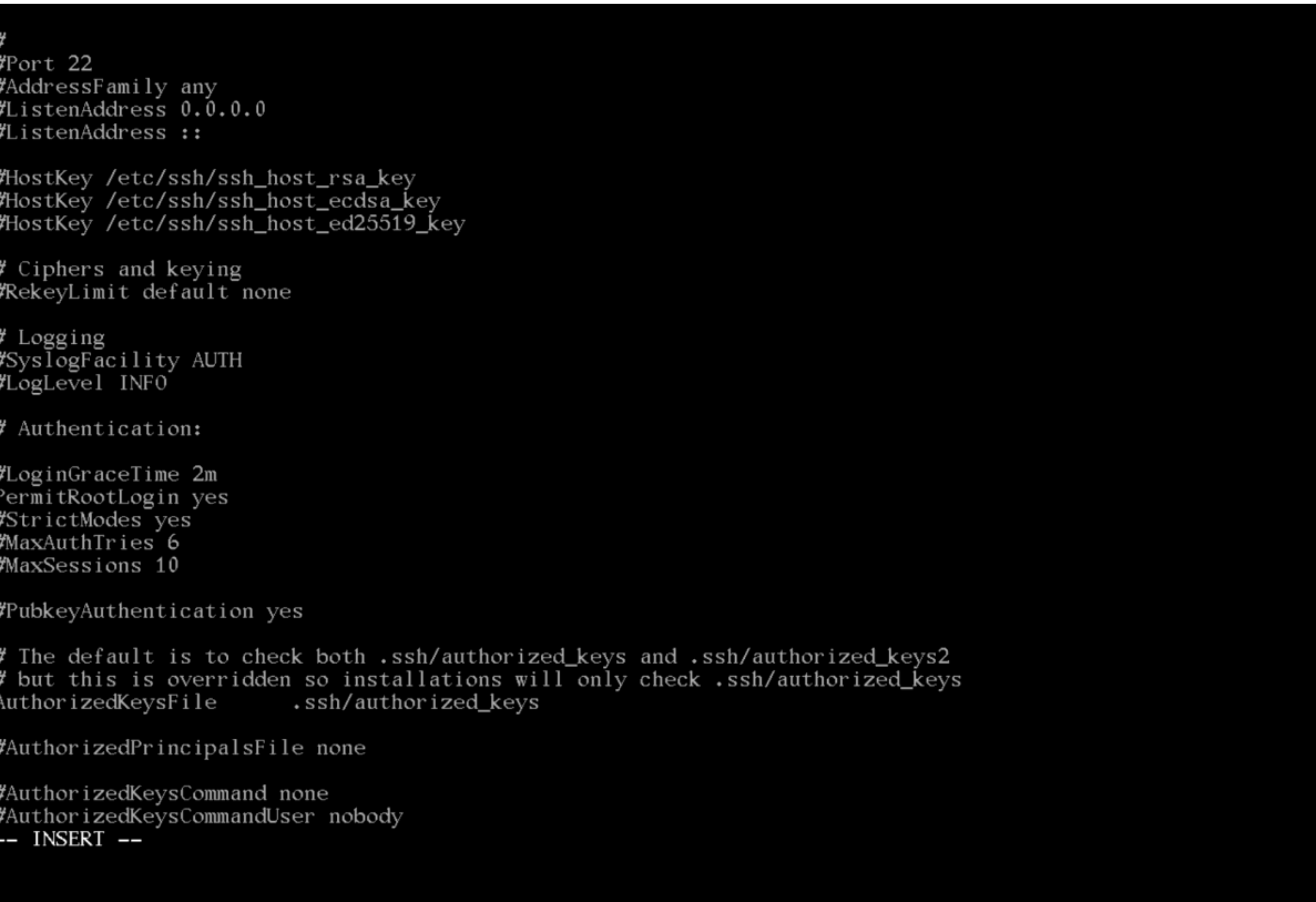
```
    Issuer:       CN=Certificate Authority,O=PROCORE.DEV
    Valid From:   2024-06-03 22:41:02+00:00
    Valid Until:  2044-06-03 22:41:02+00:00

Enrolled in IPA realm PROCORE.DEV
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Hostname (stage-web-eg3.procore.prod1) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host stage-web-eg3.procore.prod1: 10.1.30.244.
Missing reverse record(s) for address(es): 10.1.30.244.
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Could not update DNS SSHFP records.
[51546.835965] systemd-rc-local-generator[18303]: /etc/rc.d/rc.local is not marked executable, skipping.
SSSD enabled
[51548.581749] SELinux:  Converting 462 SID table entries...
[51548.598011] SELinux:  policy capability network_peer_controls=1
[51548.598745] SELinux:  policy capability open_perms=1
[51548.599427] SELinux:  policy capability extended_socket_class=1
[51548.600121] SELinux:  policy capability always_check_network=0
[51548.600783] SELinux:  policy capability cgroup_seclabel=1
[51548.601466] SELinux:  policy capability nnp_nosuid_transition=1
[51548.602141] SELinux:  policy capability genfs_seclabel_symlinks=1
[51549.636139] systemd-rc-local-generator[18349]: /etc/rc.d/rc.local is not marked executable, skipping.
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring procore.dev as NIS domain.
[51550.871903] systemd-rc-local-generator[18381]: /etc/rc.d/rc.local is not marked executable, skipping.
Configured /etc/krb5.conf for IPA realm PROCORE.DEV
Client configuration complete.
The ipa-client-install command was successful
[root@stage-web-eg3 ~]#
```

This terminal session verifies successful FreeIPA authentication and privilege escalation for the user egarrido on stage-web-eg3.procore.prod1. The user obtains a Kerberos ticket using kinit, confirms identity and group memberships with id, and logs in with su -, which automatically creates the user's home directory via IPA integration. The user then successfully escalates privileges with sudo -i, confirming proper sudo policy assignment from FreeIPA. SELinux policy messages indicate normal initialization during the privilege escalation process. All IP addresses shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&s...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

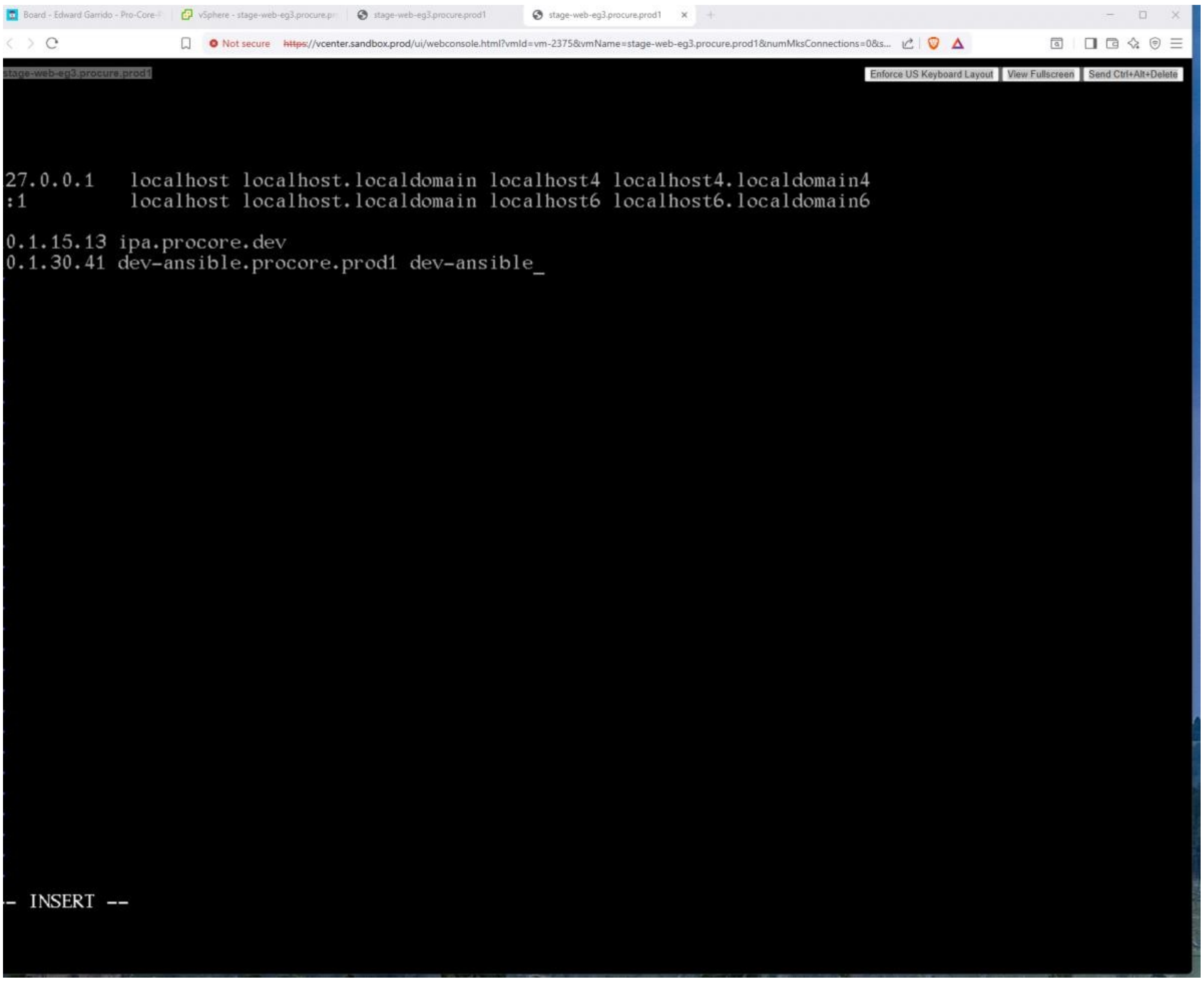
```
[root@stage-web-eg3 ~]# kinit egarrido
Password for egarrido@PROCORE.DEV:
[root@stage-web-eg3 ~]# id egarrido
uid=770000476(egarrido) gid=770000476(egarrido) groups=770000476(egarrido),770000000(admins),770000134(pro
core_interns),770000004(ssogroups),770000135(checkmk-admin),770000136(foreman_admins),770000139(sysadmins)
[root@stage-web-eg3 ~]# su - egarrido
Creating home directory for egarrido.
[egarrido@stage-web-eg3 ~]$ sudo -i

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for egarrido:
[51828.959834] SELinux:  Converting 471 SID table entries...
[51828.973928] SELinux:  policy capability network_peer_controls=1
[51828.974000] SELinux:  policy capability open_perms=1
[51828.974051] SELinux:  policy capability extended_socket_class=1
[51828.974084] SELinux:  policy capability always_check_network=0
[51828.974112] SELinux:  policy capability cgroup_seclabel=1
[51828.974148] SELinux:  policy capability nnp_nosuid_transition=1
[51828.974187] SELinux:  policy capability genfs_seclabel_symlinks=1
[root@stage-web-eg3 ~]# _
```

This view shows the OpenSSH server configuration file being edited in Vim, with core security and authentication settings visible. The configuration defines the SSH port, address family, enabled host keys (RSA, ECDSA, ED25519), logging behavior, and authentication controls such as root login permissions, session limits, and public key authentication. The file is currently open in -- INSERT -- mode, indicating active editing. All IP addresses and environment-specific details shown are sanitized for security purposes.



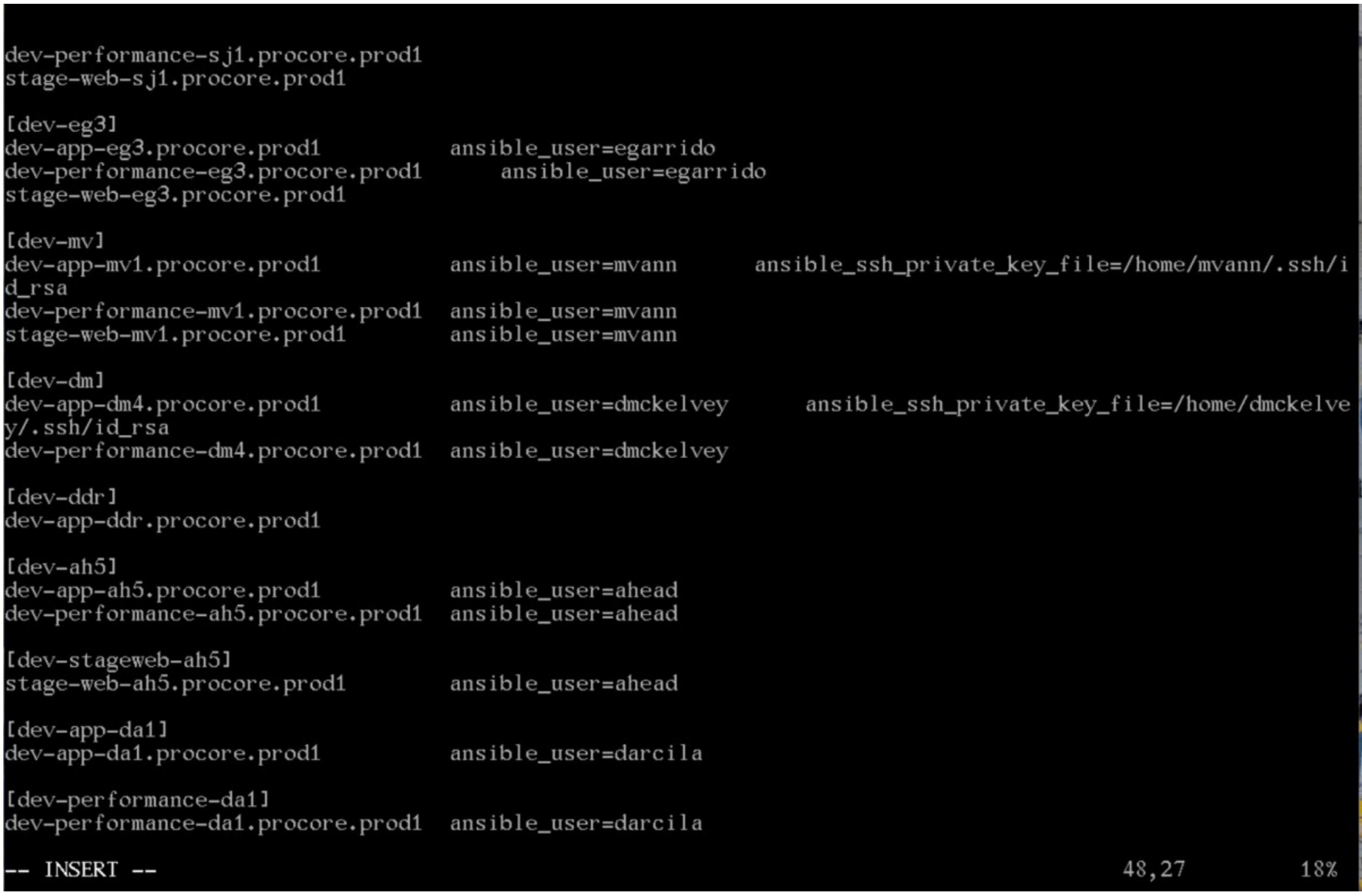
```
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
-- INSERT --
```

This screenshot shows the /etc/hosts file being edited on stage-web-eg3.procore.prod1 using Vim. In addition to the default localhost entries for IPv4 and IPv6, custom hostname mappings have been added for internal infrastructure services, including the FreeIPA server and an Ansible management host. The editor is currently in -- INSERT -- mode, indicating active modification of the file. All IP addresses and hostnames shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
stage-web-eg3.procure.prod1
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&s...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

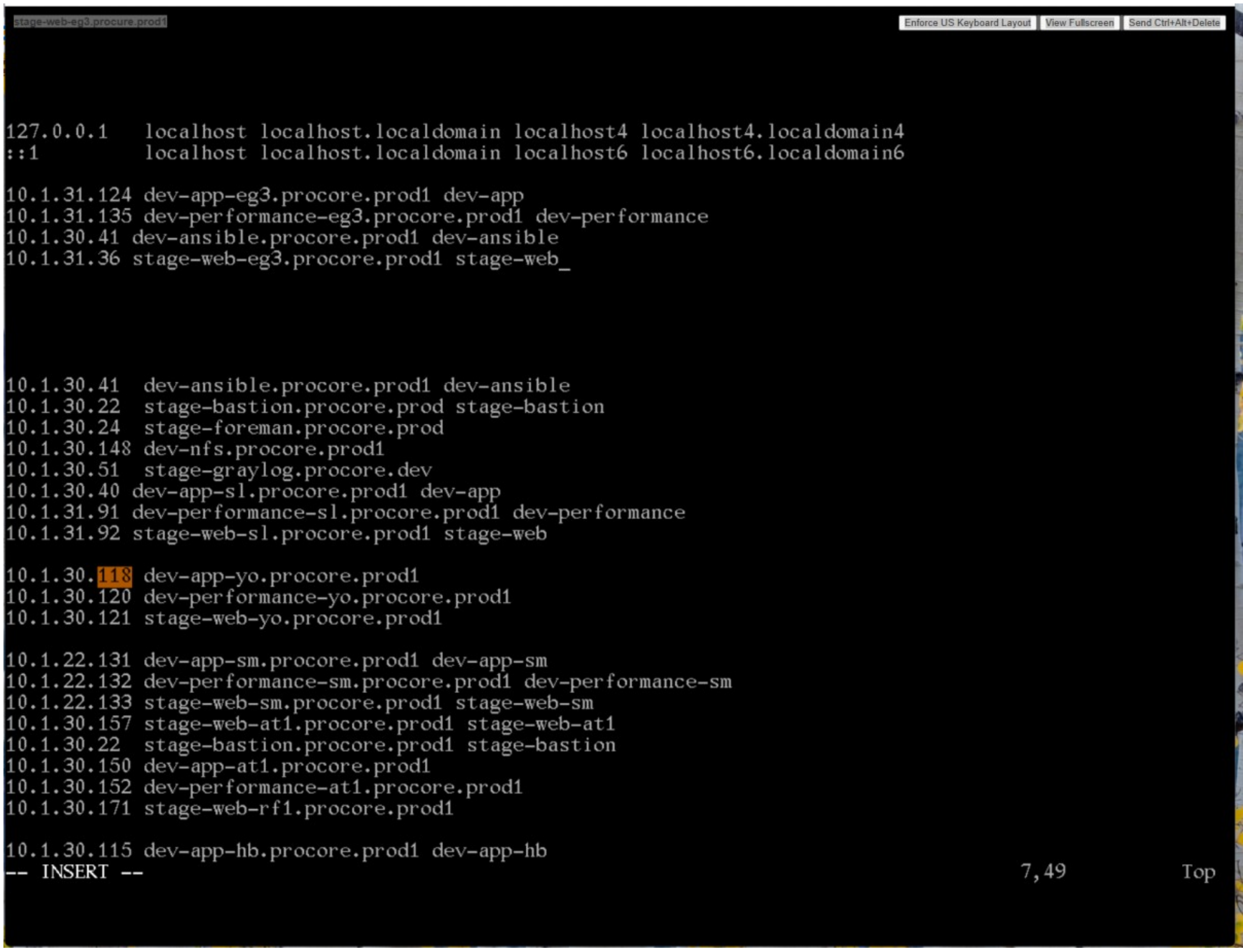
```
27.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
:1         localhost localhost.localdomain localhost6 localhost6.localdomain6

0.1.15.13 ipa.procore.dev
0.1.30.41 dev-ansible.procore.prod1 dev-ansible_




- INSERT --
```

This screenshot shows an Ansible inventory file open in Vim, organized into multiple host groups representing different environments and roles (development, performance, and stage web systems). Each group lists fully qualified hostnames with associated connection variables such as ansible_user and, where required, custom SSH private key paths. This structure enables role-based and user-specific access control across the infrastructure while supporting targeted automation runs. The file is currently in -- INSERT -- mode, indicating active editing. All hostnames, usernames, and IP-related details shown are sanitized for security purposes



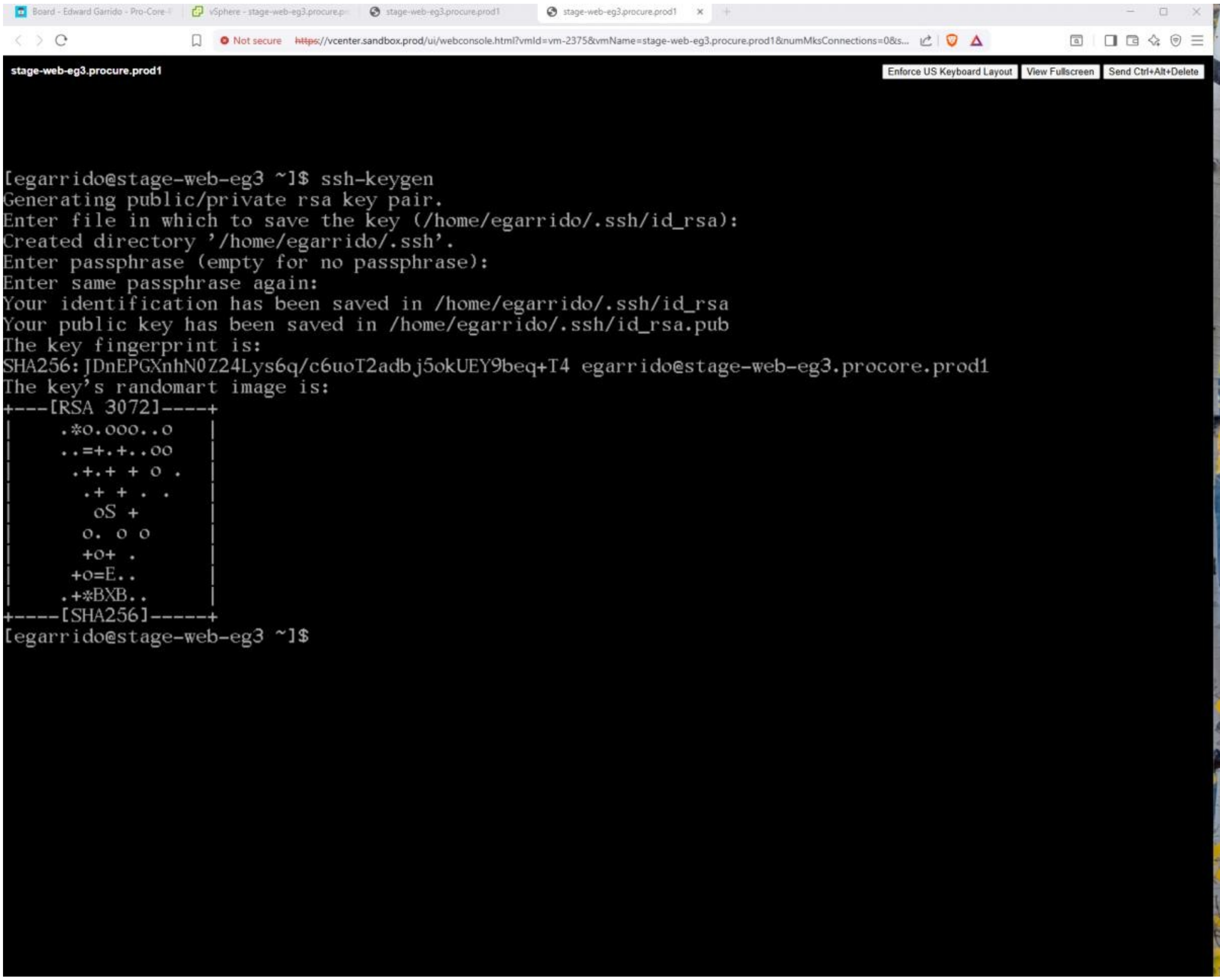
```
dev-performance-sj1.procore.prod1
stage-web-sj1.procore.prod1

[dev-eg3]
dev-app-eg3.procore.prod1         ansible_user=egarrido
dev-performance-eg3.procore.prod1     ansible_user=egarrido
stage-web-eg3.procore.prod1

[dev-mv]
dev-app-mv1.procore.prod1         ansible_user=mvann      ansible_ssh_private_key_file=/home/mvann/.ssh/i
d_rsa
dev-performance-mv1.procore.prod1  ansible_user=mvann
stage-web-mv1.procore.prod1        ansible_user=mvann

[dev-dm]
dev-app-dm4.procore.prod1         ansible_user=dmckelvey      ansible_ssh_private_key_file=/home/dmckelve
y/.ssh/id_rsa
dev-performance-dm4.procore.prod1  ansible_user=dmckelvey

[dev-ddr]
dev-app-ddr.procore.prod1

[dev-ah5]
dev-app-ah5.procore.prod1         ansible_user=ahead
dev-performance-ah5.procore.prod1  ansible_user=ahead

[dev-stageweb-ah5]
stage-web-ah5.procore.prod1        ansible_user=ahead

[dev-app-da1]
dev-app-da1.procore.prod1         ansible_user=darcila

[dev-performance-da1]
dev-performance-da1.procore.prod1  ansible_user=darcila

-- INSERT --                                                                          48,27          18%
```

This screenshot shows the /etc/hosts file on stage-web-eg3.procore.prod1 opened in Vim and populated with extensive static hostname mappings for multiple environments, including development, performance, stage web, bastion, Ansible, monitoring, and supporting infrastructure hosts. These entries provide local name resolution for internal systems when DNS is unavailable or during controlled configuration and testing. The editor is currently in -- INSERT -- mode, indicating active updates to the file. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.



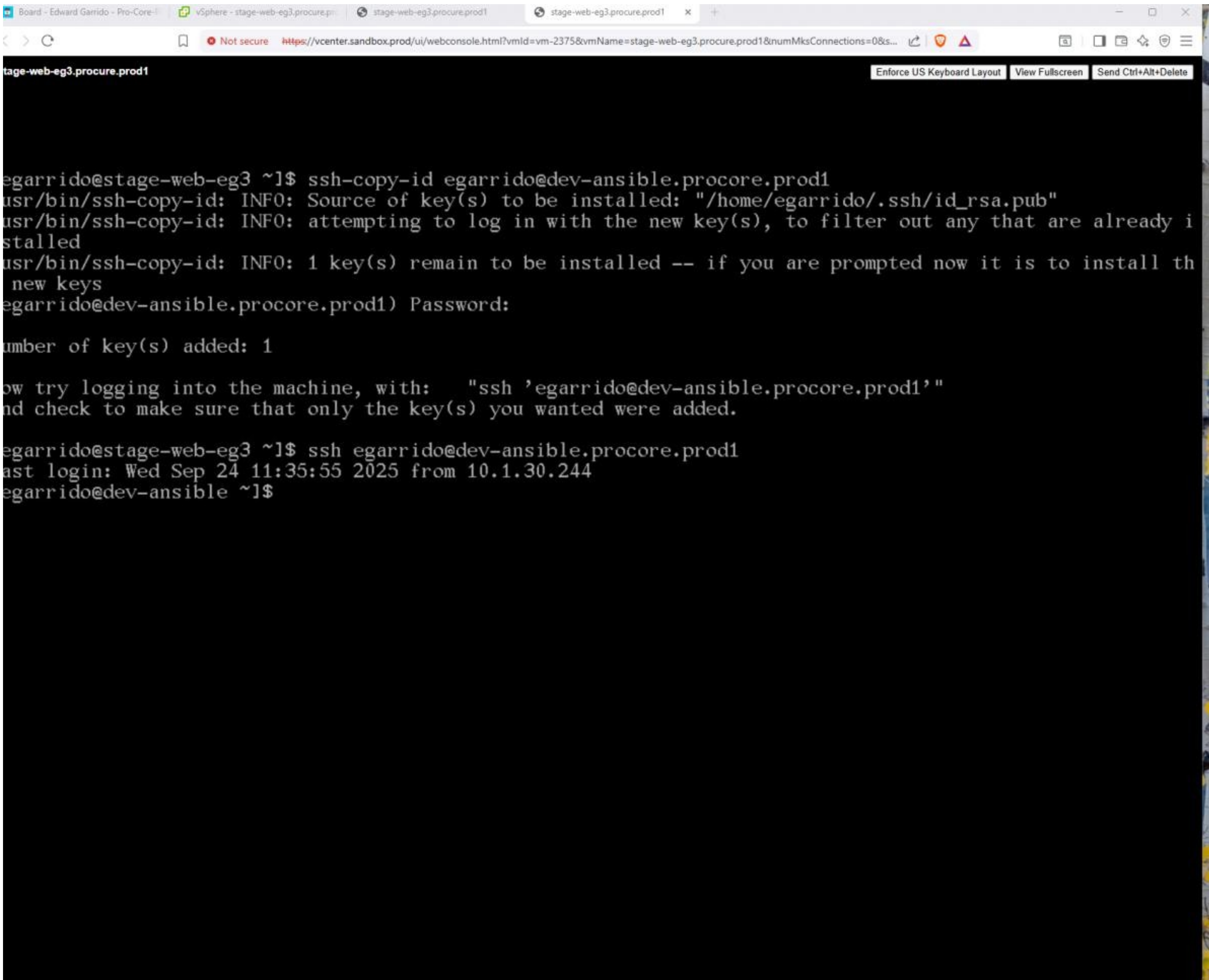
```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

10.1.31.124 dev-app-eg3.procore.prod1 dev-app
10.1.31.135 dev-performance-eg3.procore.prod1 dev-performance
10.1.30.41 dev-ansible.procore.prod1 dev-ansible
10.1.31.36 stage-web-eg3.procore.prod1 stage-web_




10.1.30.41  dev-ansible.procore.prod1 dev-ansible
10.1.30.22  stage-bastion.procore.prod stage-bastion
10.1.30.24  stage-foreman.procore.prod
10.1.30.148 dev-nfs.procore.prod1
10.1.30.51  stage-graylog.procore.dev
10.1.30.40 dev-app-sl.procore.prod1 dev-app
10.1.31.91 dev-performance-sl.procore.prod1 dev-performance
10.1.31.92 stage-web-sl.procore.prod1 stage-web

10.1.30.118 dev-app-yo.procore.prod1
10.1.30.120 dev-performance-yo.procore.prod1
10.1.30.121 stage-web-yo.procore.prod1

10.1.22.131 dev-app-sm.procore.prod1 dev-app-sm
10.1.22.132 dev-performance-sm.procore.prod1 dev-performance-sm
10.1.22.133 stage-web-sm.procore.prod1 stage-web-sm
10.1.30.157 stage-web-at1.procore.prod1 stage-web-at1
10.1.30.22  stage-bastion.procore.prod1 stage-bastion
10.1.30.150 dev-app-at1.procore.prod1
10.1.30.152 dev-performance-at1.procore.prod1
10.1.30.171 stage-web-rf1.procore.prod1

10.1.30.115 dev-app-hb.procore.prod1 dev-app-hb
-- INSERT --                                                          7,49          Top
```

This screenshot shows the successful creation of an SSH RSA key pair using ssh-keygen for the user egarrido on stage-web-eg3.procore.prod1. The private key is stored securely in the user’s .ssh directory, and the corresponding public key is generated for use with key-based authentication across managed systems. The output also displays the key fingerprint and randomart image, confirming successful key generation. All environment-specific details shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-
vSphere - stage-web-eg3.procure.p
stage-web-eg3.procure.prod1
stage-web-eg3.procure.prod1
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&s...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

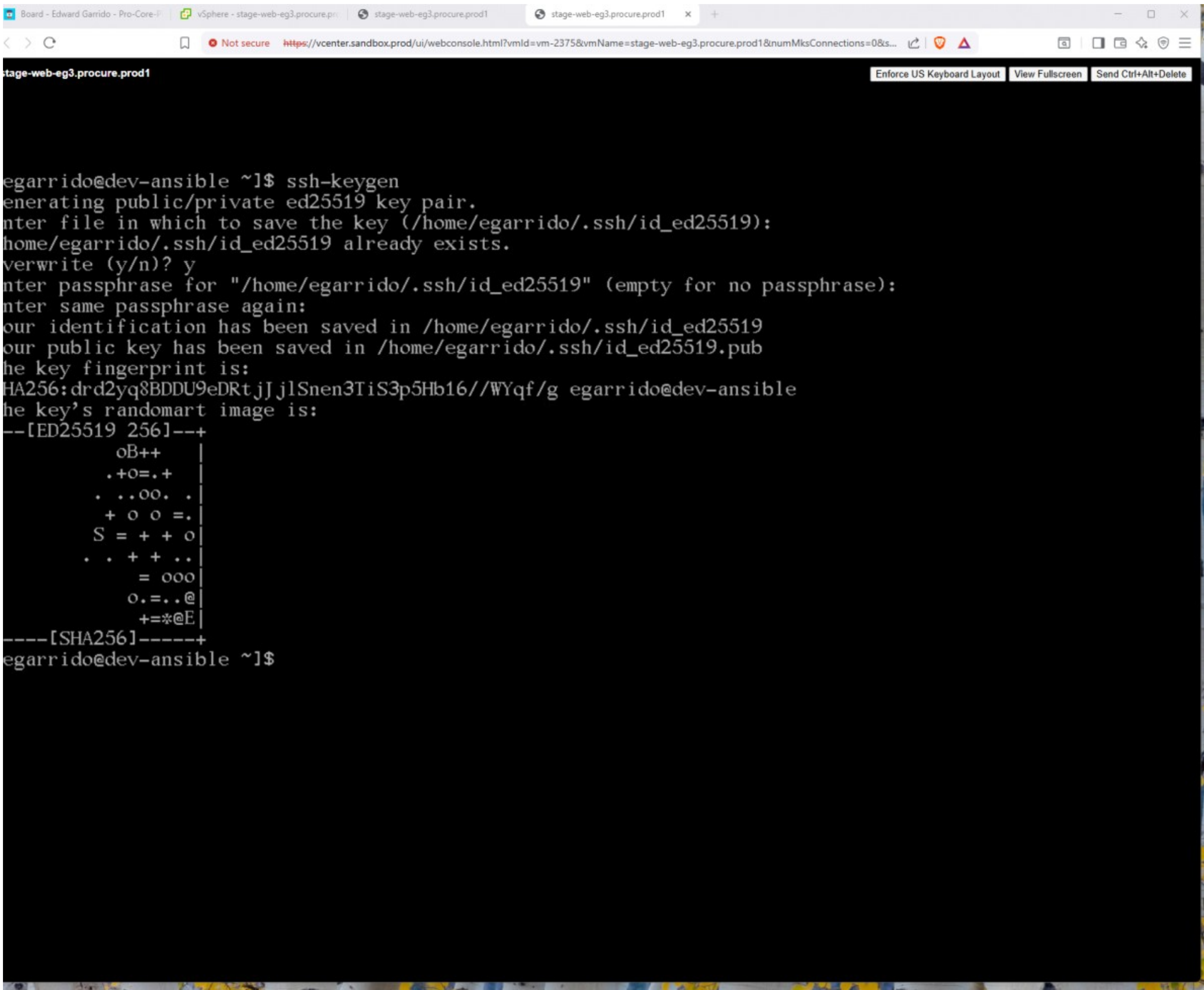
```
[egarrido@stage-web-eg3 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/egarrido/.ssh/id_rsa):
Created directory '/home/egarrido/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/egarrido/.ssh/id_rsa
Your public key has been saved in /home/egarrido/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:JDnEPGXnhN0Z24Lys6q/c6uoT2adbj5okUEY9beq+T4 egarrido@stage-web-eg3.procore.prod1
The key's randomart image is:
+---[RSA 3072]----+
|     .*o.ooo..o  |
|     ..=+.+..oo  |
|      .+.+ + o . |
|       .+ + . .  |
|        oS +     |
|       o. o o    |
|       +o+ .     |
|      +o=E..     |
|     .+*BXB..    |
+----[SHA256]-----+
[egarrido@stage-web-eg3 ~]$
```

This screenshot demonstrates SSH key-based authentication setup and validation between hosts. The user copies their public SSH key to the remote Ansible management server using ssh-copy-id, successfully installs the key, and then confirms passwordless access by logging in via SSH without errors. This verifies secure, key-based connectivity required for Ansible automation and remote management. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
stage-web-eg3.procure.prod1
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&s...
tage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

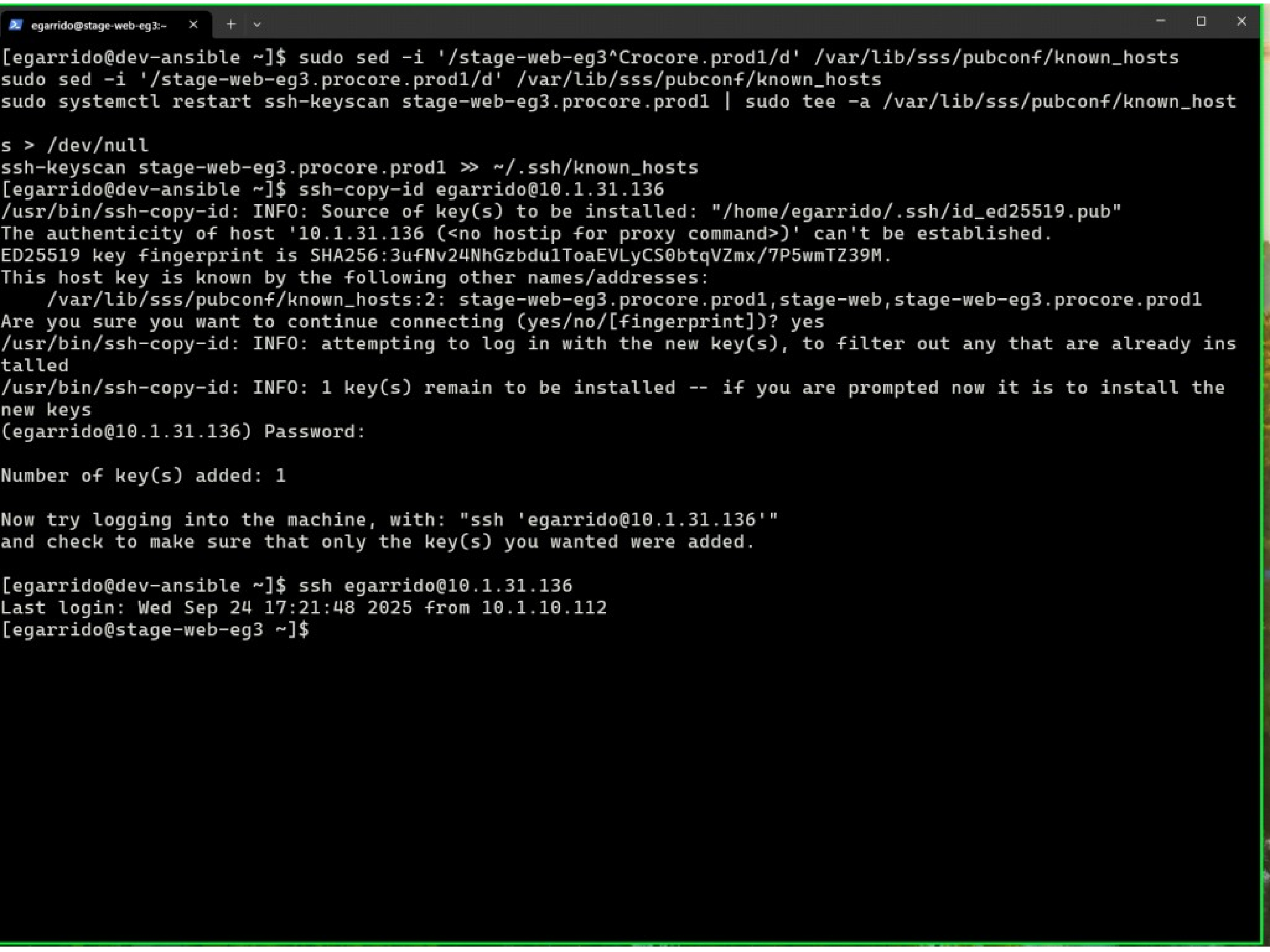
```
egarrido@stage-web-eg3 ~]$ ssh-copy-id egarrido@dev-ansible.procore.prod1
usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/egarrido/.ssh/id_rsa.pub"
usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already i
stalled
usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install th
 new keys
egarrido@dev-ansible.procore.prod1) Password:

umber of key(s) added: 1

ow try logging into the machine, with:   "ssh 'egarrido@dev-ansible.procore.prod1'"
nd check to make sure that only the key(s) you wanted were added.

egarrido@stage-web-eg3 ~]$ ssh egarrido@dev-ansible.procore.prod1
ast login: Wed Sep 24 11:35:55 2025 from 10.1.30.244
egarrido@dev-ansible ~]$
```

This screenshot shows the generation of an ED25519 SSH key pair on the Ansible management host for the user egarrido. An existing key is intentionally overwritten, and a new public/private key pair is created in the user's .ssh directory. The output confirms successful key creation by displaying the SHA256 fingerprint and randomart image. ED25519 keys provide stronger security and better performance compared to traditional RSA keys, making them well-suited for automated configuration management workflows. All environment-specific details shown are sanitized for security purposes.


Board - Edward Garrido - Pro-Core-F
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
stage-web-eg3.procure.prod1
Not secure
~~https~~://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2375&vmName=stage-web-eg3.procure.prod1&numMksConnections=0&s...
tage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

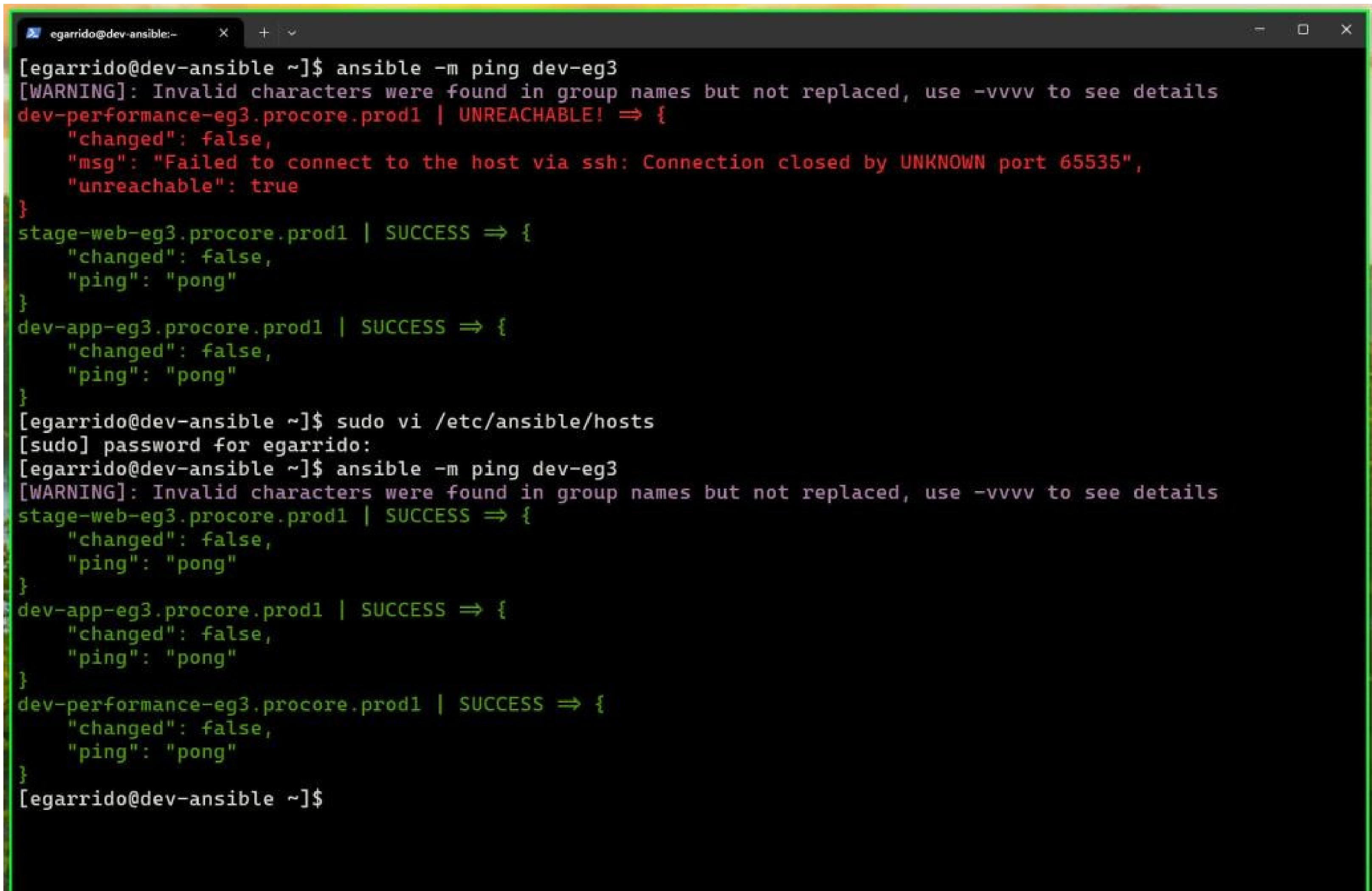
```
egarrido@dev-ansible ~]$ ssh-keygen
enerating public/private ed25519 key pair.
nter file in which to save the key (/home/egarrido/.ssh/id_ed25519):
home/egarrido/.ssh/id_ed25519 already exists.
verwrite (y/n)? y
nter passphrase for "/home/egarrido/.ssh/id_ed25519" (empty for no passphrase):
nter same passphrase again:
our identification has been saved in /home/egarrido/.ssh/id_ed25519
our public key has been saved in /home/egarrido/.ssh/id_ed25519.pub
he key fingerprint is:
HA256:drd2yq8BDDU9eDRtjJjlSnen3TiS3p5Hb16//WYqf/g egarrido@dev-ansible
he key's randomart image is:
--[ED25519 256]--+
          oB++    |
         .+o=.+   |
        . ..oo. . |
         + o o =. |
        S = + + o |
       . . + + .. |
            = ooo |
           o.=..@ |
            +=*@E |
----[SHA256]-----+
egarrido@dev-ansible ~]$
```

This terminal session shows SSH host key cleanup and re-establishment of trusted access between the Ansible management host and stage-web-eg3.procore.prod1. Existing stale host key entries are removed from both the SSSD public known_hosts file and the user's SSH known_hosts to prevent key mismatch issues. The SSH service is restarted, a fresh host key is retrieved using ssh-keyscan, and the updated key is appended to the appropriate trust stores. The user then securely re-installs their ED25519 public key with ssh-copy-id and successfully validates passwordless SSH access to the target host. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.



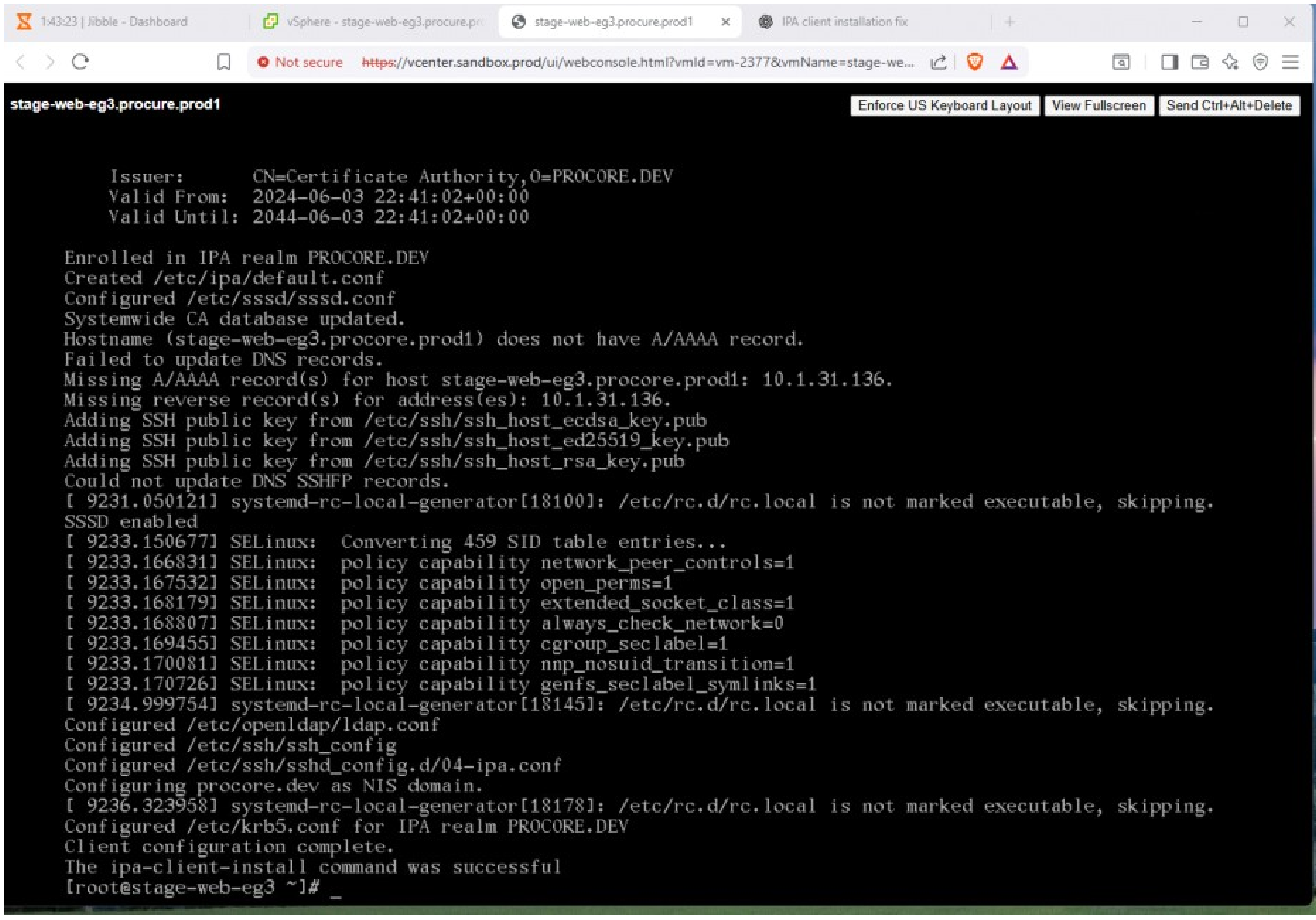
```
[egarrido@dev-ansible ~]$ sudo sed -i '/stage-web-eg3^Crocore.prod1/d' /var/lib/sss/pubconf/known_hosts
sudo sed -i '/stage-web-eg3.procore.prod1/d' /var/lib/sss/pubconf/known_hosts
sudo systemctl restart ssh-keyscan stage-web-eg3.procore.prod1 | sudo tee -a /var/lib/sss/pubconf/known_host

s > /dev/null
ssh-keyscan stage-web-eg3.procore.prod1 >> ~/.ssh/known_hosts
[egarrido@dev-ansible ~]$ ssh-copy-id egarrido@10.1.31.136
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/egarrido/.ssh/id_ed25519.pub"
The authenticity of host '10.1.31.136 (<no hostip for proxy command>)' can't be established.
ED25519 key fingerprint is SHA256:3ufNv24NhGzbdu1ToaEVLyCS0btqVZmx/7P5wmTZ39M.
This host key is known by the following other names/addresses:
    /var/lib/sss/pubconf/known_hosts:2: stage-web-eg3.procore.prod1,stage-web,stage-web-eg3.procore.prod1
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already ins
talled
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the
new keys
(egarrido@10.1.31.136) Password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'egarrido@10.1.31.136'"
and check to make sure that only the key(s) you wanted were added.

[egarrido@dev-ansible ~]$ ssh egarrido@10.1.31.136
Last login: Wed Sep 24 17:21:48 2025 from 10.1.10.112
[egarrido@stage-web-eg3 ~]$
```

This screenshot shows Ansible connectivity testing and inventory correction using the ansible -m ping module. The initial run reports one host as UNREACHABLE due to an SSH connection issue, while other hosts respond successfully. After editing the Ansible inventory (/etc/ansible/hosts) to correct group or host definitions, the ping test is rerun and all targeted hosts return SUCCESS with a pong response. This confirms that SSH access and inventory configuration are properly aligned for Ansible automation. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.



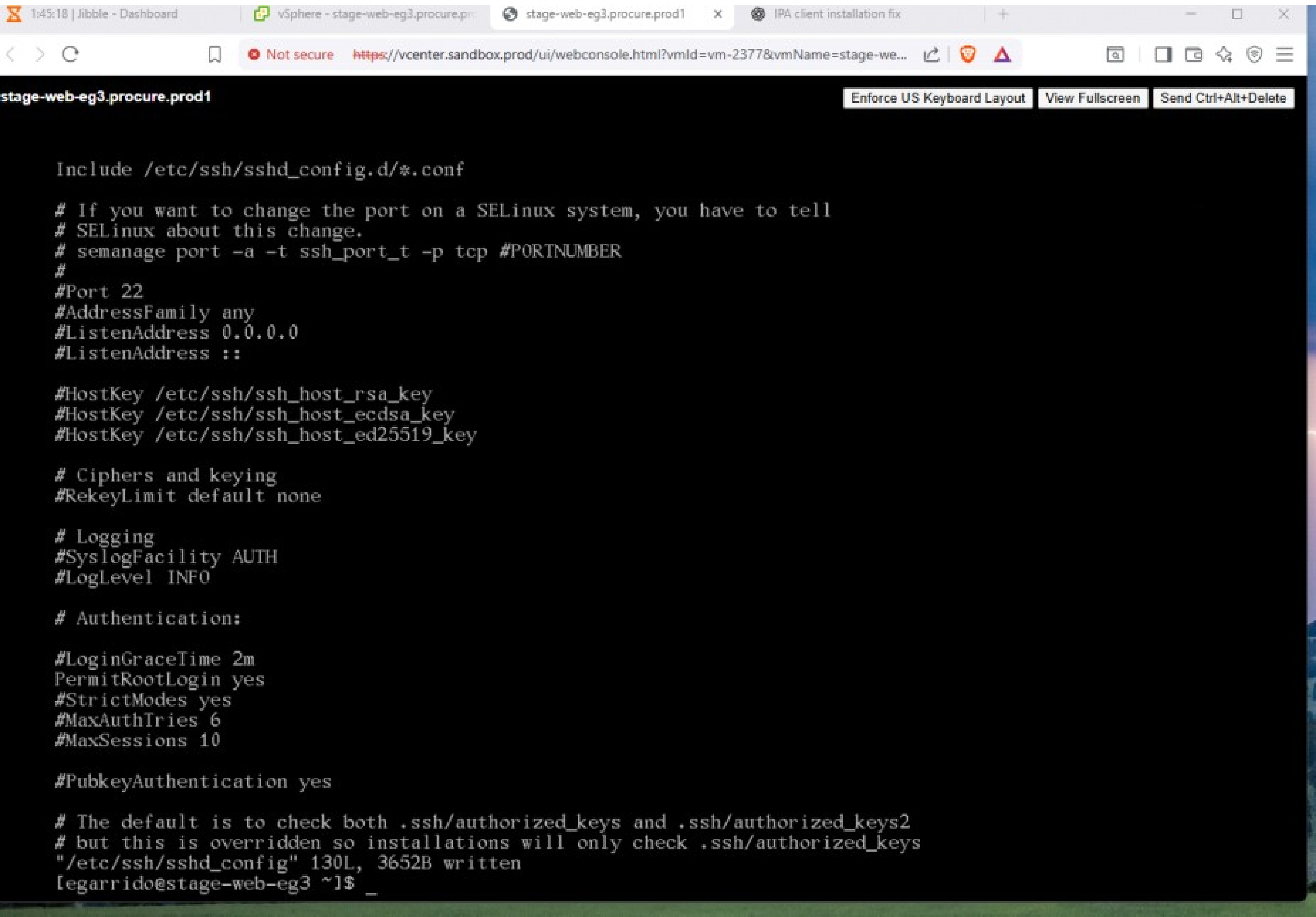
```
[egarrido@dev-ansible ~]$ ansible -m ping dev-eg3
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details
dev-performance-eg3.procore.prod1 | UNREACHABLE! => {
    "changed": false,
    "msg": "Failed to connect to the host via ssh: Connection closed by UNKNOWN port 65535",
    "unreachable": true
}
stage-web-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
dev-app-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
[egarrido@dev-ansible ~]$ sudo vi /etc/ansible/hosts
[sudo] password for egarrido:
[egarrido@dev-ansible ~]$ ansible -m ping dev-eg3
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details
stage-web-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
dev-app-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
dev-performance-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
[egarrido@dev-ansible ~]$
```

This screenshot shows the successful completion of a FreeIPA client installation on stage-web-eg3.procore.prod1. The system enrolls into the PROCORE.DEV realm, installs and trusts the Certificate Authority, and configures core identity services including SSSD, Kerberos, LDAP, and SSH. During the process, DNS updates for forward and reverse records are attempted but reported as missing; these warnings do not prevent successful enrollment. SELinux initializes required policies, and the installation concludes with confirmation that the ipa-client-install command completed successfully. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.


1:43:23 | Jibble - Dashboard
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
IPA client installation fix
Not secure https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2377&vmName=stage-we...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

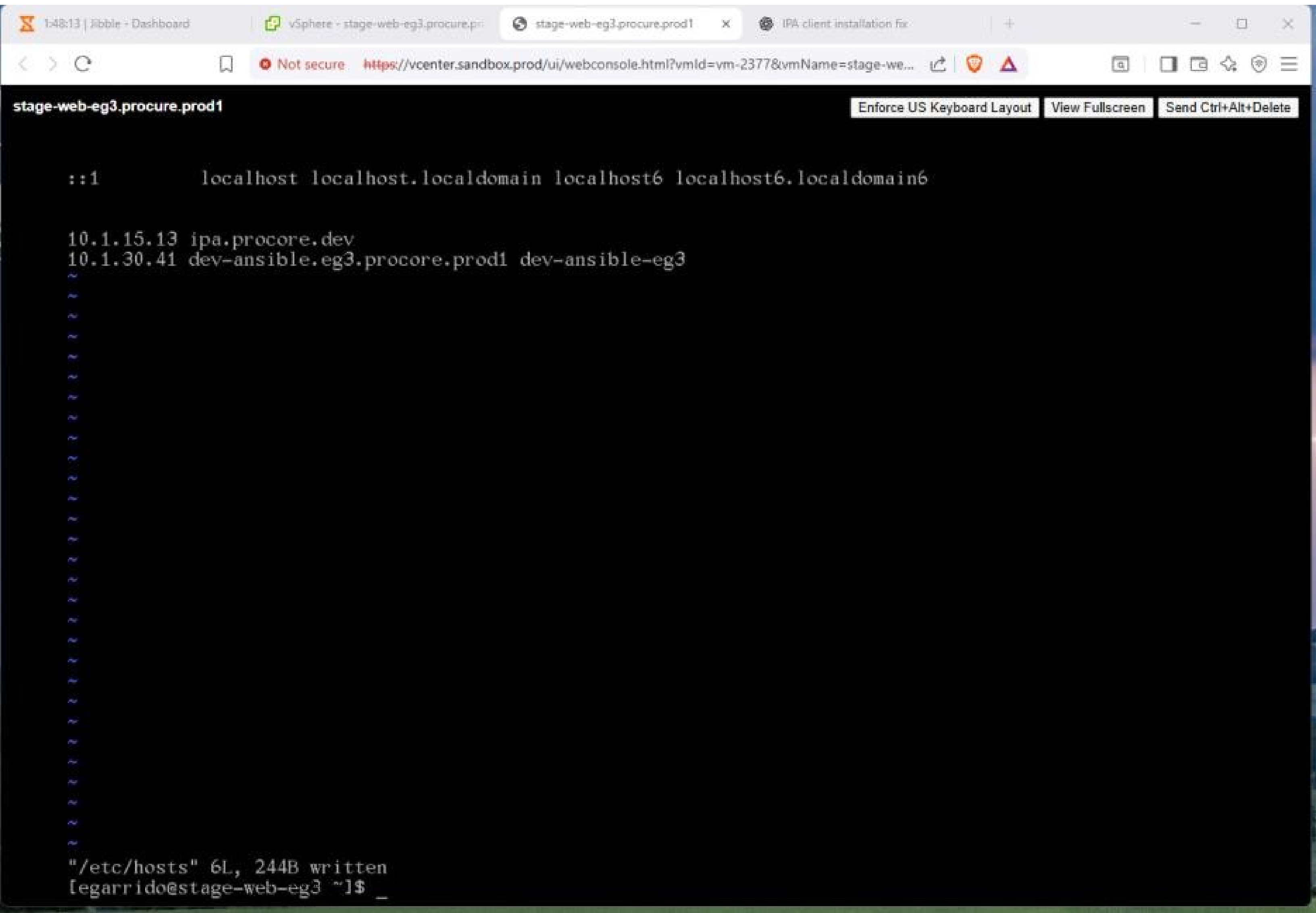
```
    Issuer:     CN=Certificate Authority,O=PROCORE.DEV
    Valid From:  2024-06-03 22:41:02+00:00
    Valid Until: 2044-06-03 22:41:02+00:00

Enrolled in IPA realm PROCORE.DEV
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Hostname (stage-web-eg3.procore.prod1) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host stage-web-eg3.procore.prod1: 10.1.31.136.
Missing reverse record(s) for address(es): 10.1.31.136.
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Could not update DNS SSHFP records.
[ 9231.050121] systemd-rc-local-generator[18100]: /etc/rc.d/rc.local is not marked executable, skipping.
SSSD enabled
[ 9233.150677] SELinux:  Converting 459 SID table entries...
[ 9233.166831] SELinux:  policy capability network_peer_controls=1
[ 9233.167532] SELinux:  policy capability open_perms=1
[ 9233.168179] SELinux:  policy capability extended_socket_class=1
[ 9233.168807] SELinux:  policy capability always_check_network=0
[ 9233.169455] SELinux:  policy capability cgroup_seclabel=1
[ 9233.170081] SELinux:  policy capability nnp_nosuid_transition=1
[ 9233.170726] SELinux:  policy capability genfs_seclabel_symlinks=1
[ 9234.999754] systemd-rc-local-generator[18145]: /etc/rc.d/rc.local is not marked executable, skipping.
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring procore.dev as NIS domain.
[ 9236.323958] systemd-rc-local-generator[18178]: /etc/rc.d/rc.local is not marked executable, skipping.
Configured /etc/krb5.conf for IPA realm PROCORE.DEV
Client configuration complete.
The ipa-client-install command was successful
[root@stage-web-eg3 ~]# _
```

This screenshot shows the OpenSSH daemon configuration (/etc/ssh/sshd_config) on stage-web-eg3.procore.prod1. The file includes the main configuration directives along with an Include statement for additional configuration snippets under sshd_config.d. Core SSH settings for ports, address families, host keys, logging, authentication behavior, and security controls are visible, reflecting a standard, hardened baseline configuration. The file has been saved successfully after review or modification. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.


1:45:18 | Jibble - Dashboard
vSphere - stage-web-eg3.procure.pr
stage-web-eg3.procure.prod1
IPA client installation fix
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2377&vmName=stage-we...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

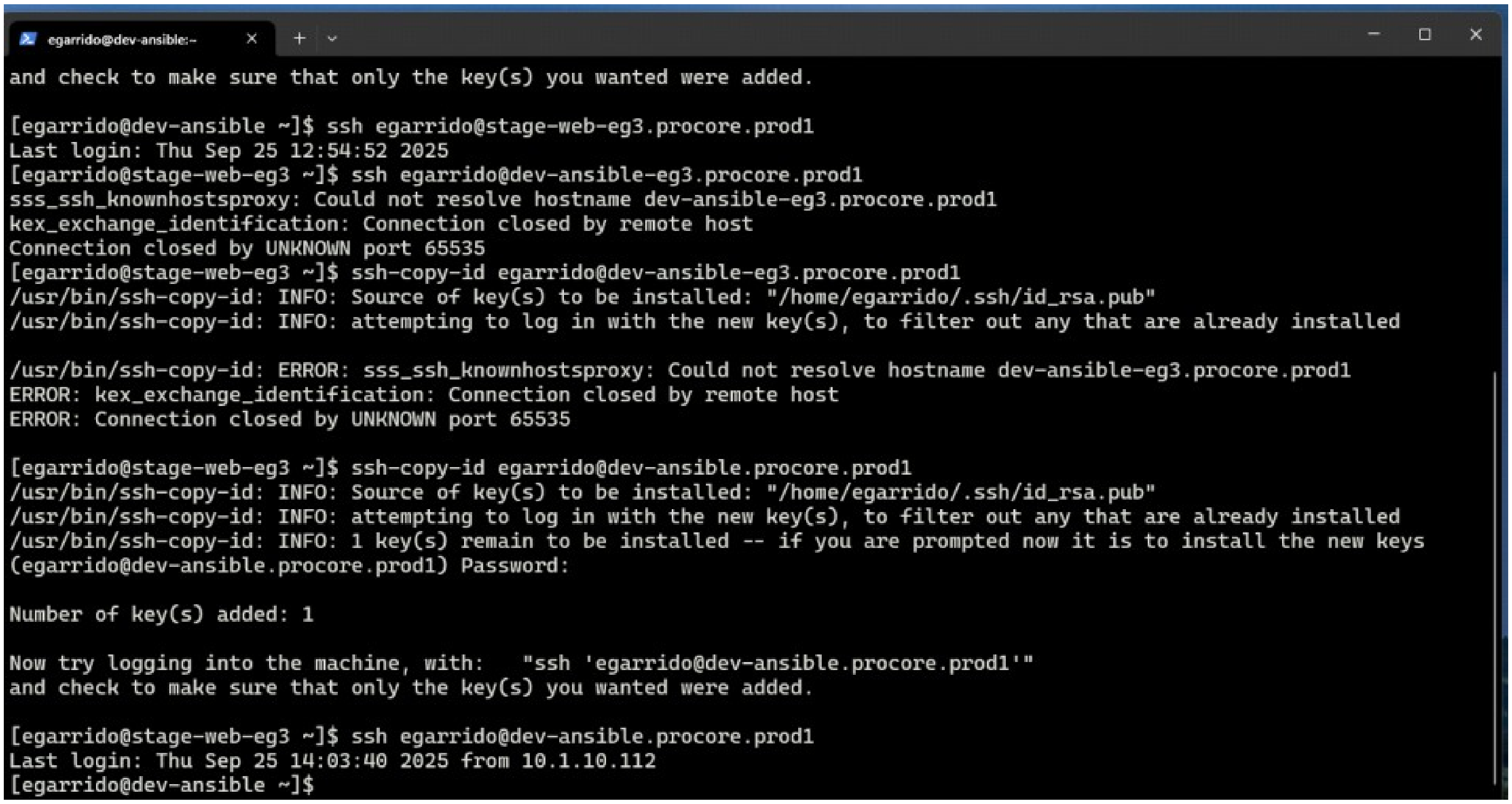
```
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
"/etc/ssh/sshd_config" 130L, 3652B written
[egarrido@stage-web-eg3 ~]$ _
```

This screenshot shows the /etc/hosts file on stage-web-eg3.procore.prod1 after being updated and saved successfully. The file includes localhost entries and custom static hostname mappings for internal infrastructure services, such as the FreeIPA server and the Ansible management host, ensuring reliable local name resolution. The write confirmation indicates the changes were committed without errors. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.


1:48:13 | Jibble - Dashboard
vSphere - stage-web-eg3.procure.p
stage-web-eg3.procure.prod1
IPA client installation fix
Not secure
https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2377&vmName=stage-we...
stage-web-eg3.procure.prod1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

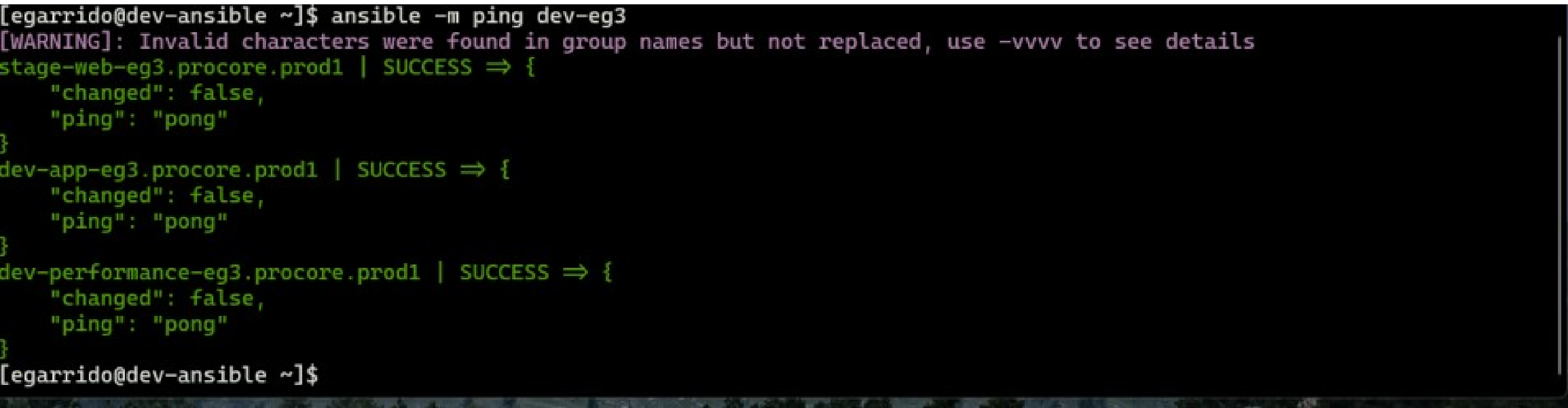
```
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6


10.1.15.13 ipa.procore.dev
10.1.30.41 dev-ansible.eg3.procore.prod1 dev-ansible-eg3
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 6L, 244B written
[egarrido@stage-web-eg3 ~]$ _
```

This screenshot captures SSH troubleshooting and resolution of hostname and trust issues between hosts. An initial SSH attempt fails due to hostname resolution problems and an unexpected port closure, indicating missing or incorrect name resolution and known_hosts data. After correcting the target hostname and re-running ssh-copy-id, the public key is successfully installed. A follow-up SSH login confirms successful, trusted access to the Ansible management host. This validates proper hostname resolution, SSH key distribution, and restored connectivity. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.



```
and check to make sure that only the key(s) you wanted were added.

[egarrido@dev-ansible ~]$ ssh egarrido@stage-web-eg3.procore.prod1
Last login: Thu Sep 25 12:54:52 2025
[egarrido@stage-web-eg3 ~]$ ssh egarrido@dev-ansible-eg3.procore.prod1
sss_ssh_knownhostsproxy: Could not resolve hostname dev-ansible-eg3.procore.prod1
kex_exchange_identification: Connection closed by remote host
Connection closed by UNKNOWN port 65535
[egarrido@stage-web-eg3 ~]$ ssh-copy-id egarrido@dev-ansible-eg3.procore.prod1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/egarrido/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: ERROR: sss_ssh_knownhostsproxy: Could not resolve hostname dev-ansible-eg3.procore.prod1
ERROR: kex_exchange_identification: Connection closed by remote host
ERROR: Connection closed by UNKNOWN port 65535

[egarrido@stage-web-eg3 ~]$ ssh-copy-id egarrido@dev-ansible.procore.prod1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/egarrido/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
(egarrido@dev-ansible.procore.prod1) Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'egarrido@dev-ansible.procore.prod1'"
and check to make sure that only the key(s) you wanted were added.

[egarrido@stage-web-eg3 ~]$ ssh egarrido@dev-ansible.procore.prod1
Last login: Thu Sep 25 14:03:40 2025 from 10.1.10.112
[egarrido@dev-ansible ~]$
```

This screenshot shows a successful Ansible connectivity verification using the ansible -m ping module against the dev-eg3 inventory group. Despite a non-blocking warning about invalid characters in group names, all targeted hosts respond with SUCCESS and a pong message, confirming functional SSH access, correct inventory configuration, and readiness for Ansible automation tasks. All IP addresses, hostnames, and environment-specific details shown are sanitized for security purposes.



```
[egarrido@dev-ansible ~]$ ansible -m ping dev-eg3
[WARNING]: Invalid characters were found in group names but not replaced, use -vvvv to see details
stage-web-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
dev-app-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
dev-performance-eg3.procore.prod1 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
[egarrido@dev-ansible ~]$
```

Summary

This project demonstrates the successful setup and validation of centralized identity management, secure SSH access, and Ansible connectivity across a multi-host Linux environment. Systems are enrolled into a FreeIPA domain, SSH key-based authentication is configured and verified, and hostname resolution and SSH trust issues are identified and resolved. Ansible inventory and connectivity are tested and confirmed using the ping module, ensuring the environment is ready for reliable automation. All IP addresses, hostnames, usernames, and environment-specific details shown are sanitized for security purposes.