Tutorial Link https://course.testpad.chitkara.edu.in/tutorials/ACL with System commands and Linux Directory Service/6305aa775611a5348833e4f5

TUTORIAL

ACL with System commands and Linux Directory Service

Topics

Account Authentication

One way of simplifying your authentication environment is to use a single authentication source for all of your nodes — Windows, Linux, or Unix. You can authenticate them all against a directory service such as Active Directory or eDirectory.

Difference Between LDAP, OpenLDAP and Active Directory

LDAP is the protocol that defines how users, devices, and clients can communicate with a directory server. It also provides a framework for how information can be organized and represented within a directory.

These frameworks are flexible and customizable, so different directories can be formatted differently, but they tend to follow a hierarchical tree structure.

With LDAP, users access IT resources by inputting credentials. The protocol searches and compares the credentials to what the LDAP server has stored for the authenticating user — if the username and password match what's listed in the directory, LDAP authenticates the user.

By using LDAP, you can centralize authentication services while providing users with quick access to many of their resources on the network.

The LDAP protocol is not software, but software packages have emerged to streamline LDAP directory creation, implementation, and management. One of the first implementations of this was OpenLDAP.

OpenLDAP is a free, open-source implementation of the LDAP protocol. Because it's a common, free iteration available to anyone, OpenLDAP is sometimes referred to as just "LDAP." However, it is more than just the protocol; it's light LDAP directory software.

OpenLDAP can be used on any platform. In contrast to other implementations that offer more robust features like a GUI and often a suite of other protocols and functionality (often, at a cost), OpenLDAP is a highly focused LDAP option that's customizable and supports all major computing platforms.

While flexibility may sound like a plus (and it often is), it can make the software more difficult to navigate. This, paired with its lack of interface, means it can require significant expertise to implement and manage.

Microsoft Active Directory (AD) is a directory service that stores user and device account data in a central location for Windows-based network, device, application, and file access.

AD is more feature-rich than OpenLDAP: it includes a GUI and more robust configuration features like Group Policy Objects for Windows devices. While OpenLDAP only uses the LDAP protocol, AD uses other protocols in addition to LDAP.

In fact, LDAP is not AD's primary protocol; instead, it leverages an implementation of Microsoft's proprietary Lightweight Directory Access Protocol and primarily uses Kerberos, Microsoft's main proprietary authentication protocol.

While AD may seem more robust overall, OpenLDAP's exclusive focus on the LDAP protocol gives it far greater depth than AD offers.

Of course, the cost difference reflects the notion of a wider breadth of functionality and the commercial nature of Microsoft solutions: OpenLDAP is free, and AD is not.

AD requires licensing, and because it runs on premised equipment, the costs of AD hardware and maintenance can add up.

While AD offers more capabilities outside the LDAP protocol, OpenLDAP is more flexible and customizable when it comes to implementation. When considering these two, businesses should decide whether they're more interested in flexibility (OpenLDAP) or ease of use (AD).

For some organizations, OpenLDAP vs. Active Directory is a better fit. Specifically, for organizations that leverage Linux-based systems and applications, networking gear, and NAS and SAN storage systems, LDAP is often the preferred protocol for those IT resources.

Further, for organizations that leverage data centers or cloud infrastructure-as-a-service technology, leveraging an OpenLDAP server is often far more effective than Active Directory.

Of course, Active Directory has its advantages as well. For organizations that are largely Windows-based and intend to leverage only Azure cloud infrastructure, the combination of Active Directory and Azure AD can be quite beneficial.

Even in this case, though, many IT organizations opt to leverage OpenLDAP as well, because of Azure AD's lack of LDAP support for cloud infrastructure.

What Are the Main Reasons to Choose OpenLDAP?

Many organizations opt for OpenLDAP for the flexibility and cost savings. OpenLDAP is highly configurable for skilled engineers, making it a better choice for organizations with niche or nuanced needs.

Additionally, it's compatible with nearly every platform or OS, while AD works best with Windows devices. Organizations that use or plan to use Mac, Linux, or other systems often choose OpenLDAP. Those with legacy applications or those that are based on Linux will often also choose OpenLDAP.

Why Should You Consider Active Directory?

If your environment is fully homogenous and based only on Microsoft and Windows, AD might be the best choice. In a Windows environment, IT administrators can use the Windows-based Active Directory Users and Computers console to perform nearly all management tasks.

However, even in these environments, you still need to consider how to account for mobile and SaaS applications, Mac and Linux device support, non-Windows-based file servers, and networking gear, as AD generally does not support them without integrations or add-ons.

AD offers an easy-to-use GUI for configuring settings and managing users and groups. For those who are less experienced with configuring open-source software, OpenLDAP's lack of interface can be an uphill battle, making AD the better choice.

While OpenLDAP and the LDAP protocol precede Microsoft's entrance into the directory services space, Microsoft AD has garnered the lion's share of the market — although, with the advent of cloud directories the IAM landscape is starting to shift.

This, in combination with its more user-friendly suite of tools, can make it an attractive choice for Windows/Azure centric organizations.

AD also offers more protocols than just LDAP while OpenLDAP is LDAP-exclusive. Multi-protocol directory services are growing in popularity as networks expand and disperse; companies need to authenticate users to a higher number and wider variety of resources, and different resources tend to work best with different protocols.

In environments with heavy reliance on cloud apps, SAML and SSO solutions are better suited. In this case, both AD and OpenLDAP require an additional identity and access management tool.

Ideally, an IAM tool or directory service should be able to authenticate and authorize users to *all* their IT resources, wherever they are (including the cloud), using whichever protocol best suits the task. This is one area where both OpenLDAP and AD fall short.

Access Control Lists(ACL) in Linux

What is ACL ?

Access control list (ACL) provides an additional, more flexible permission mechanism for file systems. It is designed to assist with UNIX file permissions. ACL allows you to give permissions for any user or group to any disc resource.

Use of ACL :

Think of a scenario in which a particular user is not a member of group created by you but still you want to give some read or write access, how can you do it without making user a member of group, here comes in picture Access Control Lists, ACL helps us to do this trick.

Basically, ACLs are used to make a flexible permission mechanism in Linux.

From Linux man pages, ACLs are used to define more fine-grained discretionary access rights for files and directories

Commands for ACL:

1.Create a file file1 using touch command. Now run ls -l command to see its permission. Select any other user for which we have to assign full permission

2. use getfacl command to display file permissions

```
#      getfacl file1
```

3. set permission for a user codequotient as

```
# setfacl -m u:codequotient:rwx file1
```

4. Set permission for any group

```
# setfacl -m g:codequotient:rwx file1
```

5. Remove permission using setfacl

```
# setfacl -x u:codequotient file1
```

6. Take all assigned permission back

```
# setfacl -b file1
```

System Monitoring Commands

1. top : To see Live process and system performance

2. VmStat : To see Virtual Memory Statistics

3. lsof : To see List Open Files

4. tcpdump -i eth0 : To see Network Packet Analyzer

5. Netstat -a : To see Network Statistics

6. iftop : To see Network Bandwidth Monitoring

7. df : To see disk partitions

8. du : To see disk usage

9. iostat : To see input output statstics

10. free : To see Free space

11. cat /etc/meminfo

12 cat /etc/cpuinfo

13 netstat -rnv to see route, numeric and verbrose information

14 du -h

system maintenance commands in linux

1. init 0 - init 6 : Used for various run levels
2. reboot : Used for rebooting Linux Server or you can use init 6
3. shutdown: To shutdown your PC.You can also use init 0
4. halt : To Power Off Linux PC forcefully.
5. Change system hostname: In RHEL6 use /etc/sysconfig/network file to change Hostname.In RHEL 7 and use /etc/hostname.
6. cat /etc/redhat-release : To see System information
7. uname -a : To see system information
8. dmidecode : To see System information
9. hostname : to see System Hostname
10. arch or uname -a command can be used to see details about system architecture

Terminal Commands

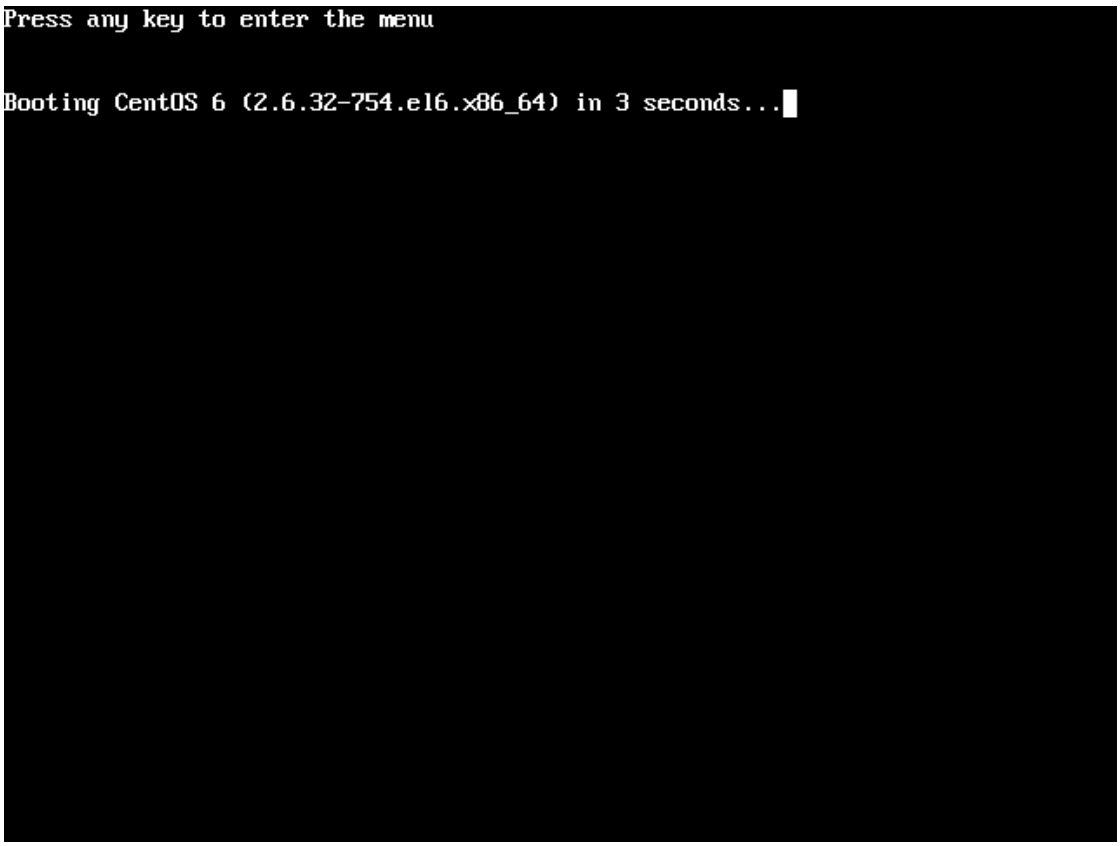
1. Control + u :To erase everything you have typed on current command
2. Control + c : To terminate current running program or command
3. Control + z :To suspend current program or command
4. Control + d :To Exit from an interactive command or program
5. clear :To clear terminal

6. exit : To exit from current user or session
7. script script_name : To start a script which records all of your commands. After completing the session you can use exit command.

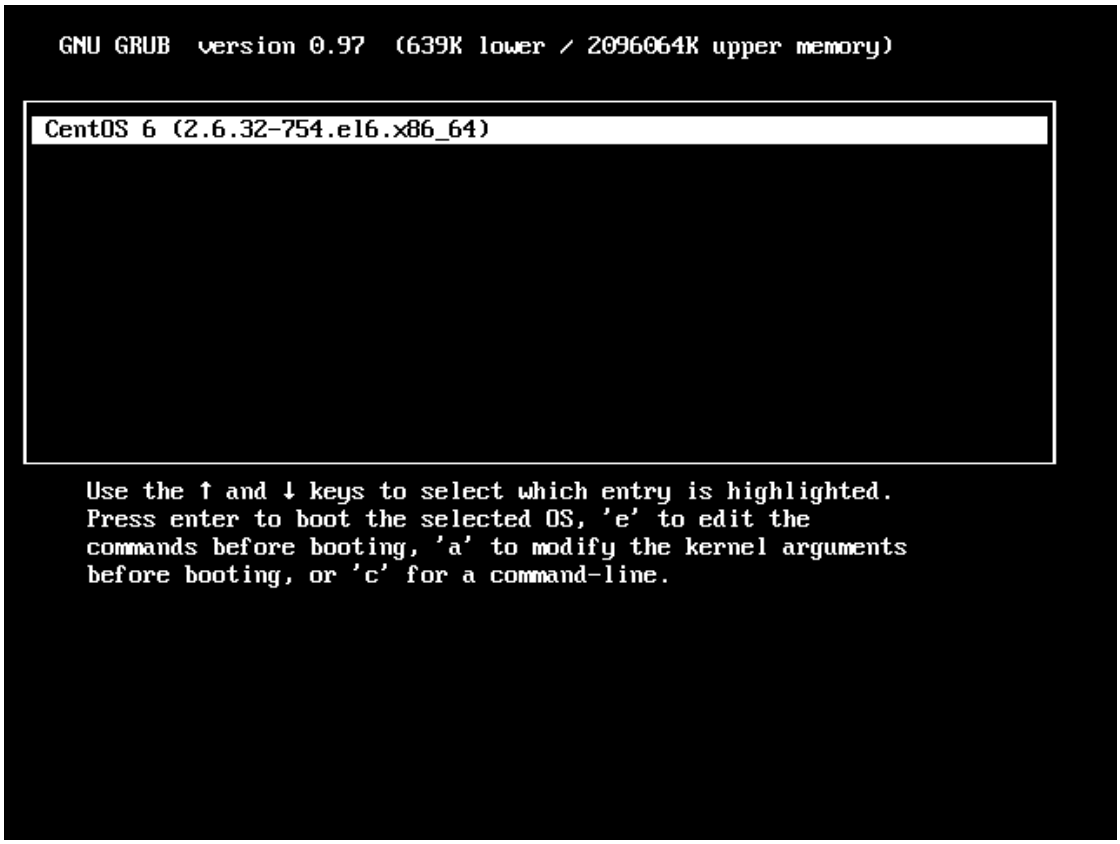
Recover Root Password in Linux

Method: Reset forgotten root password by booting into single user mode

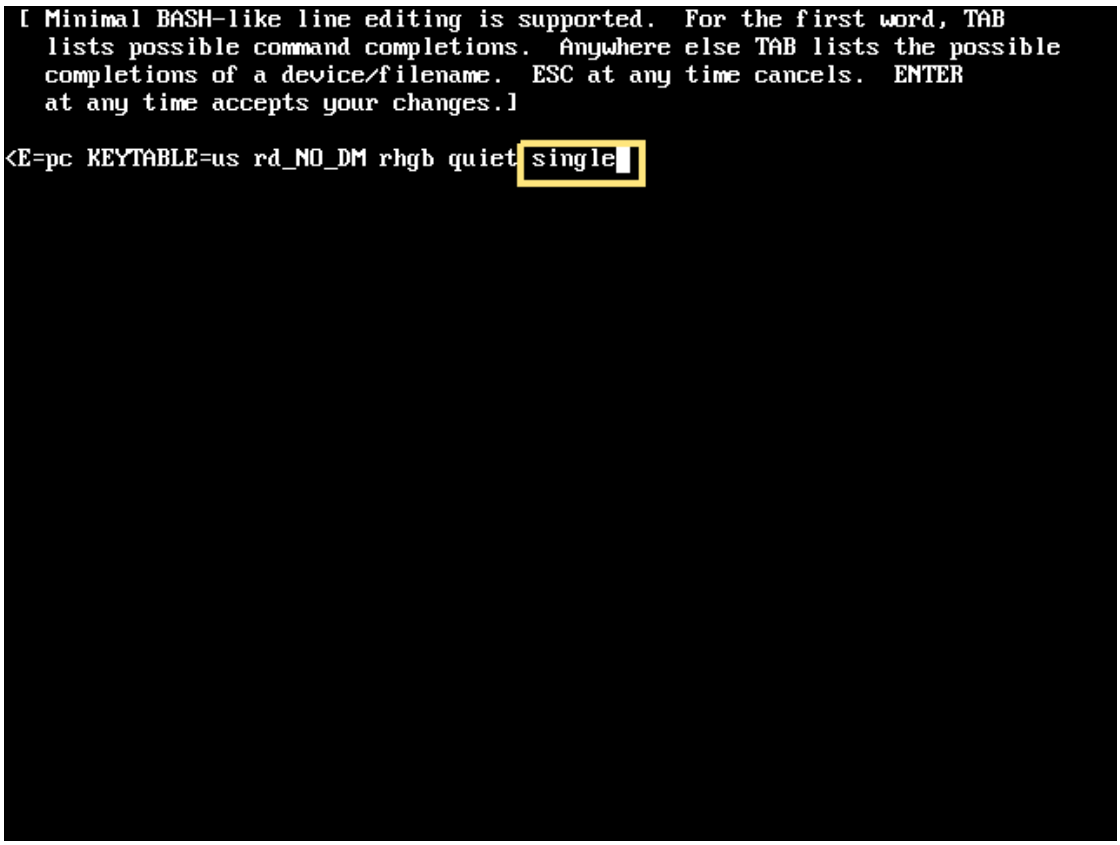
`Step-1:` Reboot your system and interrupt in boot screen by using any key from your keyboard to launch the GRUB Menu.



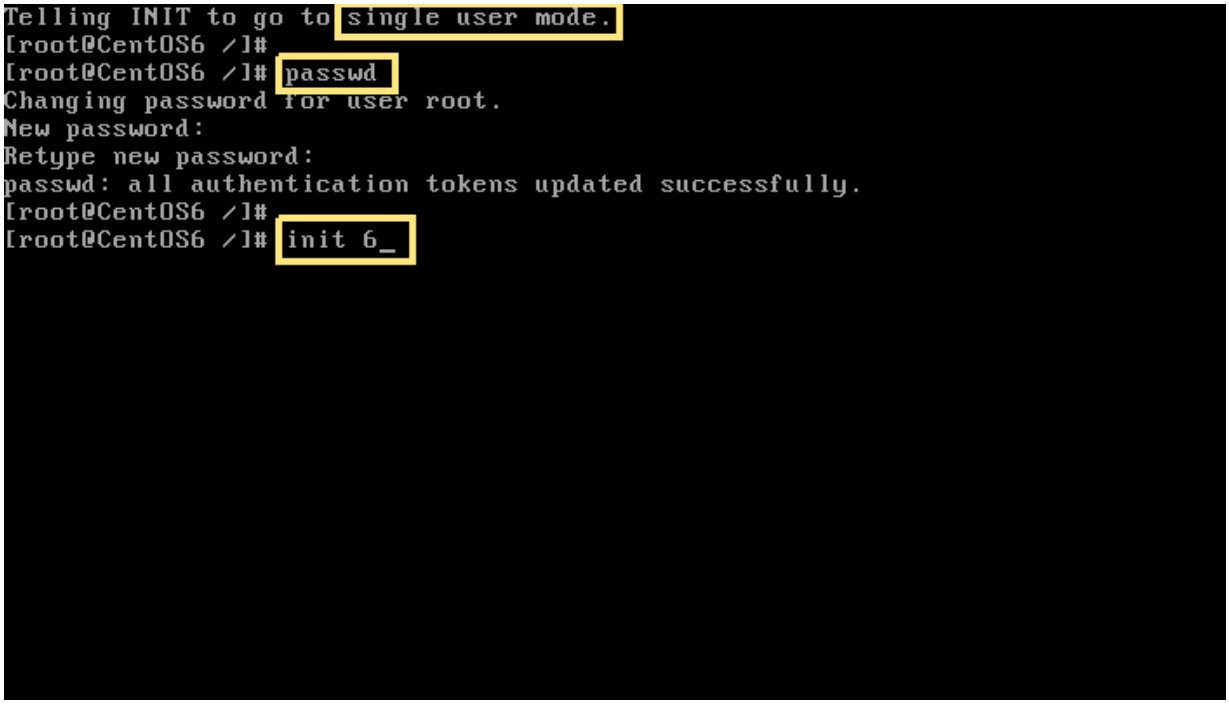
`Step-2:` In GRUB Menu, hit `a` key to modify the kernel arguments.



Step-3: Append `S` or `single` or `1` after a space at the end of the line and press `Enter` key to boot into single user mode.



Step-4: Once you hit `Enter` key then it will take to you into single user mode. Just type `passwd` command to reset the root user password. Finally reboot the system by issuing `init 6` or `shutdown -r now` command.



Step-5: Now you can login to your system with your new password.

Method-2: Reset forgotten root password by booting into rescue mode

Step-1: Insert the bootable media through USB or DVD drive which is compatible for you and reboot your system. It will take to you to the below screen. Hit `Rescue installed system` to launch the `Rescue` mode.