

How To Make The Best Use Of Live Sessions

- Please login on time
- Please do a check on your network connection and audio before the class to have a smooth session
- All participants will be on mute, by default. You will be unmuted when requested or as needed
- Please use the “Questions” panel on your webinar tool to interact with the instructor at any point during the class
- Ask and answer questions to make your learning interactive
- Please have the support phone number (US : 1855 818 0063 (toll free), India : +91 90191 17772) and raise tickets from LMS in case of any issues with the tool
- Most often logging off or rejoining will help solve the tool related issues

COURSE OUTLINE



MODULE 8

INTRODUCTION TO LINUX

INSTALLATION AND INITIALISATION

USER ADMINISTRATION

BOOT AND PACKAGE MANAGEMENT

NETWORKING

LINUX OVERVIEW AND SCRIPTING

LINUX FOR SOFTWARE DEVELOPMENT

SECURITY ADMINISTRATION

Objectives

After completing this module, you should be able to:

- Understand security administration
- Learn secure boot options
- Secure through ssh
- Learn about Antivirus in Linux
- Understand Virtualization



edureka!



Security Administration

Importance Of Security In IT Industry

01

May lose their confidential documents and the edge over their competitors.

02

Losing sensitive data may hinder the trust of the customer which will be difficult to regain.

03

Productivity loss if a program source code is tampered with. It may lead to re-writing the program.

04

Attacks such as phishing may broadcast wrong information to the receiver.

04

May hamper the performance of the software by attacks like traffic congestion.

Operating System Security

- OS security is ensuring OS integrity, confidentiality and availability.
- OS security allows different programs to stop unauthorized interference.

01

Perform regular OS updates.

02

Install Antivirus and regularly update it for new malwares and threats.

03

Keep a check on the incoming and outgoing traffic through firewall and restrict unauthorized access.

04

Create multiple accounts and provide permission adequately.

SELinux

SELinux Overview

1

Security-enhanced Linux (SELinux) is an implementation of a mandatory access control mechanism.

2

A Mandatory Access Control framework allows you to define permissions for how all processes interact with other parts of the system such as files, devices, sockets, ports, and other processes.

3

With this model, a process can be granted just the permissions it needs to be functional.

4

It follows the principle of least privilege.

5

SELinux is a set of kernel modifications and user-space tools that have been added to various Linux distributions.

6

It is a project of the United States National Security Agency (NSA) and the SELinux community.

SELinux Contexts

- Processes and files are labelled with a SELinux context that contains additional information, such as a SELinux user, role, type, and, optionally, a level.
- When running SELinux, all of this information is used to make access control decisions.

```
~]$ ls -Z file1  
-rwxrw-r-- user1 group1 unconfined_u:object_r:user_home_t:s0 file1
```

↑
User

↑
Role

↑
Type

↑
Level

SELinux Contexts Fields

User

- It is an identity known to the policy that is authorized for a specific set of roles.
- Run the `semanage login -l` command as the Linux root user to view a list of mappings between SELinux and Linux user accounts.

Role

- The role is an attribute of Role-Based Access Control (RBAC) security model.
- SELinux users are authorized for roles, and roles are authorized for domains.

Type

- Defines a domain for processes, and a type for files.
- Access is only allowed if a specific SELinux policy rule exists that allows it.

Level

- MLS range is a pair of levels, written as *lowlevel-highlevel* if the levels differ, or *lowlevel* if the levels are identical.
- Each level is a sensitivity-category pair, with categories being optional.

SELinux Status And Mode

The sestatus command returns the SELinux status and SELinux policy being used.

The status of SELinux can be :

Enforcing: SELinux security policy is enforced.

Permissive: SELinux prints warning instead of enforcing.

Disabled: No SELinux policy is loaded.

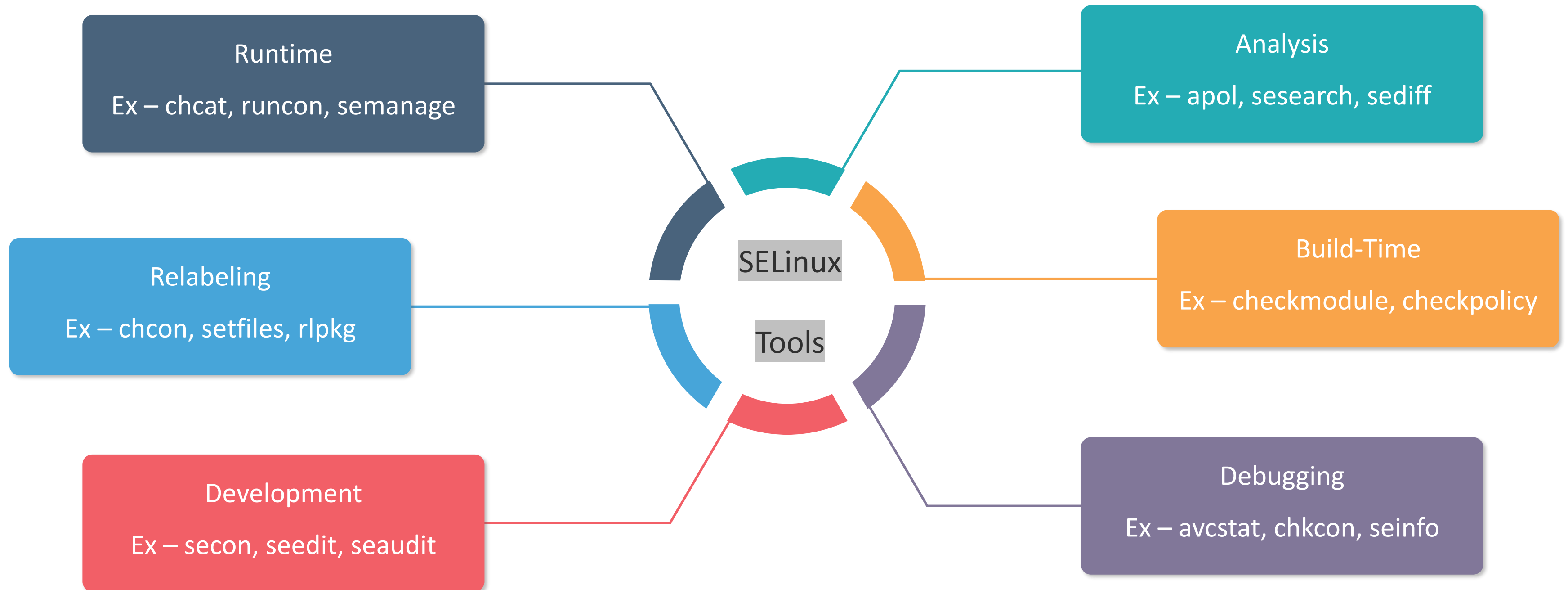
We can modify the status by
changing:

**'configure SELINUX=permissive' in
/etc/selinux/config.**

SE Boolean

- Booleans allow parts of SELinux policy to be changed at runtime, without any knowledge of SELinux policy writing.
- For a list of Booleans, an explanation of what each one is, and whether they are on or off, run the `semanage boolean -l` command as the Linux root user.
- Run the `setsebool` utility in the `setsebool boolean_name on/off` form to enable or disable Booleans.

SELinux Tools



Information Gathering Tools

avcstat

- This provides a short output of the access vector cache statistics since boot.
- You can watch the statistics in real time by specifying a time interval in seconds. The statistics file used is:
`/selinux/avc/cache_stats`, and you can specify a different cache file with the `-f` `/path/to/file`.

seinfo

- This utility is useful in describing the break down of a policy, such as:
 - the number of classes, types, Booleans, allow rules, etc.

sesearch

- Lets you search for a particular type in the policy.
- Some options are :
- `-t` : search for that have `<name>` as target.
- `-p` : search one or more specific permissions.
- `--allow` : search for only allow rules.
- `-a` : show all rules

seaudit

The seaudit application is designed to help you read, sort, and query your SELinux audit messages.

It is necessary to have super-user privileges to run seaudit, because it looks into system logs.

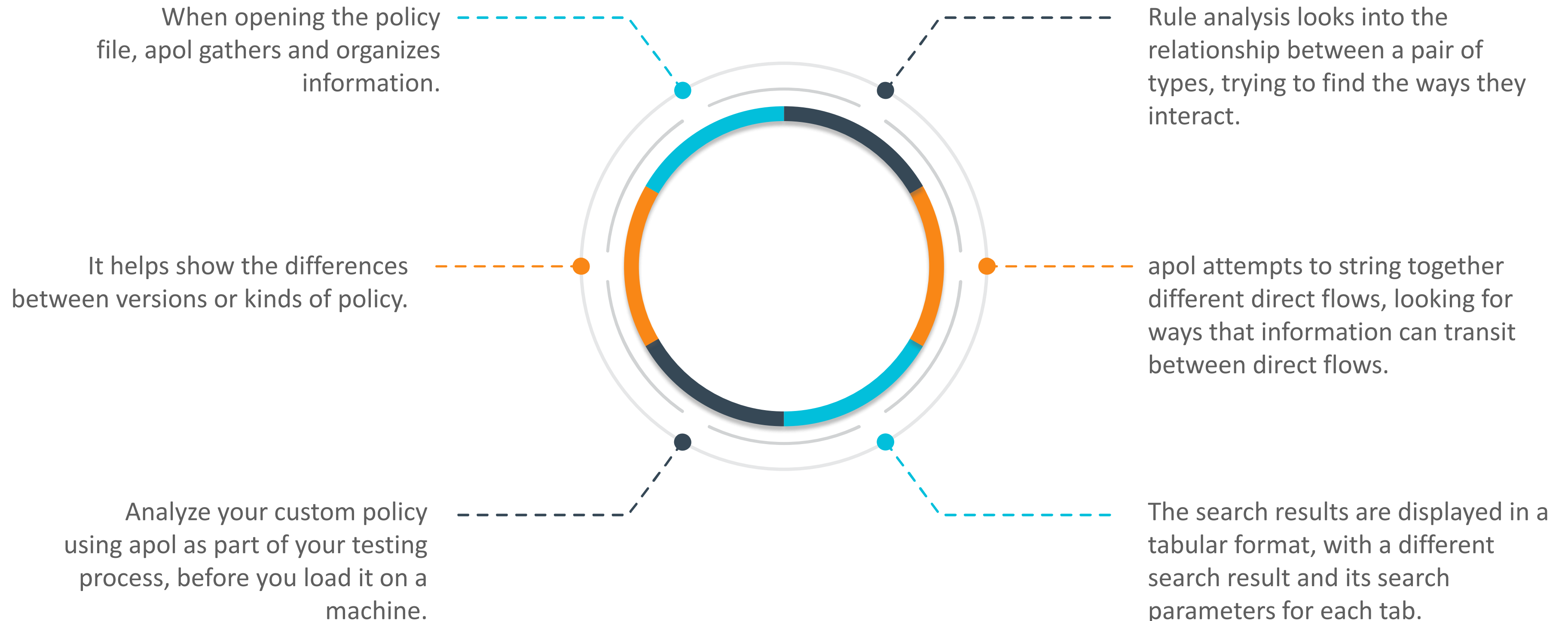
seaudit can use both binary and source policy files.

You can choose which log and policy file to use when starting the application.

You can open multiple views into the same log by opening additional tabs.

Full regular expression support is enabled for the Query policy window.





Grub – Security

Grub - Security

- If an attacker gets physical access to your hosts and are able to reboot those hosts, can sign into single user mode and change your root password.
- The user can intervene boot process by pressing a key and then by using a menu can select alternate kernels or specify additional parameters, such as booting into single user mode.
- The GRUB boot loader is the default boot loader installed by most Linux.
- To secure the GRUB boot loader, we can apply a password to the whole loader, to allow the loading of an additional menu for authenticated users.
- These controls are specified in the grub.conf configuration file that is located in the /boot/grub/ directory.

Grub.conf

- In this grub.conf file, we can see a line similar to :

```
password -md5 $1$3Gq.k1$Swh2Z8swBjRp2wvncjVaa0
```

- Steps to enable password on grub.

```
# grub
grub> md5crypt
md5crypt
Password: password
password
Encrypted: 5123tfghj1290poisw5.tghw$kcwdefrg
```

- Copy and paste the password in grub.conf file.

Grub.conf (continued)

- Using the password option, you can also specify a menu that can be launched when the appropriate password is entered.

```
password --md5 $1$3Gq.k1$Swh2Z8swBjRp2wvncjVaa0  
/boot/grub/admin-menu.lst
```

- When the appropriate password is entered, the menu specified in the **/boot/grub/admin-menu.lst** file would be displayed.
- You can also specify a password for each kernel entry by replacing the lock option with a password option.
- You also need to ensure the grub.conf file has suitable ownership and permissions. The file should be owned by root and have permissions of 0600.

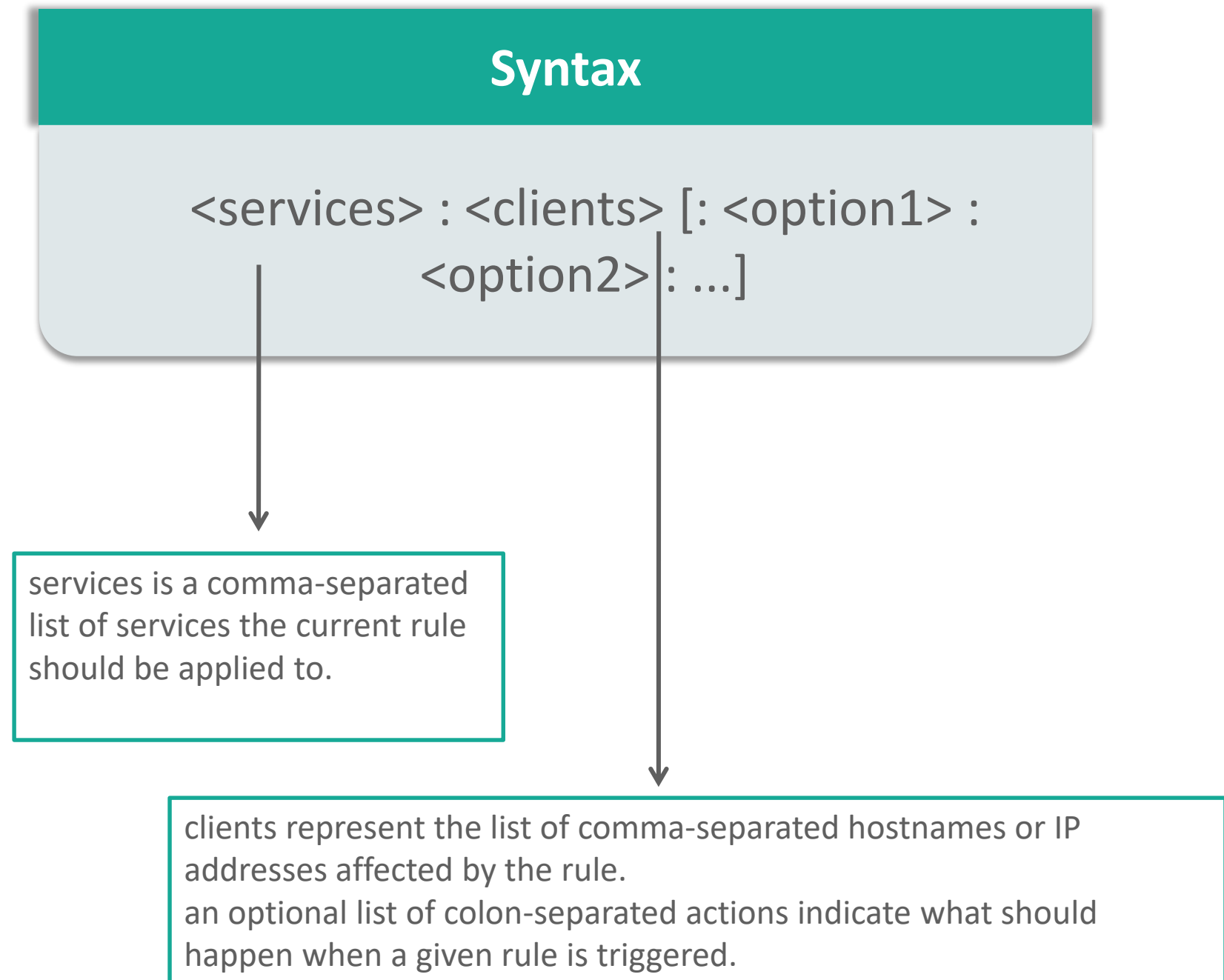


Additional Security Tools

TCP Wrappers

- When a network request reaches your server, TCP wrappers uses :
 - ‘hosts.allow’ and
 - ‘hosts.deny’ (in that order)
- to determine if the client should be allowed to use a given service.
- By default, these files are empty, all commented out, or do not exist.

Allowing access to a given service in /etc/hosts.allow takes precedence over a rule in /etc/hosts.deny prohibiting it.



TCP Wrappers - Example

- In this example we need to :

- Only allow SSH and FTP,
- Allow access to 10.10.1.123 and localhost and
- Deny all others, add this line in /etc/hosts.deny :
- Add following line in /etc/hosts.allow :

ALL:ALL

sshd,vsftpd : 10.10.1.123 , LOCAL

- These changes take place immediately without the need for a restart.
- To allow all services to hosts where the name contains example.com, add this line in hosts.allow :

ALL : .example.com

TCP Wrappers Benefit

Connections that are monitored by TCP wrapper are reported through the syslog facility.

01 Logging

02 Access Control

TCP wrapper supports a simple form of access control that is based on pattern matching. You can even hook the execution of shell commands/script when a pattern matches

TCP wrapper verifies the client host name that is returned by the address->name DNS server by looking at the host name and address that are returned by the name->address DNS server.

03 Host Name Verification

04 Spoofin Protection

/etc/inetd.conf

- 'inetd' will load a network program based upon a request from the network.
- The 'inetd.conf' file tells inetd which ports to listen to and what server to start for each port.
- Edit the 'inetd.conf' file and disable services (like ftp, telnet, shell, login, exec, talk, ntalk, imap, auth, etc.) unless you plan to use it.
- Change the permissions on this file to 600.
- Ensure that the owner is root.
- Secure the 'inetd.conf' file is to set it immutable, using the chattr command. A file with the immutable attribute set 'I' cannot be modified, deleted or renamed.

Xinetd

01

Xinetd is used to prevent a specific TCP service from being invoked on your system.

02

Locate a particular service in `'/etc/xinetd.conf'` and `disable=yes`

03

Send SIGUSR2 signal to inform xinetd of your changes.

04

One of the real strengths of Xinetd is its extensive logging capability. You can configure logging for each service individually.

05

xinetd allows you to redirect TCP connections to a different host.

Securing Shell

Change The Default Port

- By default, SSH uses port 22, but it is possible to change the port number.
- This will make it more difficult to attack your server using SSH, as an attacker would first need to locate and identify the port.
- You can choose any number higher than 1024 and lower than 65535.
- Steps to change port are :
 - Step-1** : `vi /etc/ssh/sshd_config`
 - Step-2** : modify 'port 22' to 'port <portno>'
 - Step-3** : `/etc/init.d/sshd restart`

Disable Root Access

Disabling direct access as root will make it harder for malicious individuals to log in as an administrator.

- If can use "sudo" or "su", there is no need for direct access by the 'root' user.
- One needs to login into an account and then get the root permission.
- The attacker must invade two accounts before it can harm the system.
- Steps to disable root access are :
 - Step-1** : `vi /etc/ssh/sshd_config`
 - Step-2** : Set 'PermitRootLogin no' and save
 - Step-3** : `/etc/init.d/sshd restart`

IP Blocking

- **DenyHosts** is an open source log-based intrusion prevention security script for SSH servers.
- The script works by banning IP addresses after set number of failed login attempts and also prevent such attacks from gaining access to server.

DenyHosts Features

Keeps track of /var/log/secure to find all successful and failed login attempts and filters them.

Optionally sends an email notifications of newly blocked hosts and suspicious logins.



If suspicious login attempts then bans that host IP address by adding an entry in /etc/hosts.deny file.

Maintains all valid and invalid failed user login attempts in separate files so we can delete that account or change password or disable shell for that user.

Keygen - Public Private Key

- Using Password-less login with SSH keys will increase the trust between two Linux servers for easy file synchronization or transfer.
- Steps to create password-less authentication :

Step-1

Login into server and generate a pair of public keys. “ssh-keygen –t rsa”

Step-2

Login to other system and create .ssh directory under it.

Step-3

Copy the generated public key (<filename>.pub) to .ssh directory and rename to ‘authorized_keys’.

Step-4

Set 700 permission on .ssh directory and authkORIZED_key.

Login to server.

Install Antivirus

Antivirus In Linux

- 01 There are very few Linux malware existing in world.
- 02 SAMBA and NFS server need to be scanned periodically to check for infection.
- 03 Malware may creep in while reading mails or downloaded internet data.
- 04 Antivirus is recommended if a file server or mail server is running on system.
- 05 One can stay safe on Linux by keeping software updated and not executing unrecognised and untrusted data.

ClamAV

Built-in support for all standard mail file formats.

Built-in support for various archive formats,

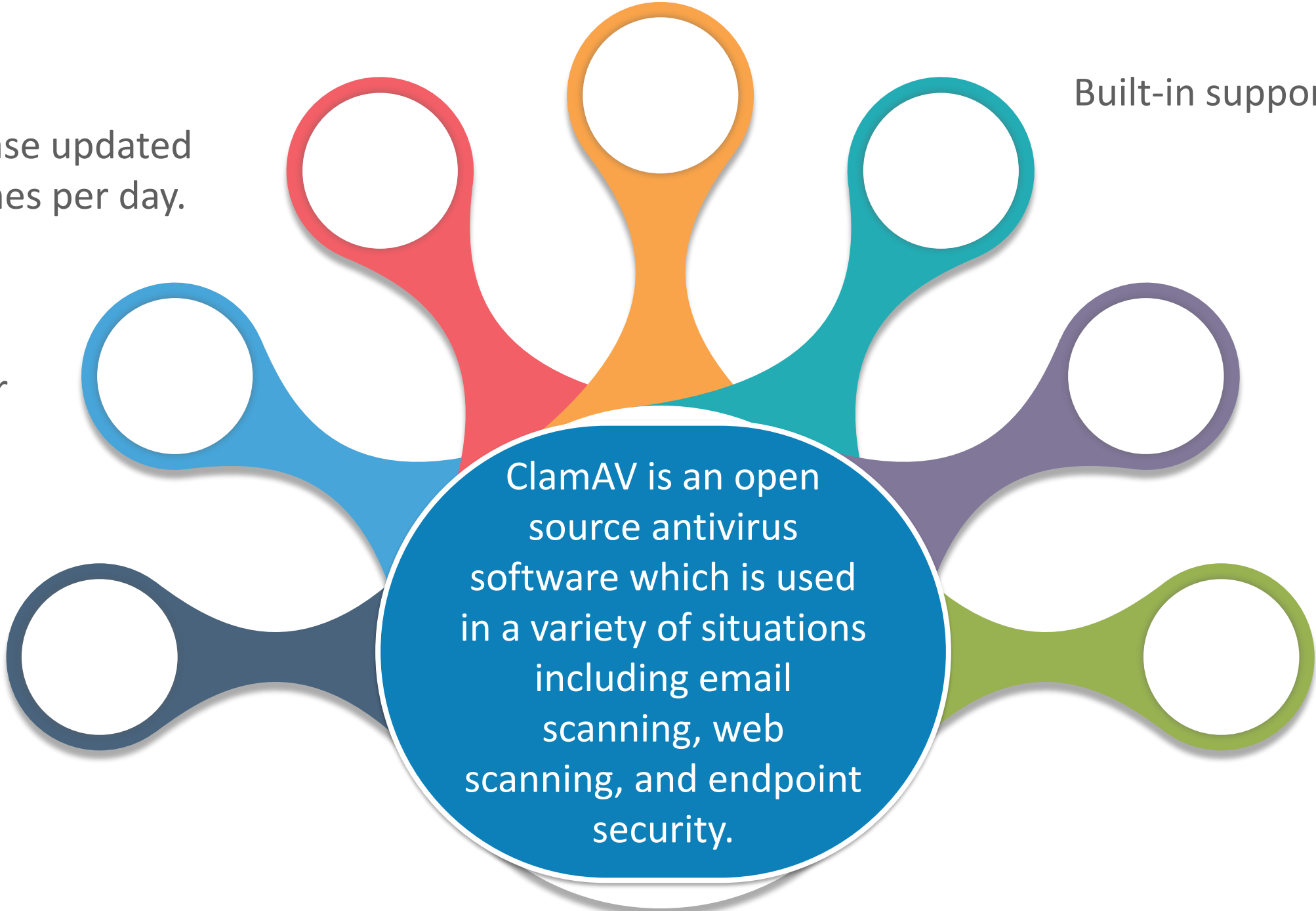
Virus database updated
multiple times per day.

Advanced database updater

Built-in support for ELF
executables and Portable
Executable files

Command-line scanner

Built-in support for popular
document formats



ClamAV is an open
source antivirus
software which is used
in a variety of situations
including email
scanning, web
scanning, and endpoint
security.

ClamAV Installation

```
//ClamAV installation is very simple can be found for  
Ubuntu in the apt repository.  
# sudo apt-get install clamav  
  
//To get a frontend install clamtk.  
# sudo apt-get install clamtk
```

- ClamTK provides a very simple GUI that helps beginners who are not comfortable to use CLI.
- The four sections in clamtk are :
 - Configuration section which enables user to configure clamAV.
 - History section which provides users with details about previous scans.
 - Updates section where new virus definitions may be imported to ClamAV.
 - Analysis section where you start your ClamAV scans.

ClamAV Configuration

```
//Update the virus definition after the installation of the tool.  
# service ClamAV-freshclam start  
  
//Edit the 'nano /etc/clamav/freshclam.conf' to specify the number  
//of times in a day it checks for new virus.  
# vi nano /etc/clamav/freshclam.conf  
    checks 1                //checks once a day.
```

LMD

- Linux Malware Detect known as 'maldet', helps to identify compromised accounts and take action quickly.
- Download maldetect package using wget.

wget <http://www.rfxn.com/downloads/maldetect-current.tar.gz>

```
//Extract the file.  
# tar -xzf maldetect-current.tar.gz  
  
//Go to the maldet folder.  
# cd maldetect-*  
  
//Install the maldet.  
# sh ./install.sh
```

LMD Configuration

Modify the `‘/usr/local/maldetect/conf.maldet’` file to configure the options based on your requirement

Email-alert	: If you would like to receive email alerts, then it should be set to 1.
email_subj	: Set your email subject here.
email_addr	: Add your email address to receive malware alerts.
quar_hits	: The default quarantine action for malware hits, it should be set 1.
quar_clean	: Cleaning detected malware injections, must set to 1.
quar_susp	: The default suspend action for users with hits, set it as per your requirements.
quar_susp_minuid	: Minimum userid that can be suspended.

LMD Commands

Some of the common used commands are :

Maldet -u	: update the maldet.
Maldet -a <path>	: scan files for a particular user.
maldet --scan-all <path>	: scan all user under given path.
maldet --clean SCANID	: clean malware results from a previous scan.
maldet --scan-recent <path> <days>	: scan files updated in last days mentioned.



KVM

What Is Virtualization?

01

It allows you to use a physical machine's full capacity by distributing its capabilities among many users or environments.

02

Software called hypervisors separate the physical resources from the virtual environments—the things that need those resources.

03

Resources are partitioned as needed from the physical environment to the many virtual environments.

04

The virtual machine functions as a single data file.

05

Servers started being used more efficiently thereby reducing the costs associated with purchase, set up, cooling, and maintenance.

Types Of Virtualization

Desktop Virtualization

Desktop virtualization allows administrator to deploy simulated desktop environments to multiple physical machines at once.

Server Virtualization

Virtualizing a server lets it to do more of specific functions and involves partitioning it so the components are used to serve multiple functions.

Data Virtualization

Virtualized access to multiple data sources, making it possible to deliver information promptly and in the appropriate contexts.

OS Virtualization

In Operating system virtualization, the kernel allows the existence of multiple isolated user-space instances.

Network Virtualization

Network functions virtualization separates a network's key functions (like file sharing, IP configuration) so they can be distributed.

Types

What Is KVM?

01

Kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux.

02

If you've got Linux 2.6.20 or newer, you've got KVM.

03

KVM converts Linux into a type-1 (bare-metal) hypervisor.

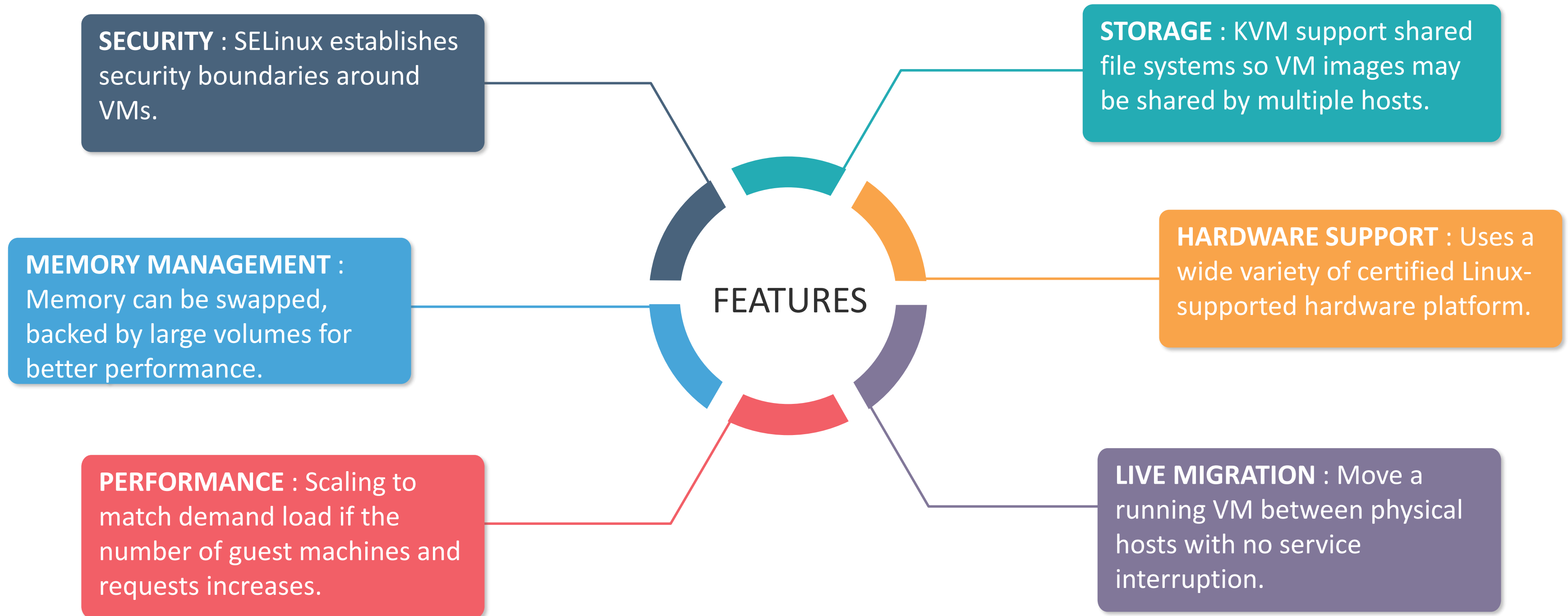
04

Every VM is implemented as a regular Linux process, scheduled by the standard Linux scheduler.

05

All hypervisors need some operating system-level components—such as a memory manager, process scheduler, input/output (I/O) stack, device drivers, security manager, a network stack, and more—to run VMs.

KVM Features



Install KVM

Steps to install and configure KVM :

```
//Install KVM in system.  
# sudo apt-get install qemu-kvm libvirt-bin virtinst bridge-utils  
cpu-checker  
  
//Verify KVM installation  
# kvm-ok           //check if KVM acceleration can be used.  
  
//Configure bridged networking  
# sudo vi /etc/network/interfaces  
  
//Modify the file to support KVM and save and close.  
  
//Restart the networking service  
# sudo systemctl restart networking
```

Install KVM (continued)

- Sample configuration should look like this

```
auto br0
iface br0 inet static
    address 10.18.44.26
    netmask 255.255.255.192
    broadcast 10.18.44.63
    dns-nameservers 10.0.80.11 10.0.80.12
    post-up route add -net 161.26.0.0 netmask
255.255.0.0 gw 10.18.44.1
    bridge_ports eth0
    bridge_stp off
    bridge_fd 0
    bridge_maxwait 0
bridge_maxwait 0
```

Install KVM (continued)

- Create another OS VM, CentOS taken here.
- ```
sudo virt-install \
--virt-type=kvm \
--name centos7 \
--ram 2048 \
--vcpus=2 \
--os-variant=centos7.0 \
--virt-type=kvm \
--hvm \
--cdrom=/var/lib/libvirt/boot/CentOS-7-x86_64-DVD-1708.iso \
--network=bridge=br0,model=virtio \
--network=bridge=br1,model=virtio \
--graphics vnc \
--disk path=/var/lib/libvirt/images/centos7.qcow2,size=40,bus=virtio,format=qcow2
```
- ```
# sudo virsh vncdisplay centos7 //to do configuration
```


Install KVM (continued)

- You need to use an SSH client to setup tunnel and a VNC client to access the remote vnc server.
- `# ssh vivek@server1.cyberciti.biz -L 5901:127.0.0.1:5901`
- Once you have ssh tunnel established, you can point your VNC client at your own 127.0.0.1 (localhost) address and port 5901.
- Start and complete the installation process.
- `# reboot`

Virtual Box

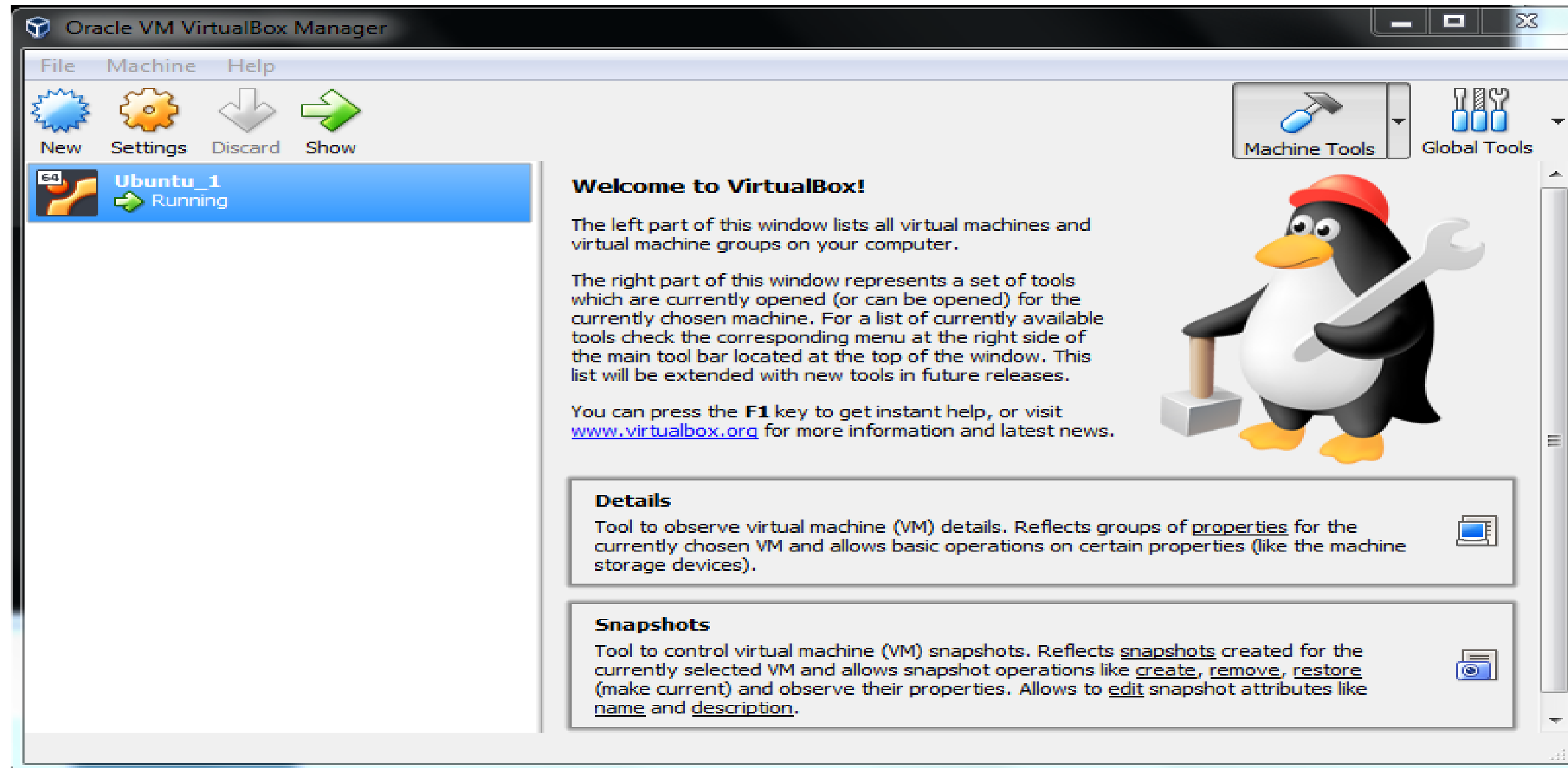
- It is the most popular virtualization tool in Windows.
- It's open-source and completely free.
- Steps to use Virtual Box :

Step-1 : Open the tool and click on new button

Step-2 : Go through the various interactive menu and select the choices you want for the VM.

Step-3 : Once done click on start button.

Demo - Virtual Box



Advantages Of Virtualization

Some of the basic advantage of virtualization are :

- Software inside a VM can't escape the VM to tamper with the rest of your system.
- The VM prevents the scammers from accessing our computer's real operating system and files.
- Helpful to test new OS without replacing your original one.
- Can also run multiple VMs at the same time, but you'll find yourself somewhat limited by your system resources.
- You won't have to mess around with partitioning or doing anything else complicated with your real hard drive as OS is stored in a virtual drive which is a big file on you real hard-drive.

Quiz



1. Which of the following stages included GRUB boot loader?
 - a. Stage 1 boot loader
 - b. Stage 2 boot loader
 - c. Kernel
 - d. Init

Answers

1. Which of the following stages included GRUB boot loader?
 - a. Stage 1 boot loader
 - b. Stage 2 boot loader
 - c. Kernel
 - d. Init

Answer B: The primary boot loader job is to find the Stage 2 boot loader which is GRUB in linux.

Summary

- In this module you should have learnt:
 - Security administration
 - Secure boot options
 - Secure ssh
 - Antivirus in Linux
 - Virtualization



Questions



Thank You



For more information please visit our website
www.edureka.co