



**inuits**

OPEN SOURCE INNOVATORS

Pavel Grochal

[darkless@inuits.eu](mailto:darkless@inuits.eu)

# Configuration Management Automation

2021-05-19

For lecture:  
PV077: UNIX – programování a správa systémů II

# Introduction

name: **Pavel Grochal**

nickname: **darkless**

email: **darkless@inuits.eu ; pavel.grochal@inuits.eu**

keyboard layouts: **English(US), Czech (QWERTY)**

favourite color: **blue**

favourite language: **Python**

favourite shell: **fish**

home igloo: **Brno**

# Tech history

2004: **HTML, CSS, PHP, SQL, JS** - Websites (Firefox 1.0, IE 6, Opera 7)

2006: **dualboot Linux** - Ubuntu 6.10 (Edgy Eft)

2008: Bc. study **FI MUNI, JAVA** ecosystem, **MVC PHP** (CodeIgniter - thesis)

2011: Mgr. study **FI MUNI**, teaching - **PB162 Programování Java**

2012: **PYTHON, DJANGO**, IT Specialist @ **Academy of Sciences**

2013: **Networking & Firewalls** (CCNA certs)

2014: **Virtualization** (KVM, XEN, OpenShift, PXE), **CFGMGMT** (ANSIBLE, Chef)

2015+ OpenSource Consultant @ **INUITS.eu**

# Overview

- (1) **Real-life story** – don't try this at home!
- (2) Where does [**CFG MGMT**] fits in?
- (3) **Concepts** of Configuration Management
- (4) Building real-life example in **Ansible**



Real-life story – don't try this at home!

# Real-life story introduction

**Task:** Install Samba(SMB) server on Ubuntu  
(used as network storage for employees)

## **Actions:**

- Prepare (Physical) Server, add DNS records, (setup other external services...)
- boot Linux, install Linux - Ubuntu (**USB / PXE**)
- Setup RAID storage (**mdadm**)
- Setup Monitoring (**Icinga**)
- Setup Backups (**Tape DRIVE + Bacula**)
- Setup FW (**iptables**)
- Setup SMB server ← **Focus part!**

# How to setup SMB server?

1) **Google** “how to install SMB server”

(<https://www.google.com/search?q=how+to+install+SMB+server>)

2) Click on **first link**

(<https://adrianmejia.com/how-to-set-up-samba-in-ubuntu-linux-and-access-it-in-mac-os-and-windows/>)

3) **Copy&paste** commands to **terminal**

4) **Profit !!!**



## Setting up the Samba File Server on Ubuntu/Linux:

FROM:

<https://adrianmeiia.com/how-to-set-up-samba-in-ubuntu-linux-and-access-it-in-mac-os-and-windows/>

1. Open the terminal
2. Install samba with the following command: `sudo apt-get install samba smbfs`
3. Configure samba typing: `vi /etc/samba/smb.conf`
4. Set your workgroup (if necessary). Go down in the file, until you see :

```
# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = WORKGROUP
```

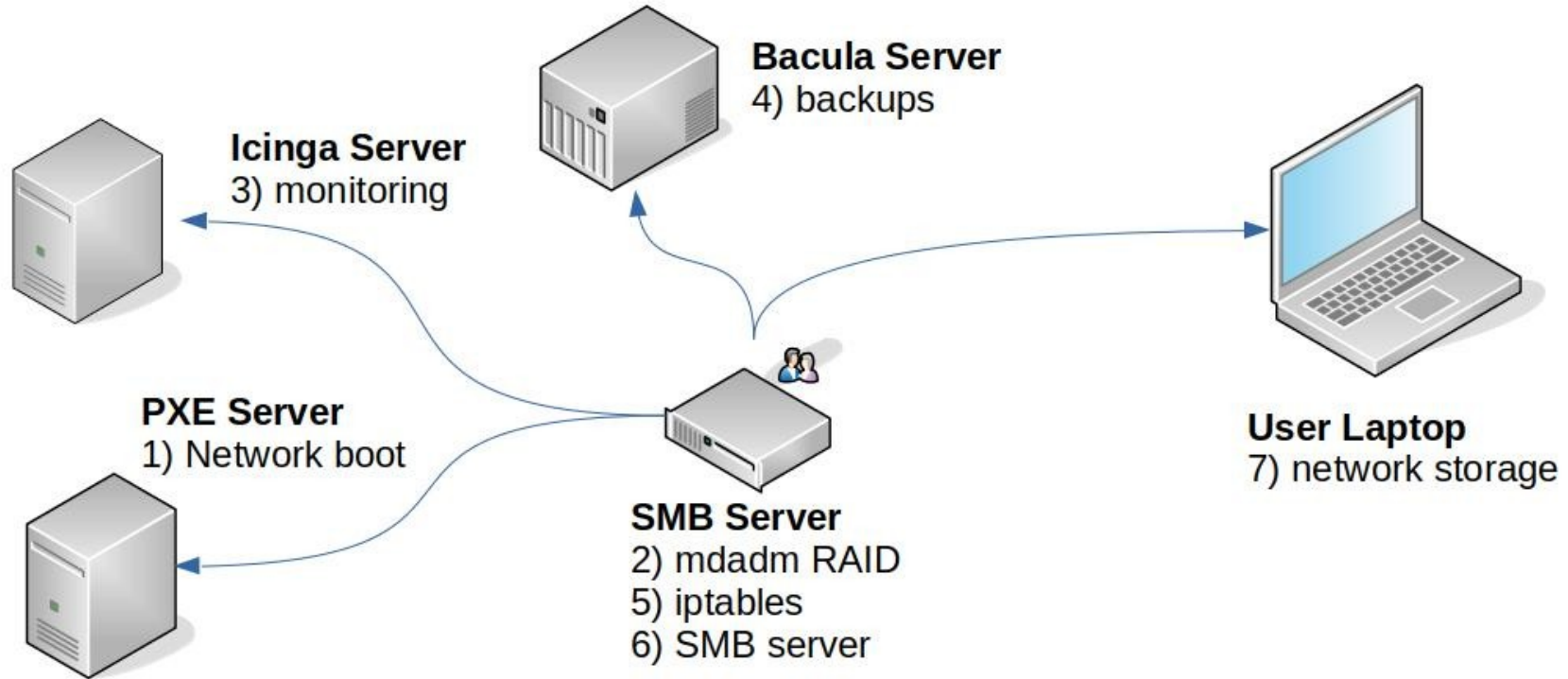
5. Set your share folders. Do something like this (change your path and comments)

```
# Adrian's share
[MyShare]
comment = YOUR COMMENTS
path = /your-share-folder
read only = no
guest ok = yes
```

6. Restart samba. type: `/etc/init.d/smbd restart`
7. Create the share folder: `sudo mkdir /your-share-folder`
8. Set the permissions: `sudo chmod 0777 /your-share-folder`
9. you are all set in ubuntu



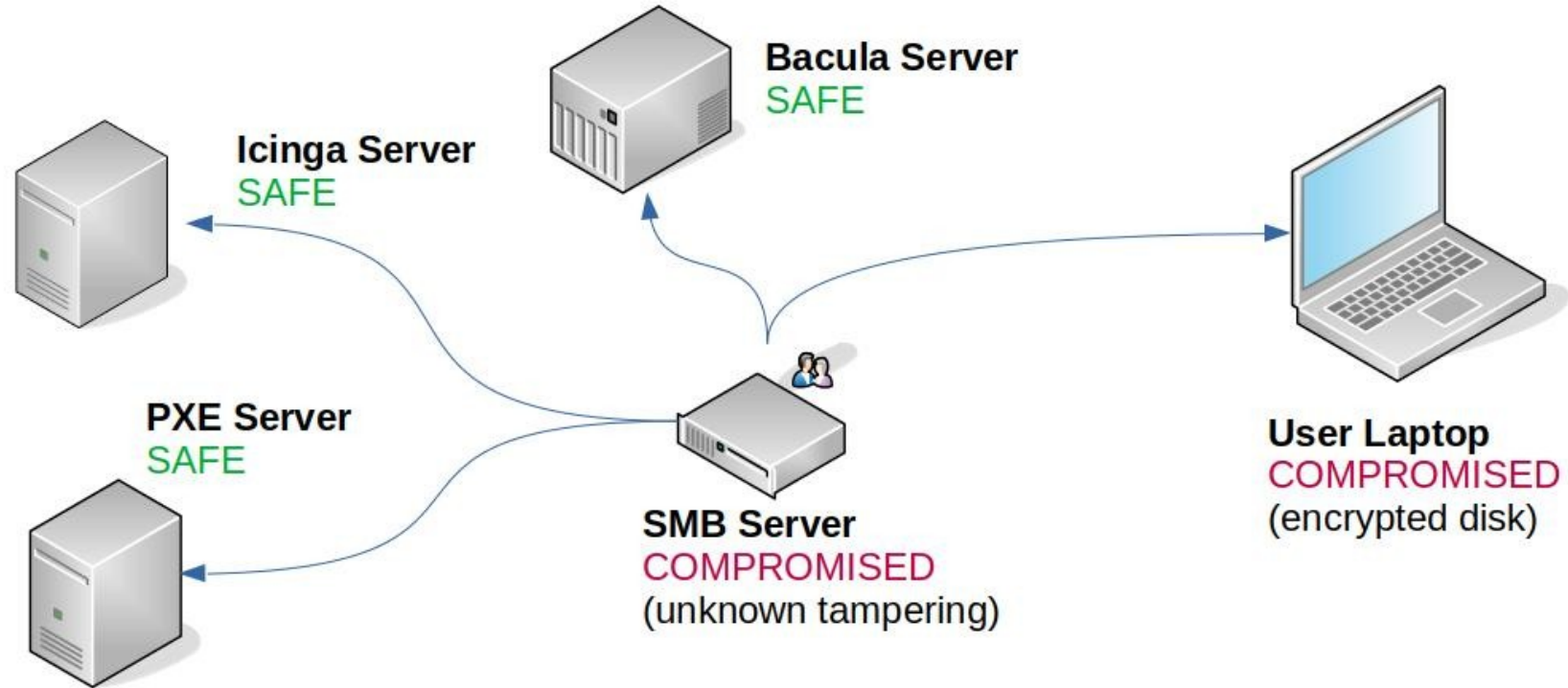
# Production Overview



# Ransomware Attack!

- One of the employees computer was **compromised** (Windows 7 Laptop)
- Shared network disk was **encrypted** demanding ransom
- Gained **access to server** due to security issue in SMB service

# Attack Overview



# First DAY mitigation

- Remove server from Network
- Inspect server via HW console in Data center
- Backup whole OS disk (dd) - for the future analysis
  - (User's data are backed on TAPE DRIVE and restorable)
- Stop server

# Difficulties

- Server was running for **1 year** periodically maintained.
- Nobody knew what was **ACTUALLY** installed on server. Only what SHOULD be installed.
- Custom-tweaked configurations for different users.

# Rinse & Repeat?

- Reinstall compromised Linux server – Ubuntu (**USB / PXE**)
- Setup RAID storage (**mdadm**)
- Setup Monitoring (**Icinga**)
- Setup Backups (**Tape DRIVE + Bacula**)
- Setup FW (**iptables**)
- Setup SMB server (**again!**)

There has to be another way!

# Configuration Management





Where does [CFG MGMT] fits in?

**BRACE YOURSELVES**



**DEFINITIONS ARE COMING**

# What is Automation?

Google: “What is Automation?”

“Automation is the use of technology to perform tasks with reduced human assistance.”

\* <https://www.redhat.com/en/topics/automation>

# IT Automation maybe?

“**IT automation**, sometimes referred to as **infrastructure automation**, is the use of software to create **repeatable instructions and processes** to replace or reduce human interaction with IT systems. Automation software works within the confines of those instructions, tools, and frameworks to carry out the tasks with little to no human intervention.”

\* <https://www.redhat.com/en/topics/automation/whats-it-automation>

# IT Automation topics

- Provisioning
- Configuration Management
- (Container) Orchestration
- IT migration
- Application deployment (CI/CD)
- Infrastructure as Code (IaC)

# Provisioning

“Provisioning is the process of **setting up IT infrastructure**. It can also refer to the steps required to manage access to data and resources, and make them available to users and systems.

**Provisioning is not the same thing as configuration**, but they are both steps in the deployment process. Once something has been provisioned, the next step is configuration.

When the term "provisioning" is used, it can mean many **different types of provisioning**, such as **server** provisioning, **network** provisioning, **user** provisioning, **service** provisioning, and more.”

\* <https://www.redhat.com/en/topics/automation/what-is-provisioning>

# Configuration Management

“Configuration management is a process for **maintaining computer systems**, servers, and software in a **desired, consistent state**. It’s a way to make sure that a system performs as it’s expected to as changes are made over time. ”

\* <https://www.redhat.com/en/topics/automation/what-is-configuration-management>



# Orchestration

“Orchestration is the automated configuration, management, and coordination of computer systems, applications, and services. Orchestration helps IT to more easily manage complex tasks and workflows.

**Automation and orchestration are different**, but related concepts.

In general, **automation refers to automating a single task**. This is different from **orchestration**, which is how you can **automate a process or workflow** that **involves many steps** across **multiple** disparate **systems**.”

\* <https://www.redhat.com/en/topics/automation/what-is-orchestration>

# Container Orchestration

“Container orchestration **automates** the **deployment, management, scaling,** and **networking** of **containers**. Enterprises that need to deploy and manage hundreds or thousands of Linux® containers and hosts can benefit from container orchestration.”

\* <https://www.redhat.com/en/topics/containers/what-is-container-orchestration>

# IT Migration

“An IT migration is the **shifting of data or software from one system to another**. Depending on the project, an IT migration could involve one or more kinds of movement: **Data** migration, **application** migration, **operating system** migration, and **cloud** migration.”

\* <https://www.redhat.com/en/topics/automation/what-is-it-migration>

# Application deployment (CI/CD)

“Continuous integration (CI) is the practice of **merging** all developers' **working copies** to a **shared mainline** several times a day.”

“Continuous delivery (CD) is a software engineering approach in which teams **produce software in short cycles**, ensuring that the **software can be reliably released at any time** and, when releasing the software, without doing so manually.”

“Continuous deployment (CD) is a software engineering approach in which **software functionalities** are **delivered frequently through automated deployments.**”

\* [https://en.wikipedia.org/wiki/Continuous\\_integration](https://en.wikipedia.org/wiki/Continuous_integration)

\* [https://en.wikipedia.org/wiki/Continuous\\_delivery](https://en.wikipedia.org/wiki/Continuous_delivery)

\* [https://en.wikipedia.org/wiki/Continuous\\_deployment](https://en.wikipedia.org/wiki/Continuous_deployment)

# Commonly Used Open Source Services for Ops

- **Provisioning:** Packer, Terraform
- **Configuration Management:** Puppet, Ansible, Chef, SaltStack
- **Container Orchestration:** Kubernetes, Nomad
- **Continous Integration/Delivery:** Jenkins, GitLab CI
- **Web servers:** Apache, Nginx, Caddy
- **Load Balancers** (including TLS termination): Nginx, HAProxy
- **Java application deployment:** JBoss, Wildfly, Tomcat
- **Databases:** MySQL, Postgres, CouchDB, MongoDB
- **Backup:** rsync, Bacula
- **Central log aggregation:** ELK, Fluentd, Graylog, Loki
- **Metrics and monitoring:** Zabbix, Icinga, Prometheus + Grafana
- **DNS server:** Bind, PowerDNS
- **Virtualization:** qemu/kvm, VirtManager, OpenNebula, Proxmox

# Infrastructure as Code (IaC)

“Infrastructure as Code (IaC) is the **managing** and **provisioning** of **infrastructure** through **code** instead of through manual processes.

With IaC, configuration files are created that contain your infrastructure specifications, which makes it easier to edit and distribute configurations. It also **ensures that you provision (and configure) the same environment every time.**”

\* <https://www.redhat.com/en/topics/automation/what-is-infrastructure-as-code-iac>

\* [https://en.wikipedia.org/wiki/Infrastructure\\_as\\_code](https://en.wikipedia.org/wiki/Infrastructure_as_code)

# General IaC Requirements

## 3 types of tools needed

### **Provisioning:**

- Create me an instance of asset X
  - Container instance
  - VM instance
  - Service X configuration via API

### **Configuration Management (Desired state, Continuous Configuration Automation, ...):**

- Ensure that this file present / service is always running
- Set X with these permissions
- Ensure User Removed

### **Orchestration:**

- Non frequent
- Trigger action X on resource Y based on characteristics A,B and or C
- First do X here then do Y there
- One off actions



# Brief intro into Provisioning Tools

**Packer:** Automates the creation of any type of machine image.

**Terraform:** Codifies cloud APIs into declarative configuration files, i.e.: Infrastructure as Code.

**Pulumi:** similar to Terraform, in that you create, deploy, and manage Infrastructure as Code on any cloud.

# Packer

Creates machine images from code:

- 1) **launch** virtual machine
- 2) **install** operating system
- 3) perform base **configuration** (Debian / Ubuntu: preseed or user-data, CentOS / RHEL: kickstart)
  - partitioning
  - base packages
  - users
  - networking
- 4) derives **machine image** from created virtual machine.

The resulting machine image can be used to launch new virtual machines from.

# Terraform

- Describes infrastructure as code and manages described infrastructure
  - **init** Terraform and providers used (e.g. Qemu, AWS, ...)
  - **validate** if the configuration is correct
  - **plan** the required changes to achieve the described infrastructure state.
  - **apply** the required changes.
  - **destroy** previously declared infrastructure.
- Functionality is not limited to virtual machines.
- Hashicorp Configuration Language (HCL).
- State Management stored in files

# Pulumi

- Similar to Terraform
- Supports and uses general purpose languages (Python, JavaScript, Go, C#, ...)
- Excellent code testing
- Mid-sized community
- State Management stored online

\* <https://www.pulumi.com/docs/intro/vs/terraform/#pulumi-vs-terraform>

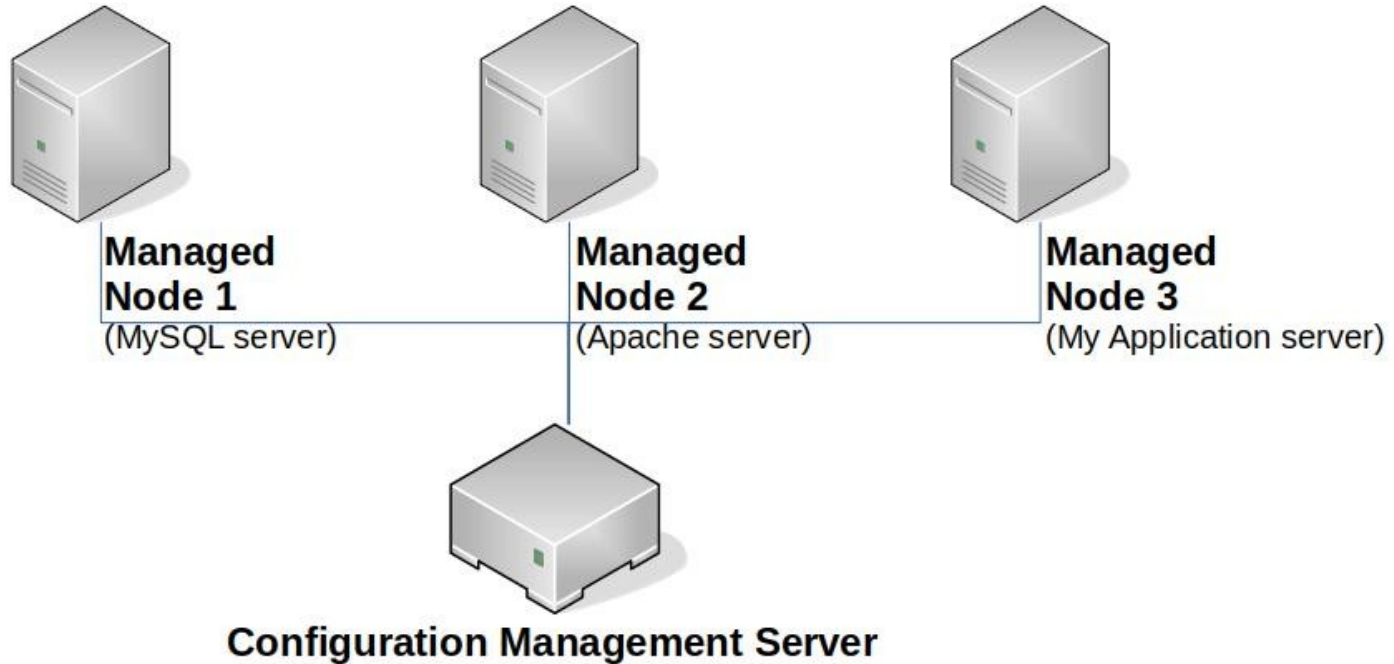


# Concepts of Configuration Management

# Concepts of CFG MGMT

- Server-client / push-pull models
- Imperative / Declarative models
- Desired State
- Idempotence
- Comparison of Configuration Management tools
  - Puppet
  - Ansible
  - Chef
  - SaltStack

# Topology Visualization





# Push vs Pull model

## Push model

Configuration Management Server **pushes** the configurations on the nodes.

- 1) **Server obtain** the **current state** of the node
- 2) **Compare** the **state** of the node with the stored **configuration**
- 3) **Perform actions** on the node to match the configuration

## Pull model

Nodes (regularly) **pull** changes from the Configuration Management Server.

- 1) **Node obtain** the **stored configuration** from server - requires **dedicated client**
- 2) **Compare** the **configuration** with the current **state** of the node
- 3) **Perform actions** on the node to match the configuration

# Imperative vs Declarative

## Imperative model

- Concept similar to Imperative Programming languages (Python, Java, PHP, ...)
- States **HOW** things should be done.
- Mostly includes Implementation details.
- **Example:** Recipe for baking a cake.

## Declarative model

- Concept similar to Declarative Programming languages (Haskell, Prolog, Lisp, ...)
- States **WHAT** the end result should be.
- Should exclude Implementation details.
- **Example:** Photo of how the cake should look like.

# Desired State

- Corresponds with Declarative model.
- Setup Managed Nodes into an expected state.
- Enforces consistency, reproducibility and automation.

\* [https://puppet.com/docs/puppet/7.6/puppet\\_overview.html#why\\_use\\_puppet](https://puppet.com/docs/puppet/7.6/puppet_overview.html#why_use_puppet)

# Idempotence

“Idempotence (UK: /,ɪdɛm'pɒʊtəns/, US: /,aɪdəm-/)  
is the property of certain operations in mathematics  
and computer science whereby they can be applied  
multiple times without changing the result beyond the  
initial application.”

\* <https://en.wikipedia.org/wiki/Idempotence>

# Idempotence Example - wrong

Create folder `/var/backups/`

```
darkless@khajit:~$ mkdir /var/backups/ ; echo $?
```

```
0
```

```
darkless@khajit:~$ mkdir /var/backups/ ; echo $?
```

```
mkdir: cannot create directory '/var/backups/': File exists
```

```
1
```

# Idempotence Example - better

```
darkless@khajit:~$ rmdir /var/backups/
```

```
darkless@khajit:~$ [ -d /var/backups/ ] || mkdir /var/backups ; echo $?
```

```
0
```

```
darkless@khajit:~$ [ -d /var/backups/ ] || mkdir /var/backups ; echo $?
```

```
0
```

# Puppet vs Ansible vs Chef vs SaltStack



- DSL (Puppet DSL)
- Pull model
  - Client required



- YAML (Python)
- Push model
  - No client (SSH)
- Pull model
  - Client (Ansible Pull)



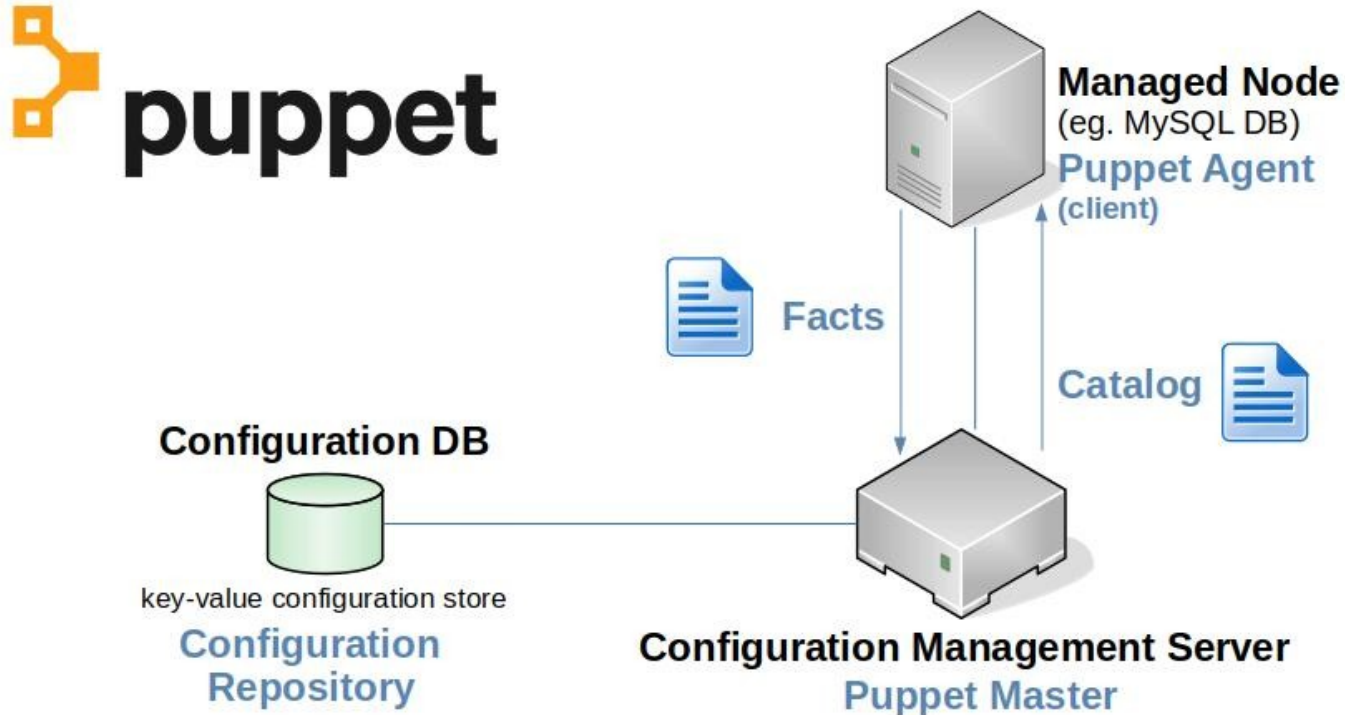
- DSL(Ruby)
- Pull model
  - Client required



- YAML(Python)
- Pull model
  - Client required
- Push model
  - No client (Salt SSH)

\* <https://medium.com/successivetech/chef-vs-puppet-vs-ansible-vs-saltstack-a-complete-comparison-9af8f1790c0d>

# Puppet Topology



\* This is **SIMPLIFIED** overview. See detailed information in respective guide.

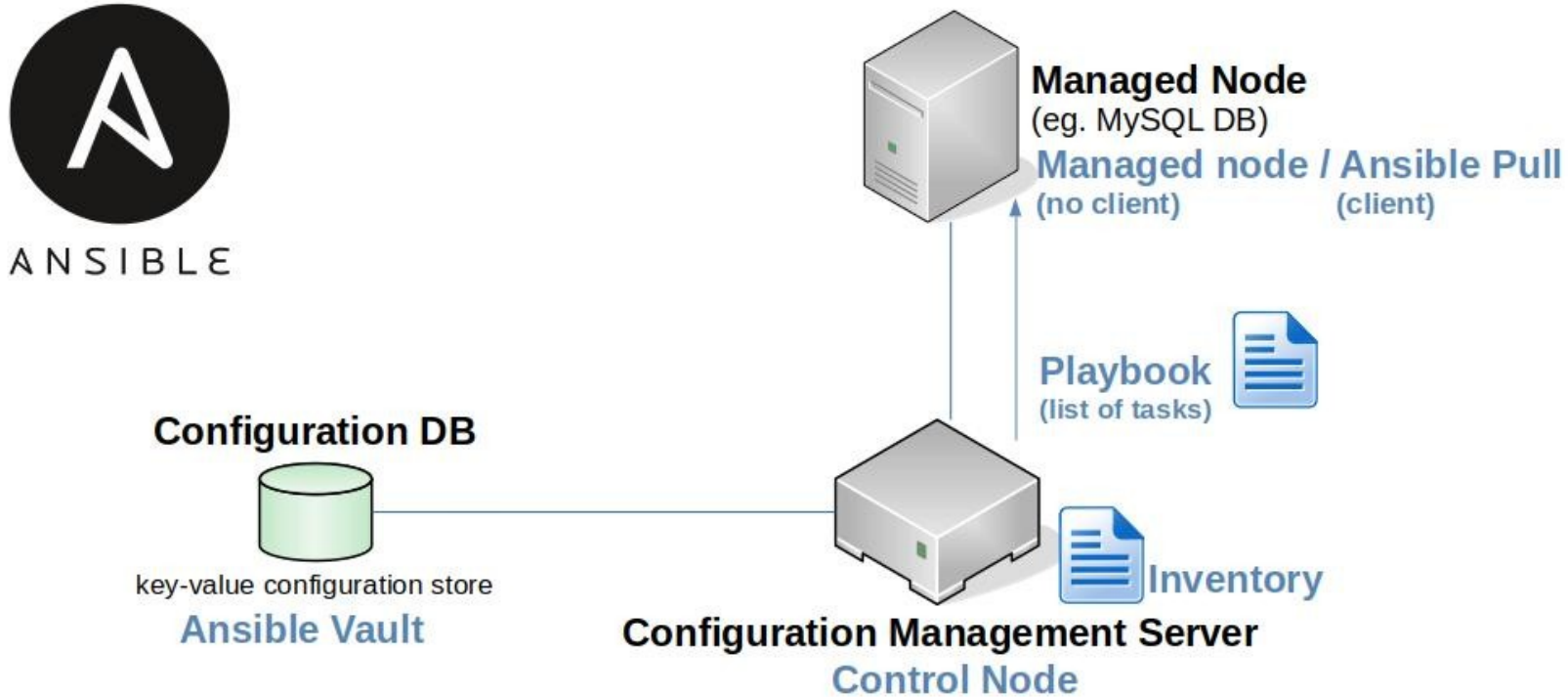


# Puppet – create folder

```
class directories {  
  file { '/var/backups':  
    ensure => 'directory',  
    owner  => 'darkless',  
    group  => 'games',  
    mode   => '0750',  
  }  
}
```

\* <https://www.puppetcookbook.com/posts/creating-a-directory.html>

# Ansible Topology



\* This is **SIMPLIFIED** overview. See detailed information in respective guide.

# Ansible – create folder

```
- name: Create a /var/backups/ directory
```

```
  ansible.builtin.file:
```

```
    path: /var/backups
```

```
    state: directory
```

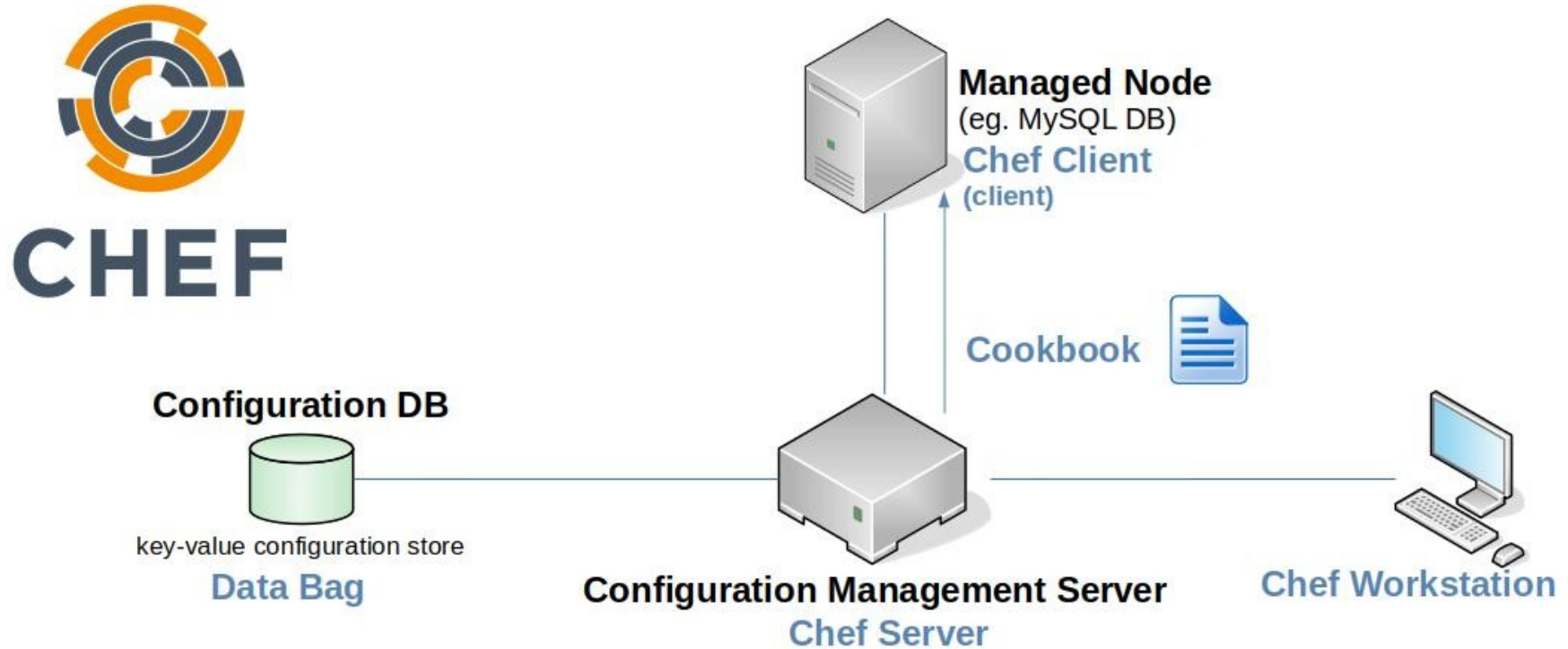
```
    owner: darkless
```

```
    group: games
```

```
    mode: '0755'
```

\* [https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file_module.html)

# Chef Topology



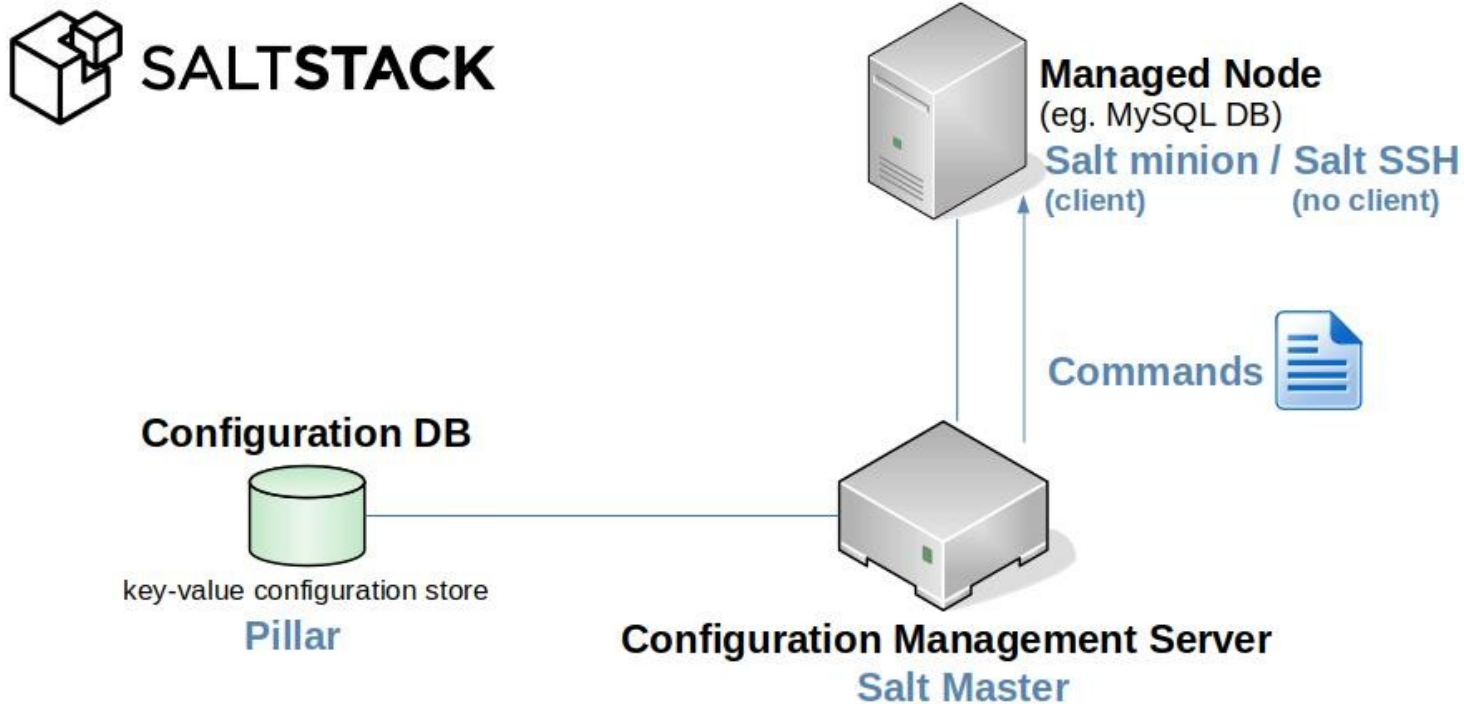
\* This is **SIMPLIFIED** overview. See detailed information in respective guide.

# Chef – create folder

```
directory '/var/backups' do
  owner 'darkless'
  group 'games'
  mode '0755'
  action :create
end
```

\* <https://docs.chef.io/resources/directory/>

# SaltStack Topology



\* This is **SIMPLIFIED** overview. See detailed information in respective guide.

# SaltStack – create folder

```
/var/backups:
```

```
file.directory:
```

- user: darkless**
- group: games**
- mode: 755**

\* <https://docs.saltproject.io/en/latest/ref/states/all/salt.states.file.html>



Building real-life example in Ansible

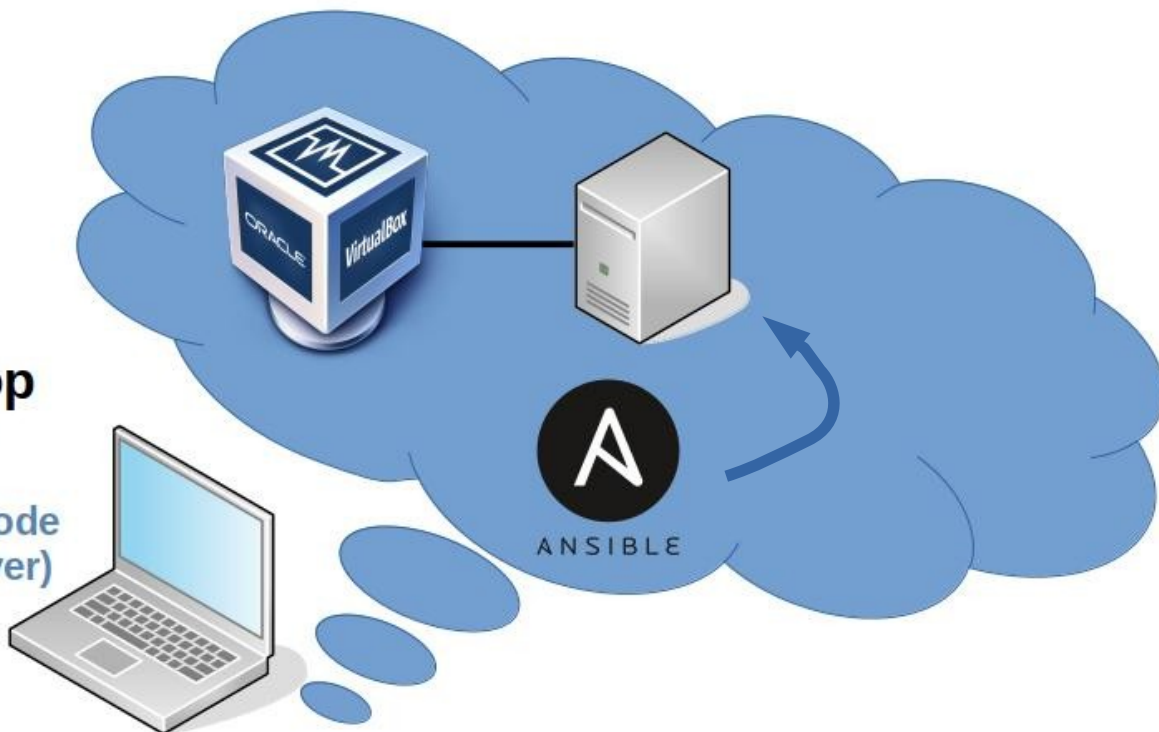


# Real-life example

- Targeted result overview
- Manual VM Provisioning
- Automatic configuration management

# Target result overview

- My Laptop**
- Control Node
  - Virtual Box
  - Managed Node (virtual server)



# Manual VM Provisioning

- Install VirtualBox
- Create new Virtual Machine
- Install Ubuntu Server on Virtual Machine
- Setup SSH Port Forwarding on VirtualBox
- Test SSH connection from localhost (Laptop)

# Install Virtualbox

<https://www.virtualbox.org/wiki/Downloads>

```
darkless@khajit:~$ apt show virtualbox
```

```
Package: virtualbox
```

```
Version: 6.1.16-dfsg-6~ubuntu1.20.04.1
```

# Download Ubuntu Server

<https://releases.ubuntu.com/20.04.2/ubuntu-20.04.2-live-server-amd64.iso>

# Create new Virtual Machine



Tools



Preferences



Import



Export



New



Add

## Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit [www.virtualbox.org](http://www.virtualbox.org) for more information and latest news.





### Create Virtual Machine ✕

## Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:   ▼

Type:  ▼ 

Version:  ▼



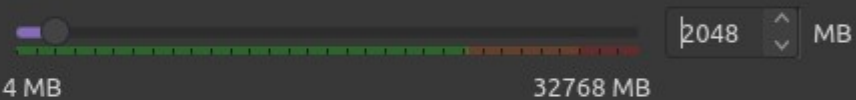
## Create Virtual Machine



### Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024 MB**.



< Back

Next >

Cancel

## Create Virtual Machine



### Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **10,00 GB**.

- Do not add a virtual hard disk
- Create a virtual hard disk now
- Use an existing virtual hard disk file

Empty



< Back

Create

Cancel

## Create Virtual Hard Disk



### Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

- VDI (VirtualBox Disk Image)
- VHD (Virtual Hard Disk)
- VMDK (Virtual Machine Disk)

Expert Mode

< Back

Next >

Cancel

## Create Virtual Hard Disk



### Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

- Dynamically allocated
- Fixed size

< Back

Next >

Cancel

## Create Virtual Hard Disk



### File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.



Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.



< Back

Create

Cancel



Tools



New



Settings



Discard



Start



myserver

Powered Off



## General

Name: myserver  
Operating System: Ubuntu (64-bit)



## System

Base Memory: 2048 MB  
Boot Order: Floppy, Optical, Hard Disk  
Acceleration: VT-x/AMD-V, Nested Paging, KVM  
Paravirtualization



## Display

Video Memory: 16 MB  
Graphics Controller: VMSVGA  
Remote Desktop Server: Disabled  
Recording: Disabled



## Storage

Controller: IDE  
IDE Secondary Master: [Optical Drive] Empty  
Controller: SATA  
SATA Port 0: myserver.vdi (Normal, 10,00 GB)



## Audio

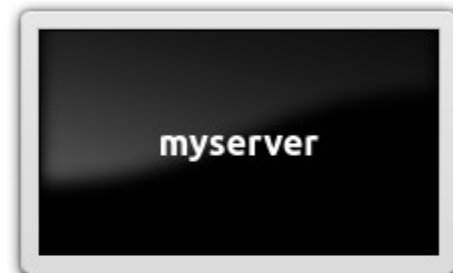
Host Driver: PulseAudio  
Controller: ICH AC97



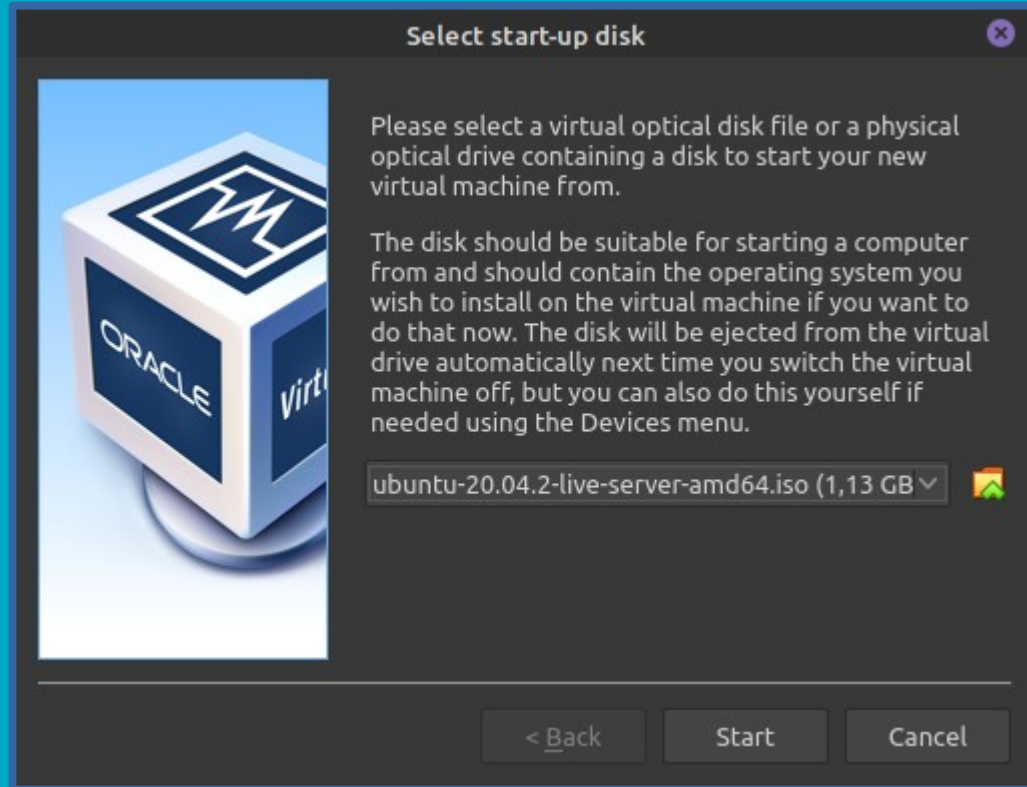
## Network



## Preview



# Install Ubuntu Server on Virtual Machine





Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!

[ Help ]

Use UP, DOWN and ENTER keys to select your language.

[ Asturianu	▶ ]
[ Bahasa Indonesia	▶ ]
[ Català	▶ ]
[ Deutsch	▶ ]
[ English	▶ ]
[ English (UK)	▶ ]
[ Español	▶ ]
[ Français	▶ ]
[ Hrvatski	▶ ]
[ Latviski	▶ ]
[ Lietuviškai	▶ ]
[ Magyar	▶ ]
[ Nederlands	▶ ]
[ Norsk bokmål	▶ ]
[ Polski	▶ ]
[ Suomi	▶ ]
[ Svenska	▶ ]
[ Čeština	▶ ]
[ Ελληνικά	▶ ]
[ Беларуская	▶ ]
[ Русский	▶ ]
[ Српски	▶ ]
[ Українська	▶ ]

## Keyboard configuration

[ Help ]

Please select your keyboard layout below, or select "Identify keyboard" to detect your layout automatically.

Layout: [ English (US) ▼ ]

Variant: [ English (US) ▼ ]

[ Identify keyboard ]

[ Done ]

[ Back ]

## Network connections

[ Help ]

Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient access for updates.

NAME	TYPE	NOTES
[ enp0s3	eth	▶ ]
DHCPv4	10.0.2.15/24	
08:00:27:c2:4c:25 / Intel Corporation / 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)		

[ Create bond ▶ ]

[ Done ]

[ Back ]

## Configure proxy

[ Help ]

If this system requires a proxy to connect to the internet, enter its details here.

Proxy address:

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user] [:pass}@]host[:port]/".

[ Done ]  
[ Back ]

Configure Ubuntu archive mirror

[ Help ]

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address:

You may provide an archive mirror that will be used instead of the default.

[ Done ]

[ Back ]

## Guided storage configuration

[ Help ]

Configure a guided storage layout, or create a custom one:

Use an entire disk

[ VBOX\_HARDDISK\_VBe6c15298-187ff282 local disk 10.000G ▼ ]

Set up this disk as an LVM group

Encrypt the LVM group with LUKS

Passphrase:

Confirm passphrase:

Custom storage layout

[ Done ]

[ Back ]

## Storage configuration

[ Help ]

## FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[ /	8.996G	new ext4	new LVM logical volume ▶ ]
[ /boot	1.000G	new ext4	new partition of local disk ▶ ]

## AVAILABLE DEVICES

No available devices

[ Create software RAID (md) ▶ ]  
[ Create volume group (LVM) ▶ ]

## USED DEVICES

DEVICE	TYPE	SIZE
[ ubuntu-vg (new)	LVM volume group	8.996G ▶ ]
ubuntu-lv	new, to be formatted as ext4, mounted at /	8.996G ▶ ]
[ VBOX_HARDDISK_VBe6c15298-187ff282	local disk	10.000G ▶ ]
partition 1	new, bios_grub	1.000M ▶ ]
partition 2	new, to be formatted as ext4, mounted at /boot	1.000G ▶ ]
partition 3	new, PV of LVM volume group ubuntu-vg	8.997G ▶ ]

[ Done ]  
[ Reset ]  
[ Back ]

## Storage configuration

[ Help ]

## FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[ /	8.996G	new ext4	new LVM logical volume ▶ ]
[ /boot	1.000G	new ext4	new partition of local disk ▶ ]

## AVAILABLE DEVICES

## Confirm destructive action

Selecting Continue below will begin the installation process and result in the loss of data on the disks selected to be formatted.

You will not be able to return to this or a previous screen once the installation has started.

Are you sure you want to continue?

[ No ]  
[ Continue ]

[ Done ]  
[ Reset ]  
[ Back ]



## Profile setup

[ Help ]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Your name: Your server's name: 

The name it uses when it talks to other computers.

Pick a username: Choose a password: Confirm your password: 

[ Done ]

SSH Setup

[ Help ]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

Install OpenSSH server

Import SSH identity: [ No ▼ ]

You can import your SSH keys from Github or Launchpad.

Import Username:

Allow password authentication over SSH

[ Done ]

[ Back ]

## Featured Server Snaps

[ Help ]

These are popular snaps in server environments. Select or deselect with SPACE, press ENTER to see more details of the package, publisher and versions available.

[ ]	microk8s	Lightweight Kubernetes for workstations and appliance	▶
[ ]	nextcloud	Nextcloud Server - A safe home for all your data	▶
[ ]	wekan	Open-Source kanban	▶
[ ]	kata-containers	Lightweight virtual machines that seamlessly plug into	▶
[ ]	docker	Docker container runtime	▶
[ ]	canonical-livepatch	Canonical Livepatch Client	▶
[ ]	rocketchat-server	Group chat server for 100s, installed in seconds.	▶
[ ]	mosquitto	Eclipse Mosquitto MQTT broker	▶
[ ]	etcd	Resilient key-value store by CoreOS	▶
[ ]	powershell	PowerShell for every system!	▶
[ ]	stress-ng	A tool to load, stress test and benchmark a computer	▶
[ ]	sabnzbd	SABnzbd	▶
[ ]	wormhole	get things from one computer to another, safely	▶
[ ]	aws-cli	Universal Command Line Interface for Amazon Web Services	▶
[ ]	google-cloud-sdk	Command-line interface for Google Cloud Platform products	▶
[ ]	slcli	Python based SoftLayer API Tool.	▶
[ ]	doctl	The official DigitalOcean command line interface	▶
[ ]	conjure-up	Package runtime for conjure-up spells	▶
[ ]	minidlna-escoand	server software with the aim of being fully compliant	▶
[ ]	postgresql10	PostgreSQL is a powerful, open source object-relational	▶
[ ]	heroku	CLI client for Heroku	▶
[ ]	keepalived	High availability VRRP/BFD and load-balancing for Linux	▶
[ ]	prometheus	The Prometheus monitoring system and time series data	▶
[ ]	juju	A model-driven operator lifecycle manager	▶

[ Done ]  
[ Back ]

Installing system

[ Help ]

```
curtin command block-meta
  removing previous storage devices
  configuring disk: disk-sda
configuring partition: partition-0
configuring partition: partition-1
configuring format: format-0
configuring partition: partition-2
configuring lvm_volgroup: lvm_volgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
writing install sources to disk
running 'curtin extract'
curtin command extract
  acquiring and extracting image from cp:///media/filesystem
configuring installed system
  running '/snap/bin/subiquity.subiquity-configure-run'
  running '/snap/bin/subiquity.subiquity-configure-apt
/snap/subiquity/2280/usr/bin/python3 true'
curtin command apt-config
curtin command in-target
running 'curtin curthooks'
curtin command curthooks
  configuring apt configuring apt
  installing missing packages
  configuring iscsi service
  configuring raid (mdadm) service
  installing kernel -
```

[ View full log ]

Install complete!

[ Help ]

```
running '/snap/bin/subiquity.subiquity-configure-apt
/snap/subiquity/2280/usr/bin/python3 true'
  curtin command apt-config
  curtin command in-target
running 'curtin curthooks'
  curtin command curthooks
    configuring apt configuring apt
    installing missing packages
    configuring iscsi service
    configuring raid (mdadm) service
    installing kernel
    setting up swap
    apply networking config
    writing etc/fstab
    configuring multipath
    updating packages on target system
    configuring pollinate user-agent on target
    updating initramfs configuration
    configuring target system bootloader
    installing grub to target devices
  finalizing installation
    running 'curtin hook' -
final system configuration
  configuring cloud-init
  installing openssh-server
  restoring apt configuration
downloading and installing security updates
subiquity/Late/run
```

[ View full log ]

[ Reboot Now ]

Ubuntu 20.04.2 LTS myserver tty1

Hint: Num Lock on

myserver login: darkless

Password:

Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86\_64)

\* Documentation: <https://help.ubuntu.com>  
\* Management: <https://landscape.canonical.com>  
\* Support: <https://ubuntu.com/advantage>

System information as of Mon 17 May 2021 06:20:32 PM UTC

System load:	0.53	Processes:	101
Usage of /:	43.2% of 8.79GB	Users logged in:	0
Memory usage:	9%	IPv4 address for enp0s3:	10.0.2.15
Swap usage:	0%		

62 updates can be installed immediately.  
0 of these updates are security updates.  
To see these additional updates run: `apt list --upgradable`

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in `/usr/share/doc/*/copyright`.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo\_root" for details.

darkless@myserver:~\$

File Machine View Input Devices Help

```
System load: 0.53          Processes:           101
Usage of /:  43.2% of 8.79GB Users logged in:     0
Memory usage: 9%          IPv4 address for enp0s3: 10.0.2.15
Swap usage:  0%
```

```
62 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
darkless@myserver:~$ ip addr
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e2:4c:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86340sec preferred_lft 86340sec
    inet6 fe80::a00:27ff:fee2:4c25/64 scope link
        valid_lft forever preferred_lft forever
darkless@myserver:~$
```

# Setup SSH Port Forwarding on VirtualBox





Tools



New



Settings



Discard



Start



myserver



Powered Off



General

Name: myserver  
Operating System: Ubuntu (64-bit)



System

Base Memory: 2048 MB  
Boot Order: Floppy, Optical, Hard Disk  
Acceleration: VT-x/AMD-V, Nested Paging, KVM  
Paravirtualization



Display

Video Memory: 16 MB  
Graphics Controller: VMSVGA  
Remote Desktop Server: Disabled  
Recording: Disabled



Storage

Controller: IDE  
IDE Secondary Master: [Optical Drive] Empty  
Controller: SATA  
SATA Port 0: myserver.vdi (Normal, 10,00 GB)



Audio

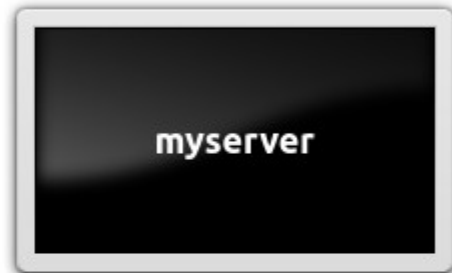
Host Driver: PulseAudio  
Controller: ICH AC97



Network



Preview





- General
- System
- Display
- Storage
- Audio
- Network**
- Serial Ports
- USB
- Shared Folders
- User Interface

## Network

Adapter 1   Adapter 2   Adapter 3   Adapter 4

Enable Network Adapter

Attached to: NAT

Name:

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027E24C25



Cable Connected

Port Forwarding

Cancel

OK

Port Forwarding Rules

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port	
Rule 1	TCP	127.0.0.1	2222	10.0.2.15	22	 

Cancel OK

# Test SSH connection from localhost (Laptop)

```
~  
) ssh -p 2222 localhost
```

The authenticity of host '[localhost]:2222 ([127.0.0.1]:2222)' can't be established.

ECDSA key fingerprint is SHA256:r+xMDk/rGkc7k9wE9lv1nT00hCyR6I7wSpEvviAGJ4s.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '[localhost]:2222' (ECDSA) to the list of known hosts

darkless@localhost's password:

Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86\_64)

- \* Documentation: <https://help.ubuntu.com>
- \* Management: <https://landscape.canonical.com>
- \* Support: <https://ubuntu.com/advantage>

System information as of Mon 17 May 2021 06:25:26 PM UTC

System load:	0.03	Processes:	111
Usage of /:	43.3% of 8.79GB	Users logged in:	1
Memory usage:	9%	IPv4 address for enp0s3:	10.0.2.15
Swap usage:	0%		

62 updates can be installed immediately.

0 of these updates are security updates.

To see these additional updates run: `apt list --upgradable`

Last login: Mon May 17 18:24:36 2021

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo\_root" for details.

```
darkless@myserver:~$
```

```
darkless@myserver:~$ ip addr
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
```

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
    inet 127.0.0.1/8 scope host lo
```

```
        valid_lft forever preferred_lft forever
```

```
    inet6 ::1/128 scope host
```

```
        valid_lft forever preferred_lft forever
```

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
```

```
    link/ether 08:00:27:e2:4c:25 brd ff:ff:ff:ff:ff:ff
```

```
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
```

```
        valid_lft 86314sec preferred_lft 86314sec
```

```
    inet6 fe80::a00:27ff:fee2:4c25/64 scope link
```

```
        valid_lft forever preferred_lft forever
```

```
darkless@myserver:~$ █
```

# Extras: VirtualBox bridged adapter

# Virtual Box Networking Modes

Table 6.1. Overview of Networking Modes

Mode	VM → Host	VM ← Host	VM1 ↔ VM2	VM → Net/LAN	VM ← Net/LAN
Host-only	+	+	+	-	-
Internal	-	-	+	-	-
Bridged	+	+	+	+	+
NAT	+	<a href="#">Port forward</a>	-	+	<a href="#">Port forward</a>
NATservice	+	<a href="#">Port forward</a>	+	+	<a href="#">Port forward</a>

\* <https://www.virtualbox.org/manual/ch06.html>





General

System

Display

Storage

Audio

Network

Serial Ports

USB

Shared Folders

User Interface

## Network

Adapter 1

Adapter 2

Adapter 3

Adapter 4

Enable Network Adapter

Attached to: Bridged Adapter

Name: wlp0s20f3

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027F911D0

Cable Connected

Port Forwarding

Cancel

OK

```
darkless@myserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e2:4c:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86326sec preferred_lft 86326sec
    inet6 fe80::a00:27ff:fee2:4c25/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:7e:55:cf brd ff:ff:ff:ff:ff:ff
darkless@myserver:~$
```

File Machine View Input Devices Help

```
darkless@myserver:~$ sudo ip link set dev enp0s8 up
[sudo] password for darkless:
darkless@myserver:~$ sudo dhclient enp0s8 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s8/08:00:27:8c:80:21
Sending on   LPF/enp0s8/08:00:27:8c:80:21
Sending on   Socket/fallback
DHCPDISCOVER on enp0s8 to 255.255.255.255 port 67 interval 3 (xid=0x42f4b318)
DHCPOFFER of 192.168.1.134 from 192.168.1.1
DHCPREQUEST for 192.168.1.134 on enp0s8 to 255.255.255.255 port 67 (xid=0x18b3f442)
DHCPACK of 192.168.1.134 from 192.168.1.1 (xid=0x42f4b318)
bound to 192.168.1.134 -- renewal in 286282 seconds.
darkless@myserver:~$ _
```

File Machine View Input Devices Help

```
darkless@myserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e2:4c:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85909sec preferred_lft 85909sec
    inet6 fe80::a00:27ff:fee2:4c25/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7e:55:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.134/24 brd 192.168.1.255 scope global dynamic enp0s8
        valid_lft 43164sec preferred_lft 43164sec
    inet6 fd0f:f930:e56c:0:a00:27ff:fe7e:55cf/64 scope global dynamic mngtmpaddr
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:55cf/64 scope link
        valid_lft forever preferred_lft forever
darkless@myserver:~$ _
```

```
fish /home/darkless
File Edit View Search Terminal Help

~
) ping 192.168.1.134 -c 4
PING 192.168.1.134 (192.168.1.134) 56(84) bytes of data.
64 bytes from 192.168.1.134: icmp_seq=1 ttl=64 time=0.802 ms
64 bytes from 192.168.1.134: icmp_seq=2 ttl=64 time=0.823 ms
64 bytes from 192.168.1.134: icmp_seq=3 ttl=64 time=0.815 ms
64 bytes from 192.168.1.134: icmp_seq=4 ttl=64 time=0.756 ms

--- 192.168.1.134 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.756/0.799/0.823/0.025 ms

~
) █
```

```
fish /home/darkless
File Edit View Search Terminal Help

~
) ping myserver -c 4
PING myserver.lan (192.168.1.134) 56(84) bytes of data.
64 bytes from myserver.lan (192.168.1.134): icmp_seq=1 ttl=64 time=0.623 ms
64 bytes from myserver.lan (192.168.1.134): icmp_seq=2 ttl=64 time=0.870 ms
64 bytes from myserver.lan (192.168.1.134): icmp_seq=3 ttl=64 time=0.863 ms
64 bytes from myserver.lan (192.168.1.134): icmp_seq=4 ttl=64 time=0.891 ms

--- myserver.lan ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.623/0.811/0.891/0.109 ms

~
) █
```

# Extras: Exporting Virtual Machine

File Machine Help

- Preferences... Ctrl+G
- Import Appliance... Ctrl+I
- Export Appliance... Ctrl+E
- New Cloud VM...
- Virtual Media Manager... Ctrl+D
- Host Network Manager... Ctrl+H
- Network Operations Manager...
- Reset All Warnings
- Exit Ctrl+Q



New Settings Discard Show

**General**

Name: myserver  
Operating System: Ubuntu (64-bit)

**System**

Base Memory: 2048 MB  
Boot Order: Floppy, Optical, Hard Disk  
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

**Display**

Video Memory: 16 MB  
Graphics Controller: VMSVGA  
Remote Desktop Server: Disabled  
Recording: Disabled

**Storage**

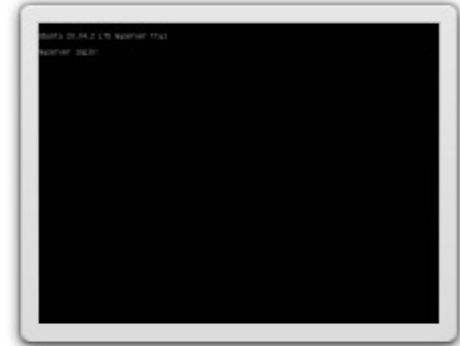
Controller: IDE  
IDE Secondary Master: [Optical Drive] Empty  
Controller: SATA  
SATA Port 0: myserver-disk001.vdi (Normal, 10,00 GB)

**Audio**

Host Driver: PulseAudio  
Controller: ICH AC97

**Network**

Adapter 1: Intel PRO/1000 MT Desktop (NAT)  
Adapter 2: Intel PRO/1000 MT Desktop (Bridged Adapter, vlnic2005)

**Preview**





## Virtual machines to export

Please select the virtual machines that should be added to the appliance. You can select more than one. Please note that these machines have to be turned off before they can be exported.



myserver

Expert Mode

< Back

Next >

Cancel



## Appliance settings

Please choose a format to export the virtual appliance to.

The **Open Virtualization Format** supports only **ovf** or **ova** extensions. If you use the **ovf** extension, several files will be written separately. If you use the **ova** extension, all the files will be combined into one Open Virtualization Format archive.

The **Oracle Cloud Infrastructure** format supports exporting to remote cloud servers only. Main virtual disk of each selected machine will be uploaded to remote server.

Format:

Please choose a filename to export the virtual appliance to. Besides that you can specify a certain amount of options which affects the size and content of resulting archive.

File:

MAC Address Policy:

Additionally:  Write Manifest file

Include ISO image files

< Back

Next >

Cancel



## Virtual system settings

This is the descriptive information which will be added to the virtual appliance. You can change it by double clicking on individual lines.

### Virtual System 1

- \* Name myserver
- Product
- Product-URL
- Vendor
- Vendor-URL
- Version
- Description
- License

[Restore Defaults](#)[< Back](#)[Export](#)[Cancel](#)

# Automatic configuration management

- Basic Ansible concepts
- Install Ansible
- Ansible Best Practices
- Setup simple Ansible Playbook

# Basic Ansible Concepts

- Control Node
- Managed Nodes
- Inventory
- Playbook
- Task
- Modules
- Collections
- Handlers
- Variables

# Control Node

[https://docs.ansible.com/ansible/latest/network/getting\\_started/basic\\_concepts.html#control-node](https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#control-node)

- Any machine with Ansible **installed**.
- You can use any computer that has a **Python** installation as a control node.
- You can have **multiple** control nodes.

# Managed Nodes

[https://docs.ansible.com/ansible/latest/network/getting\\_started/basic\\_concepts.html#managed-nodes](https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#managed-nodes)

- The network devices (and/or servers) you manage with Ansible.
- Managed nodes are also sometimes called “**hosts**”.
- Ansible is **not** installed on managed nodes.

# Inventory

[https://docs.ansible.com/ansible/latest/user\\_guide/intro\\_inventory.html#inventory-basics-formats-hosts-and-groups](https://docs.ansible.com/ansible/latest/user_guide/intro_inventory.html#inventory-basics-formats-hosts-and-groups)

- List of Managed Nodes and their groups  
(Ansible knows how to reach those Nodes)
- Sometimes called a “hostfile”
- Defaults to **/etc/ansible/hosts**
- Custom file can be used (eg. **hosts.yml**)
- Dynamic Inventories – for Cloud solutions



# Playbook

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_intro.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_intro.html)

- A **playbook** is composed of one or more '**plays**' in an **ordered list**.
- Each **play** executes part of the overall goal of the playbook, running one or more **tasks**.
- Each **task** calls an Ansible **module**.

# Task

[https://docs.ansible.com/ansible/latest/network/getting\\_started/basic\\_concepts.html#tasks](https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#tasks)

- The **units of action** in Ansible.
- You can execute a single task once with an ad-hoc command.
- Each **task** calls an Ansible **module**.

# Modules

[https://docs.ansible.com/ansible/latest/network/getting\\_started/basic\\_concepts.html#modules](https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#modules)

- The **units of code** Ansible executes.
- Example: **File Module**
  - [https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file_module.html)

# Ansible Task which uses File Module

```
- name: Create a /var/backups/ directory
```

```
  ansible.builtin.file:
```

```
    path: /var/backups
```

```
    state: directory
```

```
    owner: darkless
```

```
    group: games
```

```
    mode: '0755'
```

\* [https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file_module.html)

# Collections

[https://docs.ansible.com/ansible/latest/network/getting\\_started/basic\\_concepts.html#collections](https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#collections)

[https://docs.ansible.com/ansible/latest/galaxy/user\\_guide.html](https://docs.ansible.com/ansible/latest/galaxy/user_guide.html)

- Collections are a **distribution format** for Ansible content that can include playbooks, roles, modules, and plugins.
- You can install and use collections through **Ansible Galaxy**.

# Handlers

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_handlers.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_handlers.html)

- Handlers are tasks that only run when notified.
- Each handler should have a globally unique name.
- Example:
  - restart a service if a task updates the configuration of that service
  - do nothing if the configuration is unchanged

# Variables

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_variables.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_variables.html)

- Ansible uses variables to manage differences between systems.
- You can define these variables in:
  - Playbooks
  - Inventory
  - Re-usable (variable) files
  - Roles
  - Command line
- Define variable: **remote\_install\_path: /opt/my\_app\_config**
- Use variable: **dest: '{{ remote\_install\_path }}/foo.cfg'**

# Install Ansible

[https://docs.ansible.com/ansible/latest/installation\\_guide/intro\\_installation.html](https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html)

```
darkless@khajit:~$ apt show ansible  
  
Package: ansible  
  
Version: 2.9.6+dfsg-1
```

NOTE: Some functionality used in example requires `sshpass` package installed



# Ansible Best Practices

[https://docs.ansible.com/ansible/latest/user\\_guide/playbooks\\_best\\_practices.html](https://docs.ansible.com/ansible/latest/user_guide/playbooks_best_practices.html)

- General tips
- Playbook tips
- Inventory tips
- Execution tips

# Setup simple Ansible Playbook

- Clone Simple Ansible Skeleton (Playbook)
- Explore Skeleton Structure
- Enhance playbook:
  - Setup basic server hardening for all hosts
  - Install Docker via roles from Ansible-Galaxy
  - Deploy example Docker app on subset of hosts

# Simple Ansible Skeleton

Git clone:

[https://github.com/Darkless012/ansible\\_tutorial](https://github.com/Darkless012/ansible_tutorial)

Or fork :)

# Explore Skeleton Structure

tasks/

all/

hostname.yml

vars/

all/

external\_vars.yml.example → external\_vars.yml

.gitignore

handlers.yml

hosts.yml.example → hosts.yml

playbook.yml

# Setup basic server hardening for all hosts

## IDK GOOGLE?

- <https://www.google.com/search?q=ubuntu+server+20.04+hardening>

## HERE YA GO:

- <https://www.informaticar.net/security-hardening-ubuntu-20-04/>
- <https://implex.io/posts/ubuntu-20-04-setup/>
- <https://gist.github.com/lokhman/cc716d2e2d373dd696b2d9264c0287a3>

# Hardening steps (from internet)

## In this tutorial:

- System Updates
- Create Non-root User
- Disable Root User (SSH and system)
- Configure SSH settings
- Firewall setup
- Install Fail2Ban
- Sysctl.conf
- Secure Shared Memory
- Set Hostname and Host File
- Set Locale and Timezone

## Out of scope

**!!! DO try this at home !!!**

- 2FA
- Install AntiVirus
- Add Swap
- Set Security Limits
- IP Spoofing

# Install Docker via collections (Ansible-Galaxy)

- Geerling Guy – check his playbooks
- <https://github.com/geerlingguy/ansible-role-docker>
- roles and collections defined **requirements.yml**
- Install “dependencies” via:  
`ansible-galaxy install -r requirements.yml`

# Deploy example Docker app

## IDK GOOGLE?

- <https://www.google.com/search?q=hello+world+web+app+docker>

## HERE YA GO:

- browsing
- browsing
- This could be it: <https://github.com/crccheck/docker-hello-world>



**AUTOMATE**



**ALL THE THINGS!**



## **INUITS bvba**

**Essensteenweg 31  
2930 Brasschaat  
Belgium  
BE 0891.514.231**

**Contact:  
+32.380.821.05  
info@inuits.eu  
  
inuits.eu**

**Pavel Grochal**  
pavel.grochal@inuits.eu

## **INUITS s.r.o.**

**Brno Igloo**  
Hybešova 985/30  
602 00 Brno

**Prague Igloo**  
ImpactHub  
Drtinova 557/10  
150 00 Prague