ViciBox

Release 12.0

James Pearson

Sep 29, 2025

CONTENTS

1 Introduction **3**
- 1.1 Foreword . . . 3
- 1.2 Hardware . . . 4
- 1.3 Network . . . 8

2 Installation **13**
- 2.1 Media . . . 13
- 2.2 Phase 1 . . . 15
- 2.3 Phase 1.5 . . . 26
- 2.4 Phase 2 . . . 38

3 Networking **57**
- 3.1 Deployments . . . 57
- 3.2 Firewall . . . 58
- 3.3 SSL . . . 64

4 Maintenance **67**
- 4.1 Change Time Zone . . . 67
- 4.2 Change Root Password . . . 70
- 4.3 Change External IP . . . 72

5 Bug Fixes **73**
- 5.1 ViciBox 11.0 . . . 73
- 5.2 ViciBox 12.0 . . . 76

ViciBox is the official installation image for the ViciDial® Call Center Suite.

Official support is available through the ViciDial Group.

Free community-based support is available on the ViciDial Forums.

ViciBox is based upon the OpenSuSE Leap distribution. The official OpenSuSE Documentation is also available online.

See the *Installation Video* for a visual guide to installing ViciBox.

CHAPTER

ONE

INTRODUCTION

1.1 Foreword

This documentation is for the IT professional or sysadmin tasked with installing and maintaining ViciBox, focusing on back-end aspects that integrate with ViciDial. It does not cover ViciDial administration such as creating users, loading leads, configuring campaigns, etc. The goal is to get ViciBox to the point where those things are all that's left.

For ViciDial administration, we recommend downloading the official manuals. There is an Agent and Manager manual which cover all aspects of their respective web interfaces. They are available in either a free low-resolution black and white version or a high-resolution color paid-for version. The manuals are available at Eflo.net.

While this documentation aims to be complete, it will never cover everything. That is why the ViciBox manual was recreated as a GitHub project. This allows anyone to submit changes and additions to the manual for review. Who knows, the next one who benefits from what you submit might just be future you the next time you run into a problem. Ask me how I know.

1.1.1 Recommended Skills

This documentation is designed to help those who are new or inexperienced with ViciBox and not necessarily Linux itself. If you have never installed Linux before, it might be a good idea to find someone more experienced to help you. The good news is basic Linux experience will likely be enough to follow along with these instructions.

For network experience, you will need a decent understanding of what a LAN/WAN is and how a basic NAT firewall works. If you have never done a port forward before, then it might be a good idea to find someone more experienced to help you. ViciDial is very sensitive to its networking environment, so it's important that it be properly implemented.

You will be required to interact with the command line interface in order to install and set up ViciBox. While this can be done directly from the server itself, it's highly recommended to connect via SSH. You can use a stand-alone SSH client like Putty or the built-in `ssh` command if your operating system supports it.

1.1.2 Reading Guide

In order to remove as much ambiguity as possible, a certain syntax or style has been implemented. It is there to help readers understand what the intent of that instruction is. The following table shows how this style is implemented, what the intent is, along with a working example.

Table 1: Style and Syntax Example

As Written	Intention	Example
some **Prompt**	Look for the Prompt to come up on the CLI or console	at command prompt #
type `this`	Type everything in the block on the keyboard	type `yast lan` and
press `KEY`	Press the corresponding key, do not type out K E Y	press the `ENTER` key
press `TAB`	You may need to press the tab key multiple times	press `TAB` to move
press `KEY1-KEY2`	Press KEY1 and KEY2 at the same time	press `ALT-O` for OK

1.2 Hardware

The recommendations and suggestions in this section are based on a relatively conservative outbound dialing ratio. This assumes an outbound dial ratio of 5:1 for 25 agents. Actual capacity may vary depending upon dialing levels, lead quality, areas being called, time of day, etc. These recommendations should be viewed as a starting point for your own installs.

1.2.1 Dimensioning

Server scaling and dimensioning is one of the hardest parts of ViciDial. The specifications provided are more of a guideline than a hard rule. ViciBox and ViciDial itself will run on anything you can install it to. If you're just doing sandbox testing or dev work, then literally anything will work.

Express Box

Use the *Recommended* hardware specification at a minimum for an Express install. This is good for around 10-15 agents. If this server needs to be split and turned into a cluster then it should remain as the Web server.

Use the *Dedicated Database for 150 Agents* hardware specification for a more future-proof Express install. The hardware would likely be fine up to about 20 agents before resource contention becomes an issue. The good thing about starting with this hardware is that different roles can be split off of it while allowing it to continue being the dedicated database.

Telephony Server

Use the *Minimum* hardware specification if there is no call recording.

Use the *Recommended* hardware specification if there is call recording.

Both the above hardware specifications will allow for 25-agents and 125-trunks of capacity per server when using predictive dialing. For an inbound-only call center or one with minimal to no predictive dialing the above hardware specifications will allow for 50-agents and 250-trunks of capacity per server.

The biggest limitation is Asterisk, the telephony engine used in ViciDial. This is due to locking issue with Asterisk's internal channels. A channel is any connection between the Asterisk core process and any endpoint or module. For

example, a logged in agent is using two channels. One channel for their phone connection and one channel for the meetme conference. Every call placed or received through a SIP Carrier also creates its own channel. Starting a call recording uses a channel as well. At any one time a single agent can be using up to 6 channels in Asterisk. The more channels you have and the more activity you have on them is what drives the locking issue. This is especially prevalent with automated predictive dialing methods where a large number of channels are simultaneously created and generating a lot of activity with the Asterisk core. It's why 5 is the recommended calls per second for for most telephony servers. Asterisk also does not scale linearly with CPU performance. For example, a quad-core CPU might start having issues around 25-agents but an octal-core CPU might only get you up to 30-agents.

The second consideration with a telephony server centers around call recordings. The process of recording a call is initally done to a temporary RAM drive before being compressed to MP3 and written to the actual drive. Both of these processes require significantly more RAM and drive space. More memory might be needed if the calls are long (more then 30 minutes on average) or there are a high number of inbound calls. Drive size is mostly dictated by how many recordings you generate per day and the size of the recordings. If the recordings are not being offloaded to an archive server or NAS then it might be better to install a 2TB or larger drive. This is essentially required if it's a single-server ViciBox Express installation.

Web Server

The *Minimum* hardware specification is fine for 75 or so agents with SSL. Memory will likely need to be increased more then anything else.

The *Recommended* hardware specification is good for 150 or so agents with SSL. Once you start going above 150 agents I would just add RAM or CPU as you need it until you hit the TCP port limit. Drive storage needed for a web server is very minimal so the 500G drive listed in this spec is probably more then needed.

The ultimate limiting factor in a Web server is the number of available TCP ports. Apache, the web engine used in ViciBox, is configured to use all available TCP ports between 1024 and 65535. Once all of these ports are in use the web server essentially becomes unreachable for any new requests. Determining when you will hit this limit is difficult. It is dependant upon multiple factors such as how many agents you have, the features enabled in the agent interface, how much API use (or abuse) you are doing, and how long it takes for the database to respond with results. When this limit is finally hit there is no fix other then to have multiple web servers.

Apache itself mostly scales through available RAM followed by CPU performance. SSL in particular tends to be quite resource intensive and can easily cut the servers capacity in half. Fortunately memory and CPU is relatively cheap.

Database Server

The *Recommended* hardware specification is good up to about 75 agents as a dedicated database.

The *Dedicated Database for 150 Agents* hardware specification is good up to about 150 agents.

The *Dedicated Database for 300 Agents* hardware specification is good up to about 300 agents.

The limiting factor of the database is the memory table type in MariaDB. The memory table is a single-threaded table that runs exclusively in RAM. They are used for temporary tracking info and statistics within ViciDial. What happens is eventually this single thread cannot read the data from RAM, parse it, and return results fast enough. This results in queries being locked and delayed waiting to run against the table. Eventually this delay becomes great enough that it prevents ViciDial from operating correctly. Faster raw CPU speed helps but once you hit 5 or so Ghz there's no where left to go. In that situation the recommendation is to split the cluster into two smaller clusters. The good news is this isn't really an issue until you get to around 450 to 500 agents.

Memory is probably the best performance to value option with a database up to 64G. Everything after 64G or RAM is less effective due to the heavy write nature of ViciDial. In other words if 90% of the database load is all within the same 500-megs of data on the drive then there's only so much you can do with cache and buffers. Eventually the database just gets stuck waiting to read/write data from/to the drive.

For the drives it's recommended to use either a prosumer or enterprise grade drive. The Samsung Pro or Western Digital Black line of SSD drives are good examples of prosumer grade drives. An example of an enterprise grade drives would be the Intel Optane or Samsung PM lines. The primary drive metric you are looking for is mixed or random IO writes. ViciDial is very write intensive for a database application and random writes are what it does the most. The performance of even a basic SATA SSD is good enough for most smaller clusters. The second consideration with SSDs is their write endurance. This is why the prosumer grade or higher drives are recommended as their write endurance is much better. This is thanks to the use of MLC or TLC cells in the SSD as opposed to cheaper QLC cells.

Archive Server

The Archive server is an optional roll for ViciDial. Essentially all an archive server does is provide upload via FTP while allowing retrieval via HTTP. This is very likely a service that a common NAS or another server on the network can provide. The Archive server can even run in a VM.

Beyond providing the above services, all an archive server really needs is lots of reliable bulk storage. Hard Drives are a good fit for an archive server. It's recommended to use Enterprise-Class SATA Hard Drives for an archive server.

1.2.2 Specifications

CPU requirements are pretty lax for ViciDial. Anything newer than an AMD Zen1 (Ryzen 1000/Epyc 7001) or Intel Sandy Bridge (i3-2300/E3-1200) will work. The database will get the most benefit from multiple and faster CPU cores more than anything else.

ECC memory is not required but highly recommended. You can potentially do without ECC memory on the telephony servers since they should be rebooted daily in most cases.

SATA SSD is the recommended minimum for all drives used. Given how inexpensive SSDs are in the 500GB to 1TB size range, there really is no reason to be using spinning drives. The only use case for spinning drives in ViciDial would be in an archive server or NAS where you need tens to hundreds of terabytes of bulk storage.

RAID1 is also highly recommended for all servers. This can be accomplished through either a hardware RAID card or through two drives and the use of a software RAID. ViciBox has installation images available for both.

Minimum

- Quad (4) Core CPU 2.0+ GHz
- 8 GB RAM
- 160 GB storage

Recommended

- Quad (4) Core CPU 2.0+ GHz
- 16 GB RAM
- 500 GB storage

1.2.3 Dedicated Database for 150 Agents

- Octal (8) Core CPU 2.0+ GHz
- 32 GB RAM
- 500 GB storage

1.2.4 Dedicated Database for 300 Agents

- Sedecim (16) Core CPU 3.0+ GHz
- 64 GB RAM
- 500 GB NVMe storage

1.2.5 Example Installs

All the following examples use the *Recommended* hardware specification unless noted otherwise. Predictive Dialing is also assumed to be in use with a 5:1 dialing ratio. If the call center is inbound only or uses very minimal to no predictive dialing, you can also double the agent and trunk capacity shown.

15-Agent / 75-Trunk ViciBox Express

- All-In-One install, best for small call centers
- 75 trunk capacity
- Recommend using a 2TB drive if you want call recordings

75-Agent / 375-Trunk ViciDial Cluster

- Three telephony servers
- One web server
- One database
- Optionally an archive server or NAS to offload the recordings to

150-Agent / 750-Trunk ViciDial Cluster

- Six telephony servers
- One web server
- One database server using the *Dedicated Database for 150 Agents* hardware specification
- Optionally a second database server doing replication for reporting and backup

300-Agent / 1500-Trunk ViciDial Cluster

- Twelve telephony servers
- Two web servers to split agents onto
- One database server using the *Dedicated Database for 300 Agents* hardware specification
- Optionally a load balancer to distribute agent connections
- Optionally a second database server doing replication for reporting

1.3 Network

The network quality needed for VoIP is very different than what is needed for things like streaming or general productivity. It's most similar to the network quality needed for FPS gaming. In order of importance, you will want to monitor the Packet Loss, Jitter, and Latency between you and various endpoints like your SIP Carrier. Rarely is bandwidth solely the issue, and any sort of internet 'Speed Test' will generally not help.

All checks should be done from the servers themselves or from a host on the same physical network as the servers. Unfortunately, the quality of the internet varies with every hop, which can be problematic with work-from-home agents and SIP carriers. It's not uncommon to end up with an agent or carrier in New York who can connect to your server in Tampa just fine, while another agent or carrier in Los Angeles might be having issues. The internet is a fickle beast kept running with zip ties and extension cords while a chunk of pallet is used to keep the door shut and a trash bag for weather-proofing. Those from the telco world will get that joke. The rest of you will just have to learn it the hard way.

PingPlotter is recommended to check for network issues. For Linux and Mac users, you can also use the MyTraceRoute aka 'mtr' console application. Any examples or screenshots given in the following sections will be from PingPlotter.

And it pains me to write this, but WiFi should never ever be used for anything. All network connections should be wired. This is usually only a problem for work-from-home agents. My suggestion is to just buy them a very long cable.

1.3.1 Packet Loss

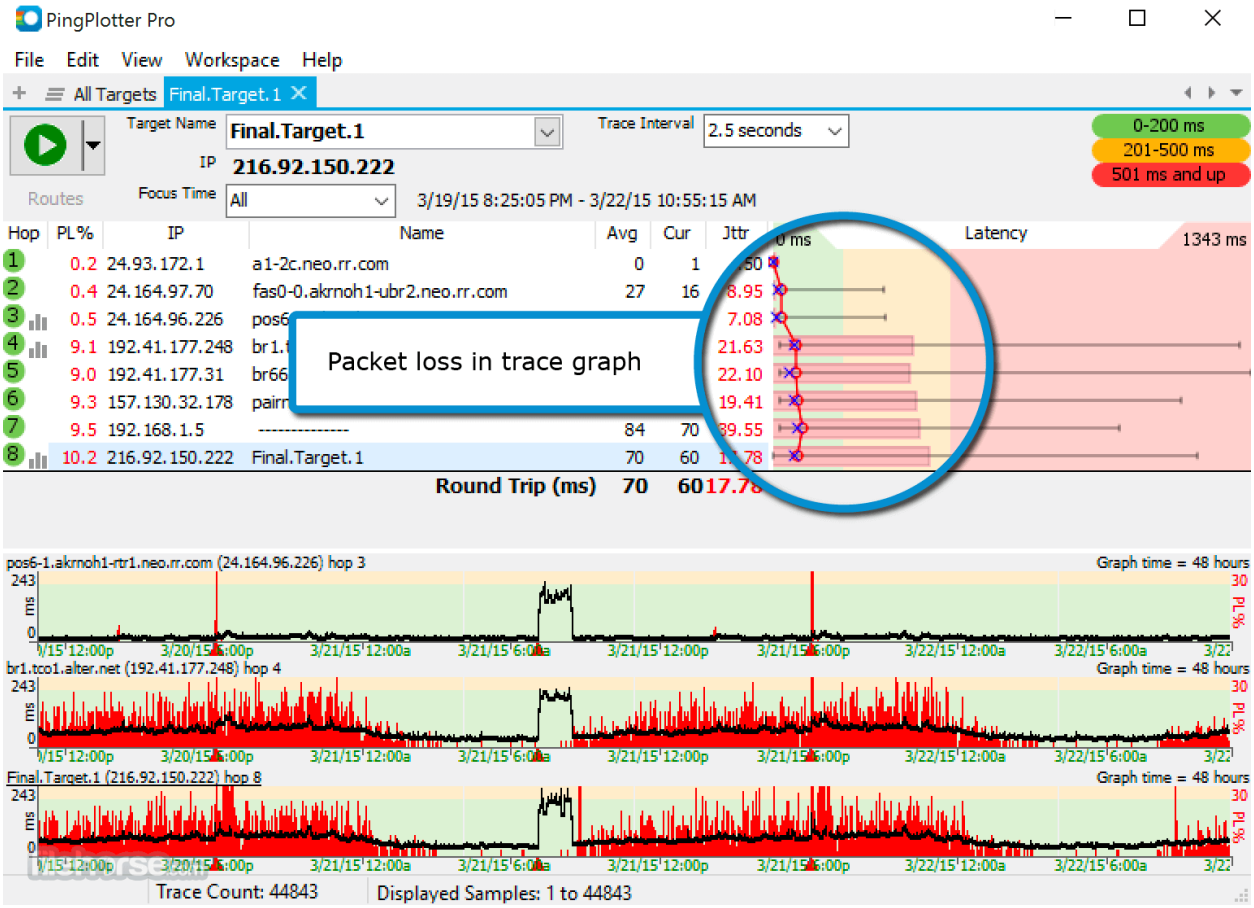
VoIP, especially SIP, is very sensitive to packet loss. Typically, any packet loss above 2-3% will start to result in significant audio quality issues. This will usually start as choppy audio or what sounds like clipping/stuttering. While less common, it might also manifest as chirping noises. The general rule is the greater the number of hops, the more likely and worse the packet loss will be. This loosely tracks with geographical distance. For instance, going from New York to the Philippines will greatly increase your chances of packet loss as opposed to going from New York to Los Angeles.

Generally, there is very little you can do about packet loss as it mostly seems to happen in the middle of the internet. Very rarely is the issue within your network or even your ISP's network. If your ISP is a large regional cable modem provider, then you are basically stuck waiting it out. If you are in an enterprise network space like a Data Center or Colocation Facility, then they might be able to help. It will depend upon how close the bad hop is to their network and if they have any alternate routing paths available. The good news is that packet loss is bad for everybody, so things will generally correct themselves pretty quickly.

When packet loss occurs, it will show up on the graph as a red shaded loss with every hop after it having a similar amount of loss. That means that the packet loss occurring at that hop is translating into packet loss at all the hops after it. If a hop is red showing packet loss, but all the hops after it don't have a similar amount of packet loss, then it's just that hop ignoring pings. Ignoring pings on routers is common as pings are viewed as a nuisance resource hog.

Example

This screenshot shows packet loss occurring at hop 4. You can tell because all hops after hop 4 have similar levels of packet loss. Real packet loss is always inherited to all the hops after it.



1.3.2 Jitter

Jitter is the difference between ping times to an endpoint over time. For example, if host A pings host B and gets 20ms, then pings them again 5 seconds later and gets a 30ms ping, the jitter is 10ms between host A and B. If you repeat this every 5 seconds and average the results over 5 or so minutes, you will get a good measurement of the network's jitter. All networks have a base level of jitter. The problem is when this jitter starts to exceed 100ms on average. This is where audio starts to be affected.

Jitter mostly manifests in the audio as distortion. Common descriptions of the audio would be that it sounded 'muddy', 'underwater', or 'warped'. Sometimes it will also manifest as chirps or slurring. This is less common and can often be confused with packet loss.

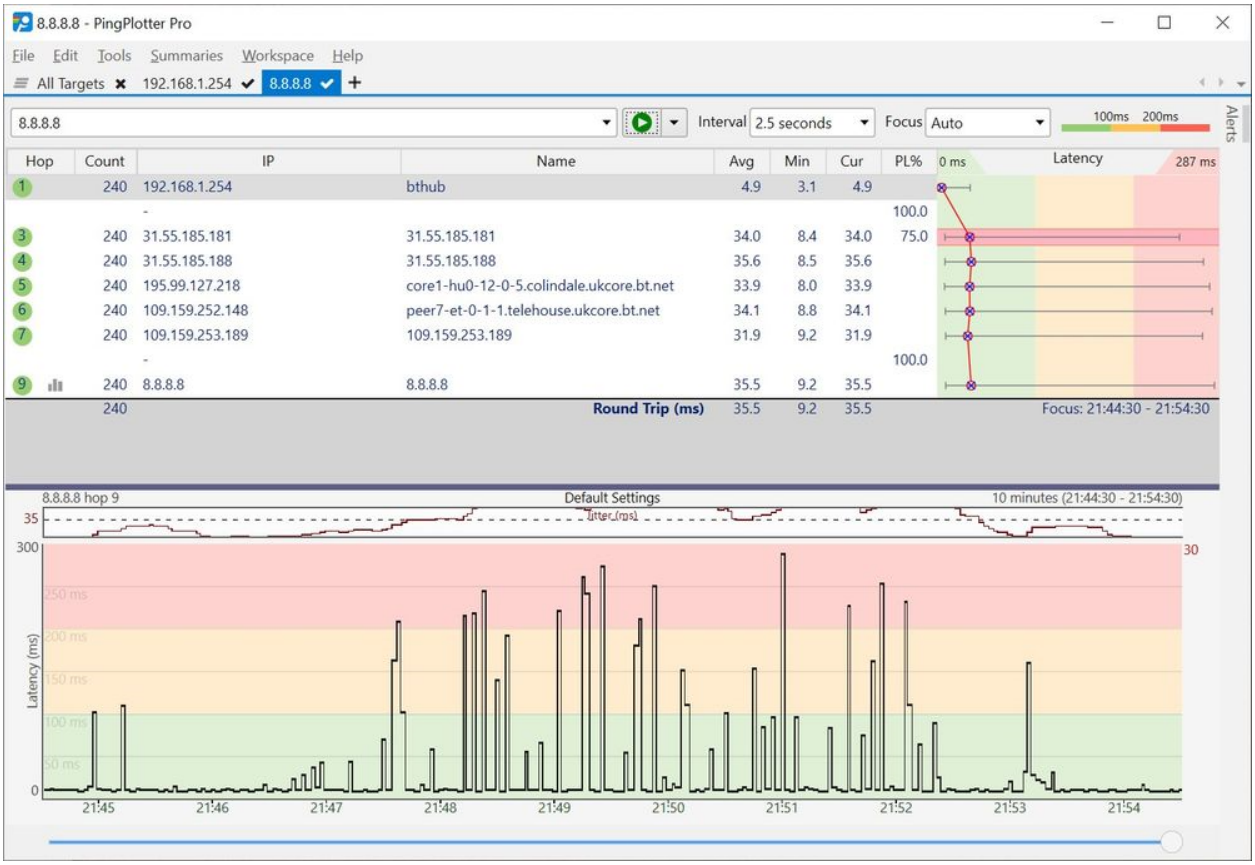
High jitter spikes are usually attributed to network connections nearing their capacity. This causes buffering on the network interfaces, which results in network delays. In our experience, jitter is either happening in the middle of the network like with packet loss, or it's happening at the local router. If jitter is happening in the middle of the internet, then there is not much you can do but hurry up and wait. Things will usually clear out with time, but it's not uncommon to have jitter be an issue for minutes to hours at a time.

If the jitter is happening at the network's local router, then it's usually the result of a bandwidth restriction. High-bandwidth sites like YouTube and Netflix or large file downloads like Windows Updates or automated backups can

saturate the connection with the ISP. The solution is to either get more bandwidth and/or restrict what people should be accessing on the internet. If you have a more advanced router, you can do things like bandwidth restrictions and block websites. Sometimes the issue is that the router is just overloaded. This is most common on the cheap routers. If you are running a mid-range router like an Asus RT-AC86U or better, then the router is likely not an issue.

Example

The screenshot shows bad jitter in the bottom graph. You can see the black lines go from around 35ms (the average ping time) to as high as 290ms every 5 seconds or so. This is excessively high jitter and this connection will have bad audio. Also of note on this example is that hop 3 looks like it is experiencing packet loss but it's not. You can see that the next few hops after hop 3 do not show similar levels of packet loss. This means that hop 3 is just ignoring ping, which is normal.



1.3.3 Latency

Latency is the measure of how long it takes data to go from Host A to Host B. Latency under 100ms is considered good. It really only becomes a problem when you start getting up to 250ms of latency. At this point, the delay in the audio becomes apparent to the caller and agent. It's possible for agents to learn to work with the delay, but it's not desirable. In situations where you have US callers with agents in the Philippines, there's nothing you can do but work with it. It is quite impressive how well some agents can work around the delay.

Latency mostly tracks with geographical distance since the speed of light is only so fast. So the latency from New York to the Philippines will always be much higher than the latency from New York to Los Angeles. If you are using a large regional ISP like a cable modem provider, then there is really nothing you can do. Latency is not much of an issue for what most of the internet is used for. If you are in an enterprise network space like a Data Center or Colocation

Facility, then there's a chance they might be able to help. It will depend upon if they have any alternate routes with better network conditions.

CHAPTER

TWO

INSTALLATION

ViciBox is installed in two phases. The first phase installs the base ViciBox operating system onto the server. The second phase involves setting up ViciDial itself. There is an interim phase, referred to as Phase 1.5, where some ancillary processes happen.

2.1 Media

ViciBox supports installation from a USB flash drive as well as a CD/DVD drive. This is accomplished through a hybrid ISO file that can be used for either media type. A simple ISO to USB writer like ImageUSB or Rufus can be used to create the installation thumb drive. There are two different installation media currently available for ViciBox.

2.1.1 Standard ISO

`Standard Installation Image`
: The 'standard' version is for installation into a system with a single drive. It's the ideal option if you have a Hardware RAID, a Network or SAN you boot from, or are using a VM Guest for install. It's also the least involved to setup since it lacks the MD software RAID.

2.1.2 MultiDevice ISO

`MD RAID1 Installation Image`
: The 'MD' or MultiDevice RAID media installs the OS into a software RAID-1. This allows two plain drives to be used together for failure redundancy without any special hardware or server support. For best results, the two drives should be a matched pair in terms of size and connection type (SATA/NVMe). If one drive is slightly smaller or faster it should be installed as the first drive in the system. The smaller or faster drive also needs to be the selected target drive during the Phase 1 installation. If you install to a larger drive you won't be able to add the smaller one to the RAID array. Unfortunately, drives don't let you put 2TB of stuff into a 1TB bucket.

  The RAID setup tool, `vicibox-mdraid1`, supports mixing between SATA and NVMe drives. You can add new drives to the array as well as spares or to replace a failed drive. Unfortunately, the tool does not support removing drives from the array or converting the array to any other type (RAID 0/5/6/10/50/60/etc). Fortunately, if you have a hot-swap drive chassis you can just safely yank the drive and Linux will carry on as if nothing happened.

2.1.3 Create USB Install Media

This guide will walk you through creating a USB flash install media. The USB flash drive needs to be at least the size of the downloaded ISO. Any data that exists on the USB flash drive will be lost if you follow the below instructions.

Windows

There are many different programs available to write an ISO image to a USB flash drive. Rufus was used in this example since it's well known. Other options that have worked well is imageUSB from OS Forensics. If you run into problems with either of these you may need to run them as Administrator.

1. Download the appropriate install image: *Standard ISO* or *MultiDevice ISO*
2. Download Rufus
3. Run the downloaded Rufus executable from the previous step, I.E. 'rufus-4.0.exe'
4. Under 'Device' make sure it lists the correct USB flash drive to use
5. Boot selection should say "Disk or ISO image"
6. Click the Select button and select the downloaded ISO from step 1
7. Leaving all the rest of the settings at their defaults, click the 'Start' button at the bottom
8. In the pop-up window, click the 'OK' button to start writing the image to the USB flash drive
9. Sometimes there is a warning pop-up about searching for grub. If that happens, just click "OK" to continue
10. In the warning pop-up explaining that the flash drive is about to be erased, click the 'OK' button
11. When it's done, just click the 'close' button and remove your USB flash drive. It's now ready to install ViciBox.

Mac

balenaEtcher is a cross-platform tool that makes it easy to write ISO images to USB drives.

1. Download the appropriate install image: *Standard ISO* or *MultiDevice ISO*
2. Download and install balenaEtcher
3. Open balenaEtcher from your Applications folder
4. Click "Flash from file" and select the downloaded ISO
5. Click "Select target" and choose your USB drive
6. Click "Flash!" to begin writing the image
7. Enter your administrator password when prompted
8. Wait for verification to complete
9. Once complete, safely eject the USB drive. It's now ready to install ViciBox.

Linux

They're only reading this part to complain about how I didn't use the right utility with the right flags in some superior form of shell. I win.

1. Install Linux
2. ???
3. Profit, err, successfully written install media

2.2 Phase 1

The following section uses the MD (MultiDevice) software RAID version of ViciBox. If you run into issues with RAID setup, it is recommended to wipe the drives with `wipefs -fa /dev/sdX` (replace sdX with device ID) and start over. The installation of the non-MD version is similar but with fewer steps.

Note: The installation process will destroy all data on the installation target disk. Make sure to back up any data you want to keep before proceeding.

2.2.1 Installation Steps

1. Boot from the install *Phase 1*.
2. By default the install media will boot from the server's local drive. Select **Install ViciBox** and press `Enter` to start the ViciBox install.
3. If there are multiple disks present in the system you will need to select the boot disk. Typically the first disk in the list is the first boot disk. Using the up and down arrow keys select the installation disk and press `Enter`.
4. A confirmation dialog box will open to confirm the destruction of all data on the installation disk. If you proceed past this point there will be permanent data loss on the installation disk. Press `Enter` to select **Yes** and start the installation process.
5. You will see a couple of progress indicators as the installer copies ViciBox to the installation disk. After that the system will boot from the installation disk and continue installing. After a short wait a **login:** prompt will be displayed along with the current network configuration. At this point the rest of the instruction can be carried out through either the console or SSH.
6. At the **login:** prompt type `root` and press `Enter`.
7. The first root login to the system will start a configuration wizard. Press `Enter` to continue.
8. Using the up and down arrow keys, select the system's localisation and press `Enter`.
9. Using the up and down arrow keys, select the system's keyboard layout and press `Enter`.
10. Using the up and down arrow keys, read through the license until satisfied. Press `Enter` to continue.
11. Using the `Tab` key, select **Yes** and press `Enter` to accept the license.
12. Using the up and down arrow keys, select the system's local timezone and press `Enter`.
13. Type in the new root password you want to use and press `Enter`. To keep the old root password type in `vicidial`.
14. Type in the new root password again from the above step to confirm it and press `ENTER`.

15. If internet connectivity is available, the system will ask to install updates. Press `ENTER` to continue and install updates.
16. If the MD RAID installation image was used, the system will ask to setup the RAID array if appropriate target drives are present. Select the appropriate drive number from the shown list and press `ENTER`.
17. The RAID setup tool will ask to confirm the destruction of the target drive. Press `ENTER` to confirm the target drive.
18. The RAID setup is complicated with all the various states that old drives can be in. If you run into any issues with RAID setup it is recommended to wipe the drives with `wipefs -fa /dev/sdX` (replace sdX with device ID) and restart the installation from step 1.
19. Once the **vicibox12:~ #** command prompt is displayed with a cursor, the installation is complete. It is highly recommended to remove the installation media and reboot. To reboot, type `reboot` and press `ENTER`.

Congrats, ViciBox has been installed. Please remember the password you used as it will be needed in the next phase.

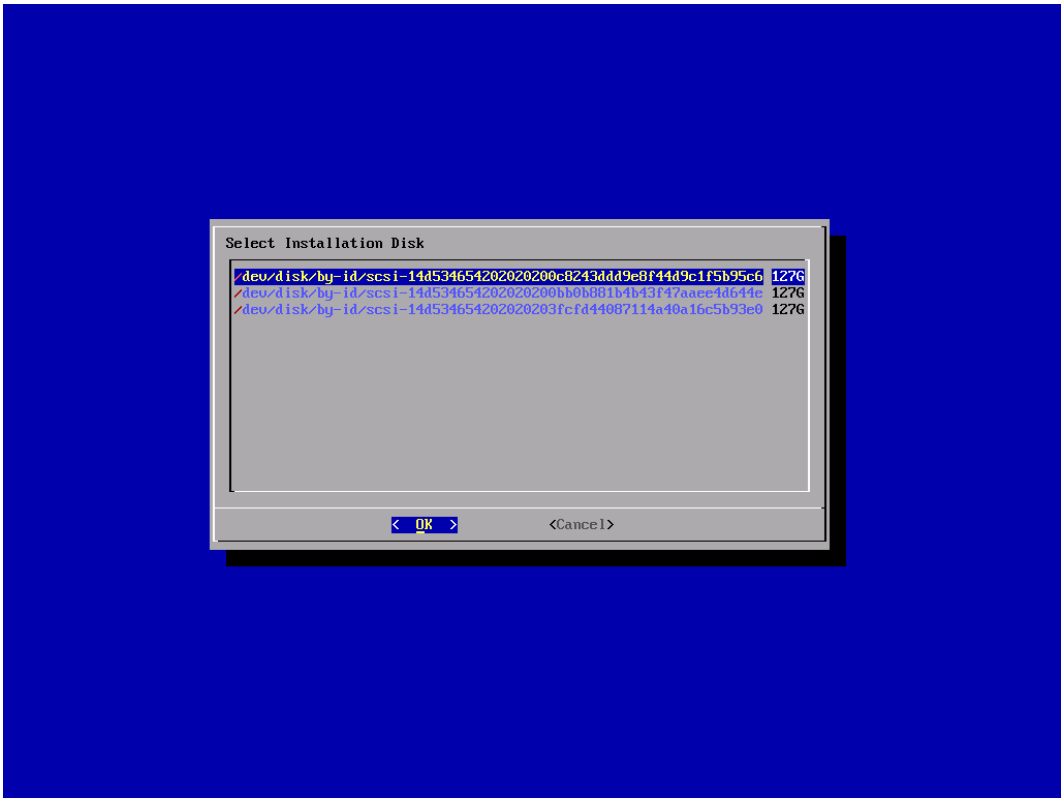
2.2.2 Installation Video

Watch the ViciBox v.12.0 Phase 1 Installation Video.

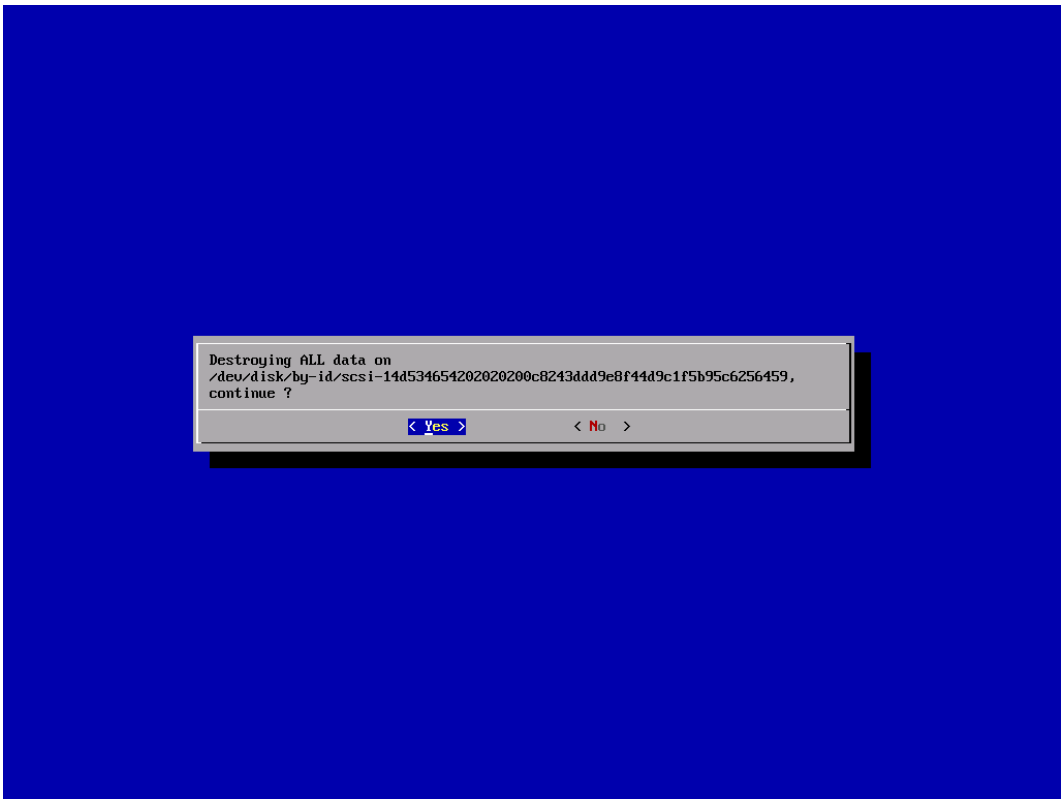
2.2.3 Screenshots

Select Install ViciBox

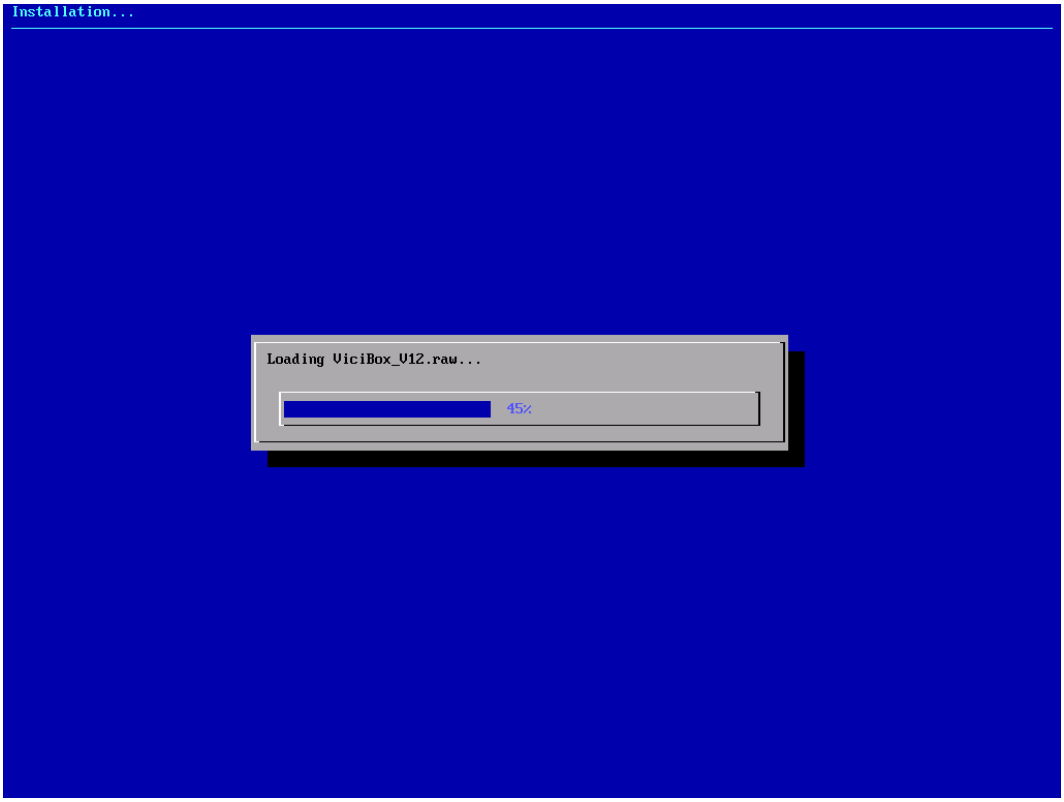
Select Installation Disk



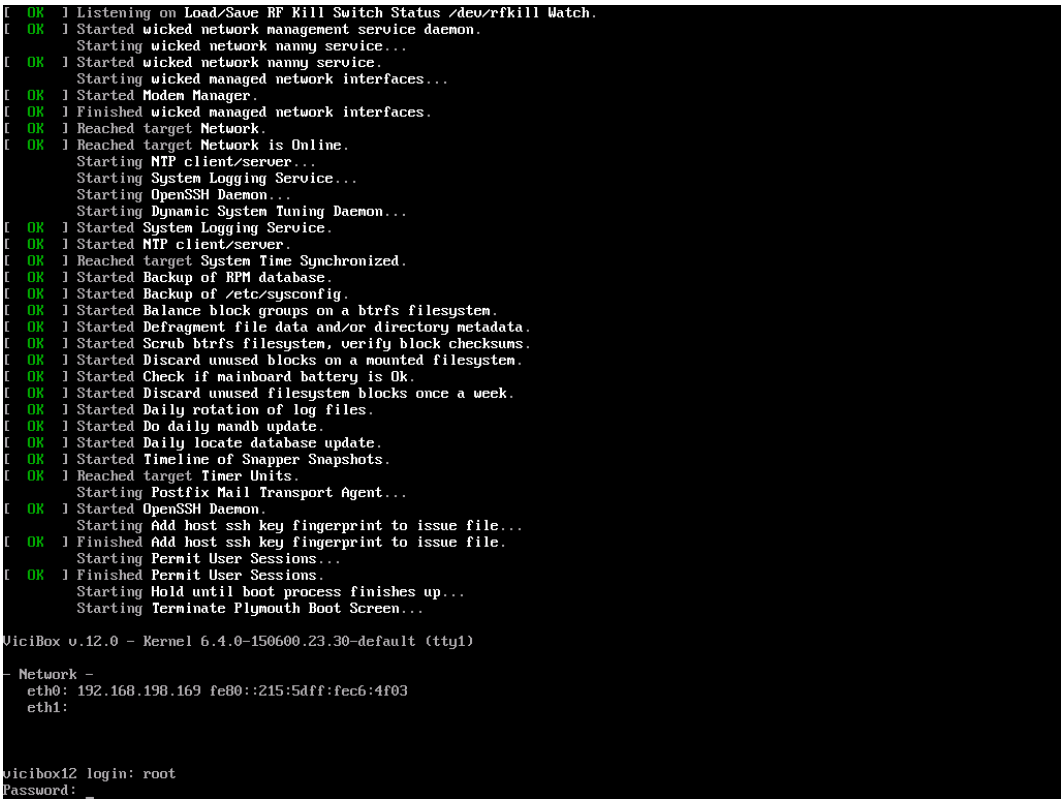
Confirm data destruction



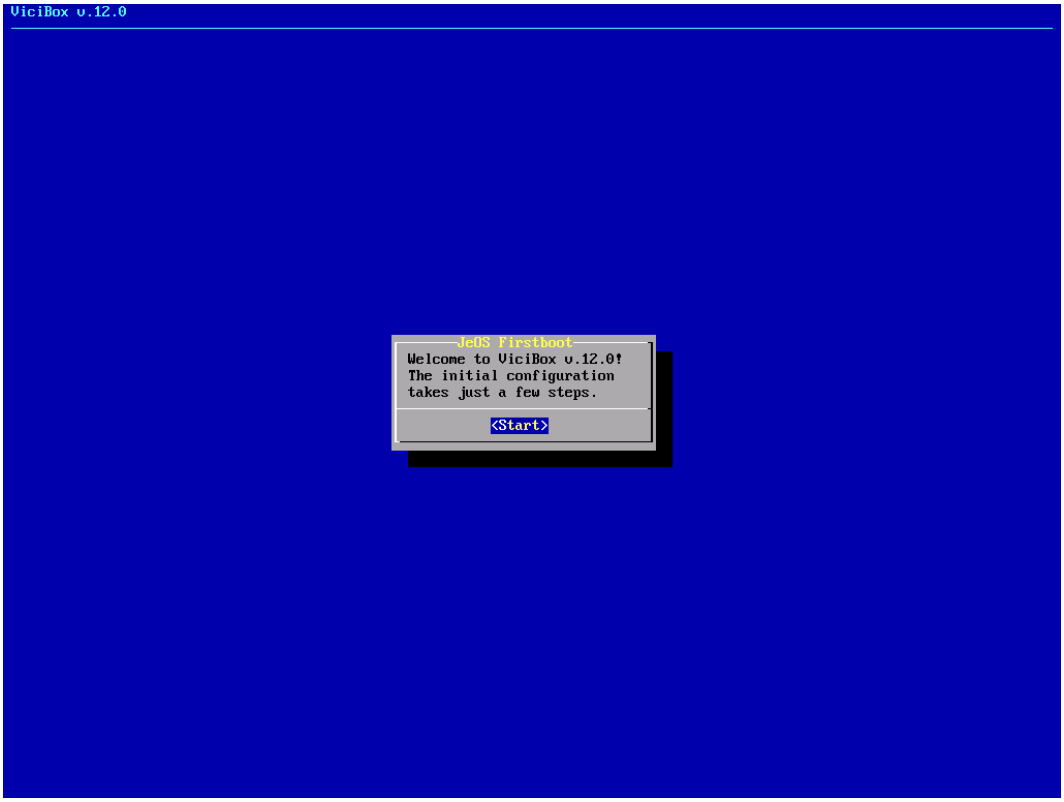
Installing to disk



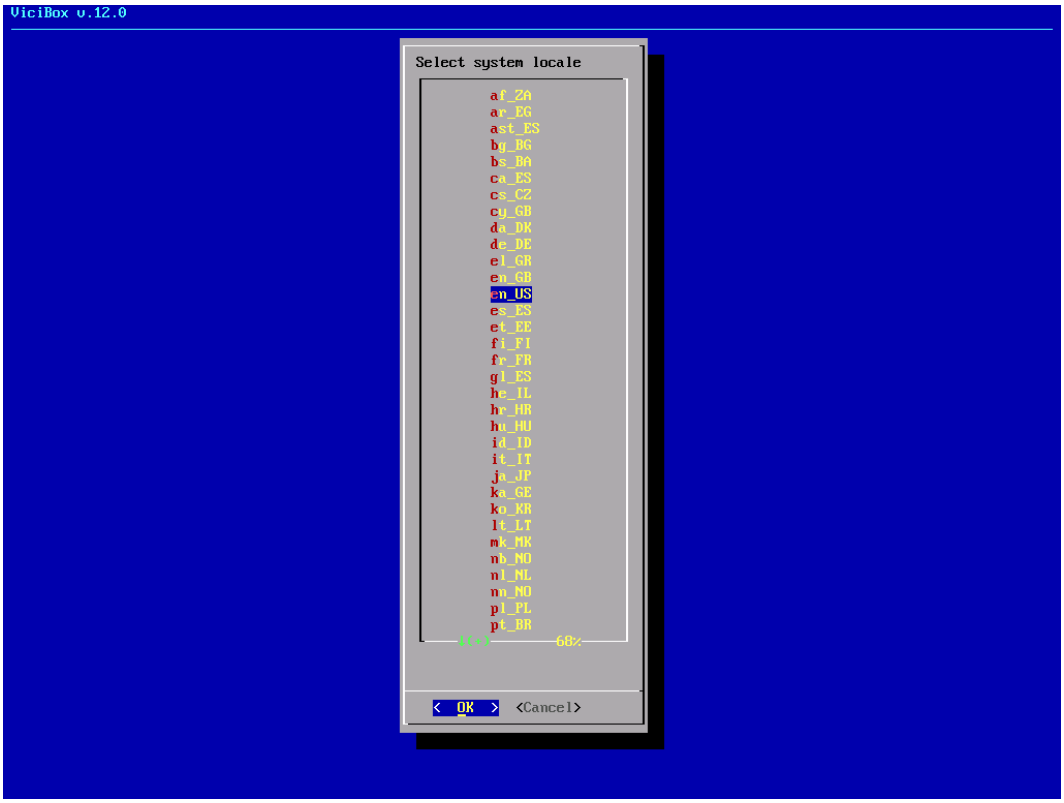
Login as root



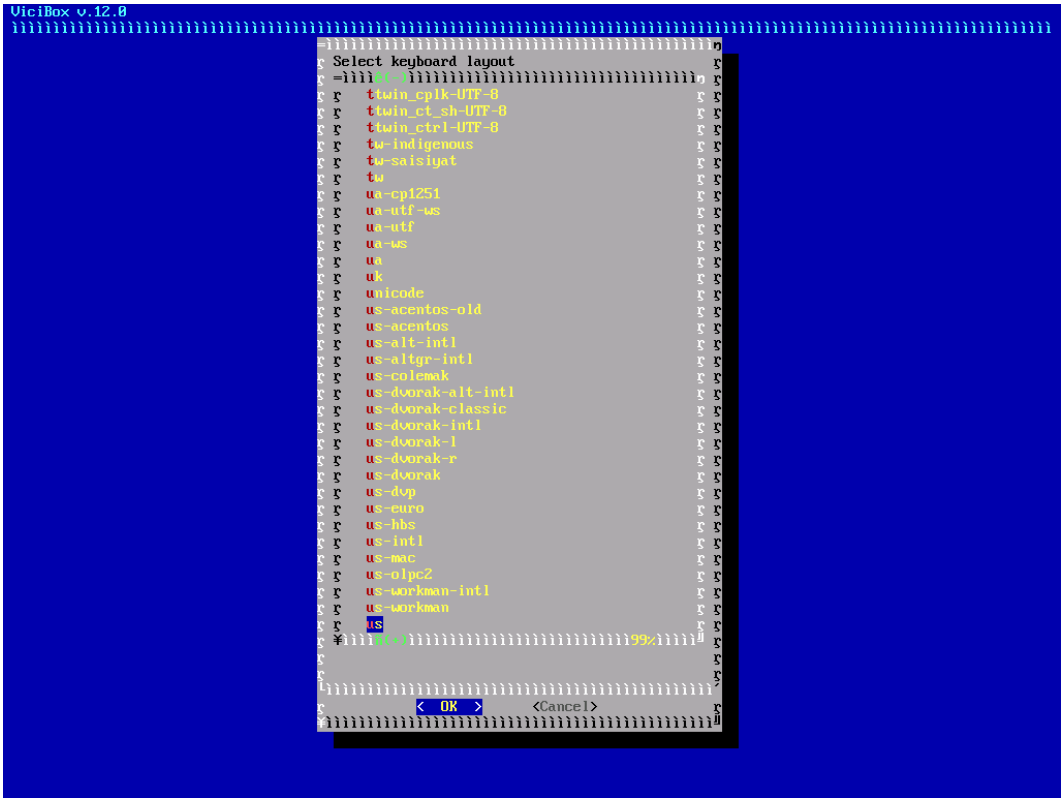
First Login



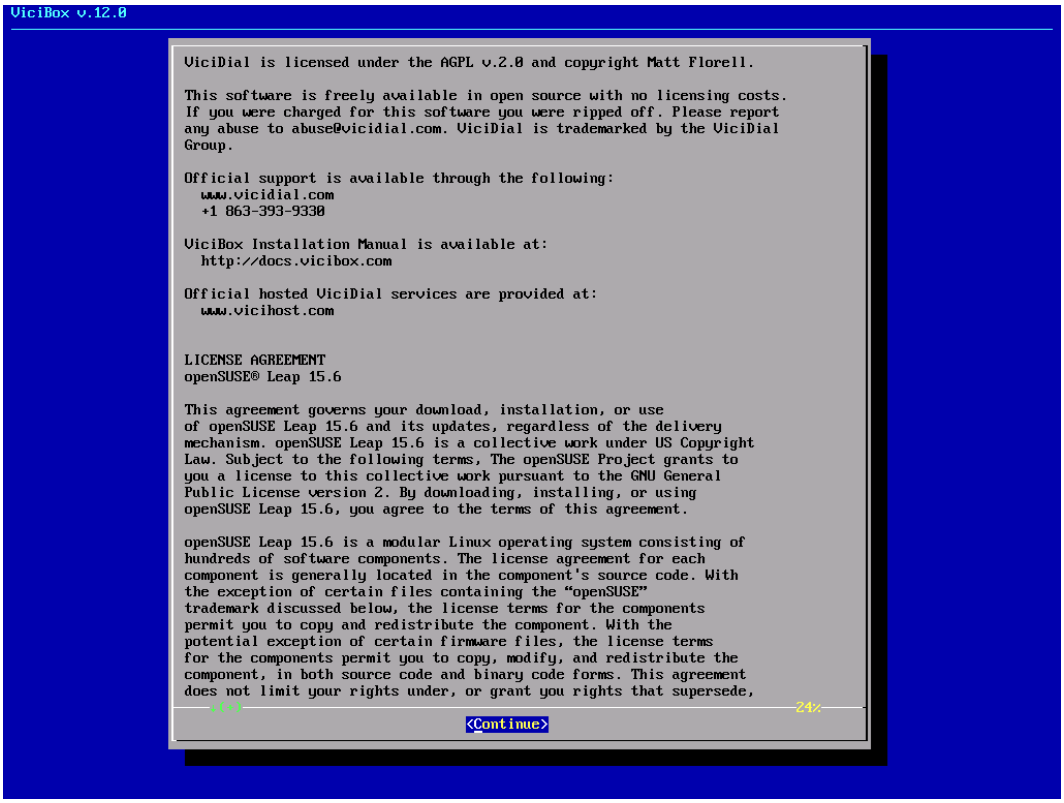
Select system locale



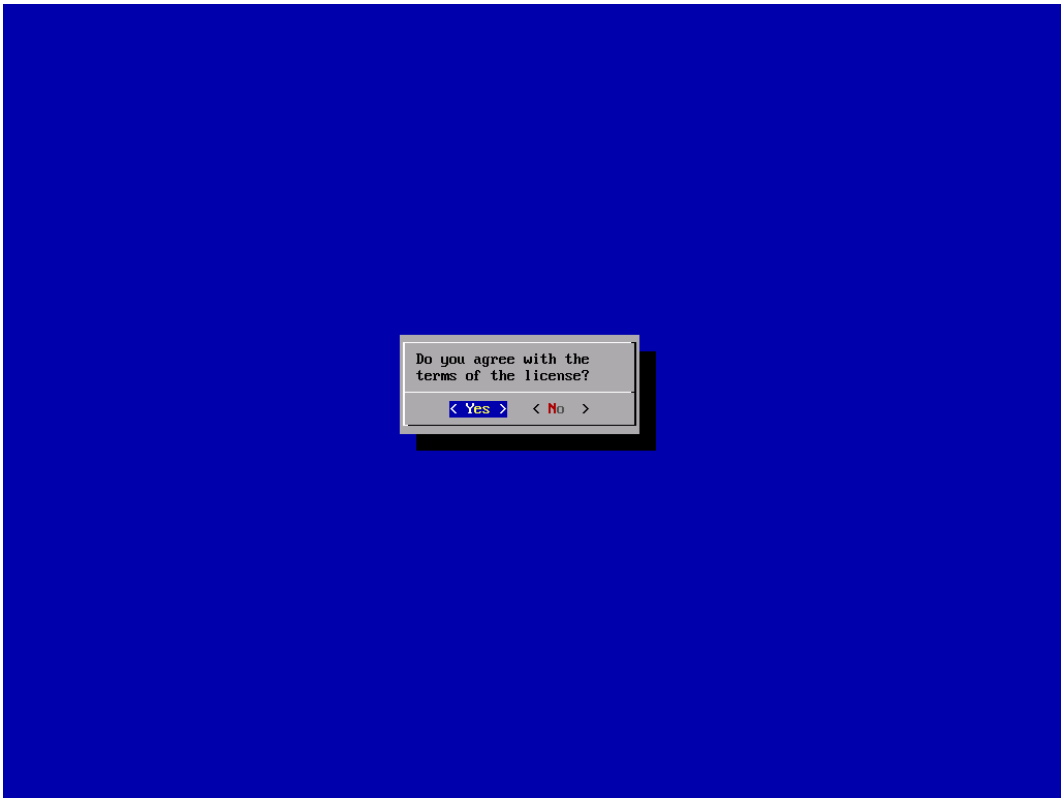
Select keyboard layout



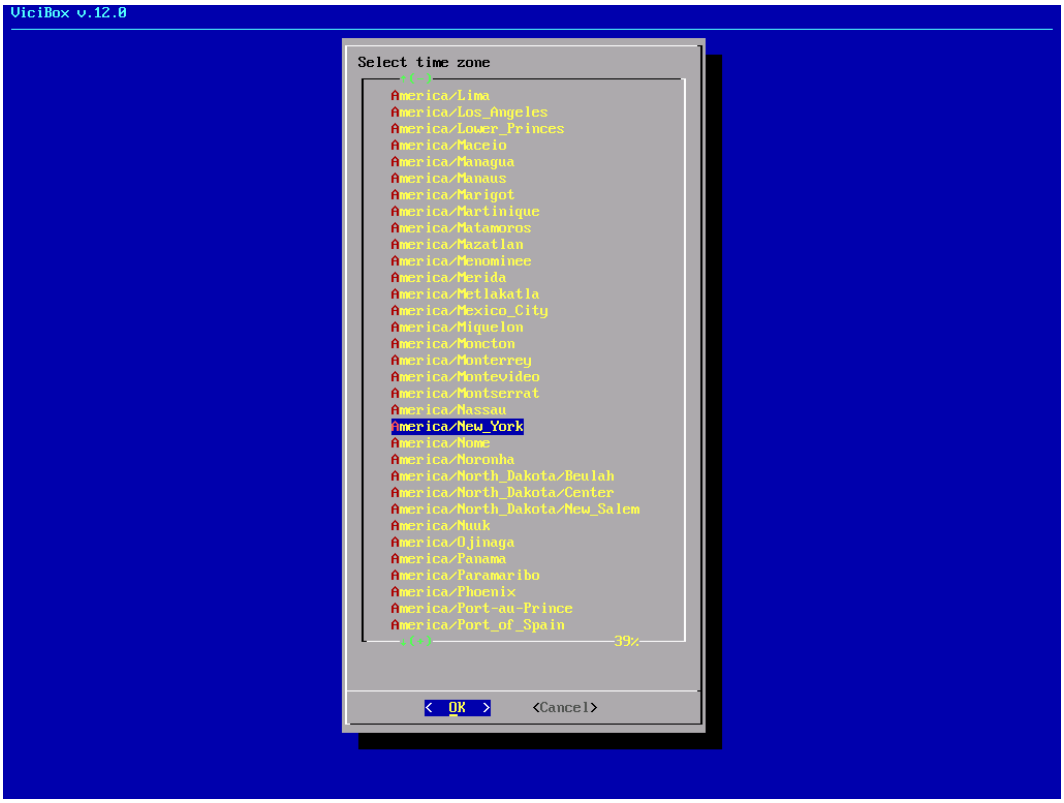
Read through license



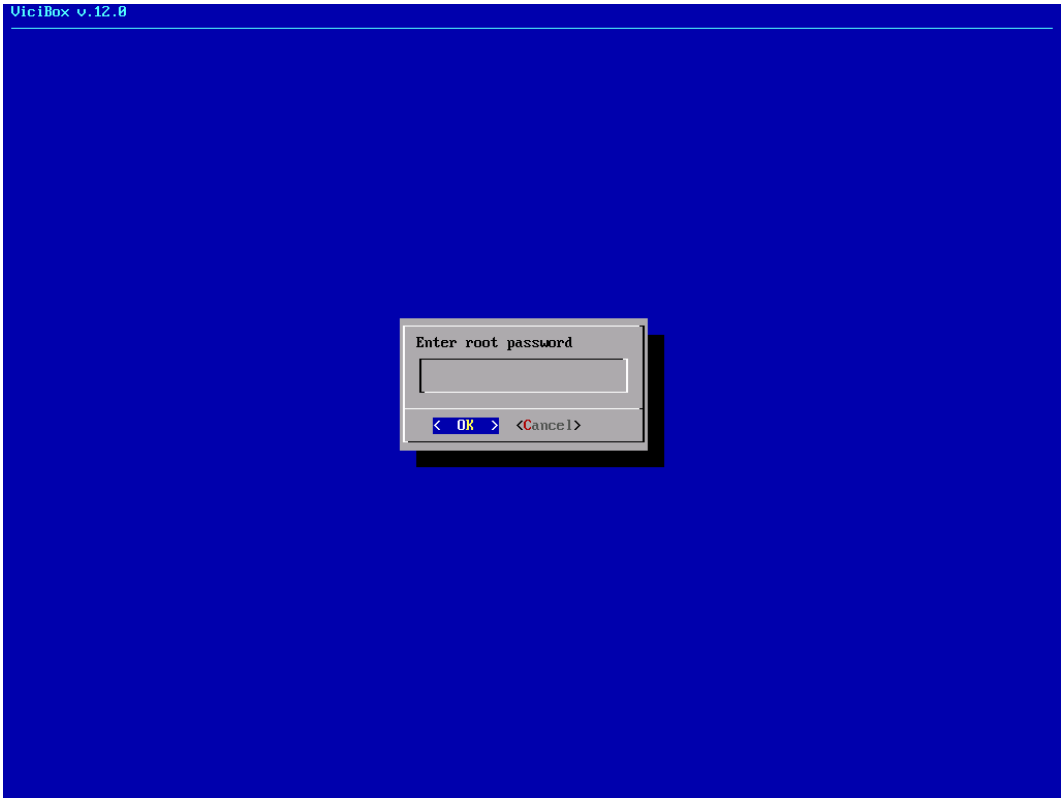
Accept the license



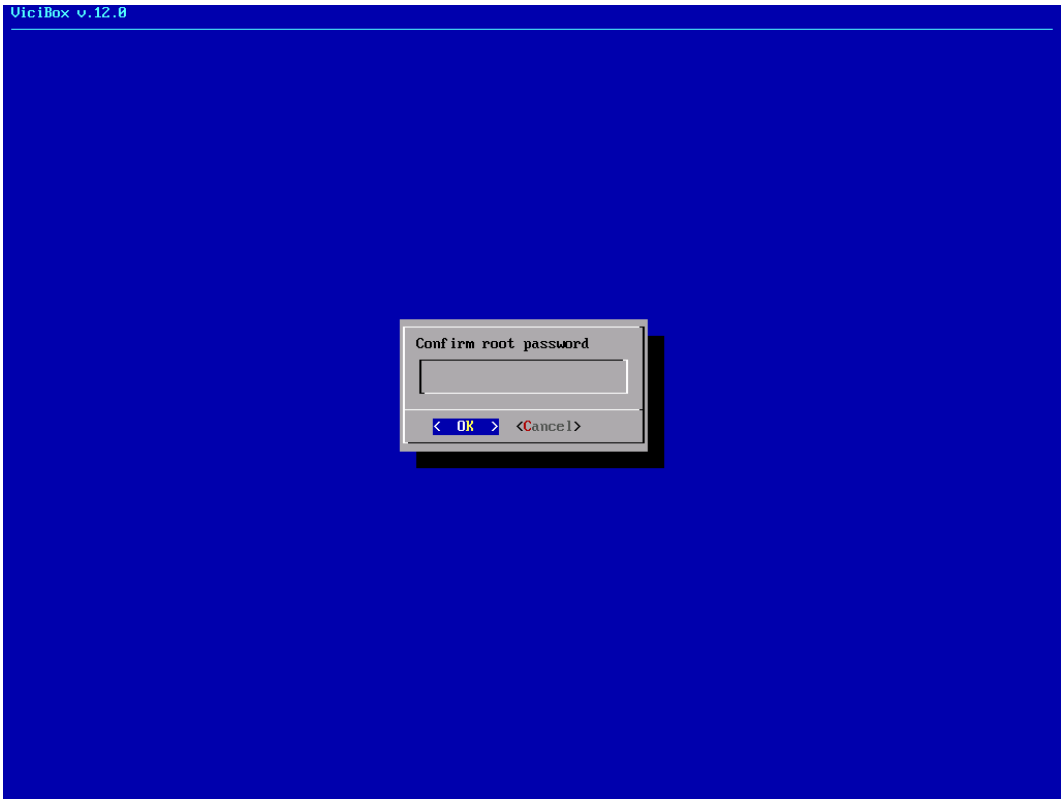
Select timezone



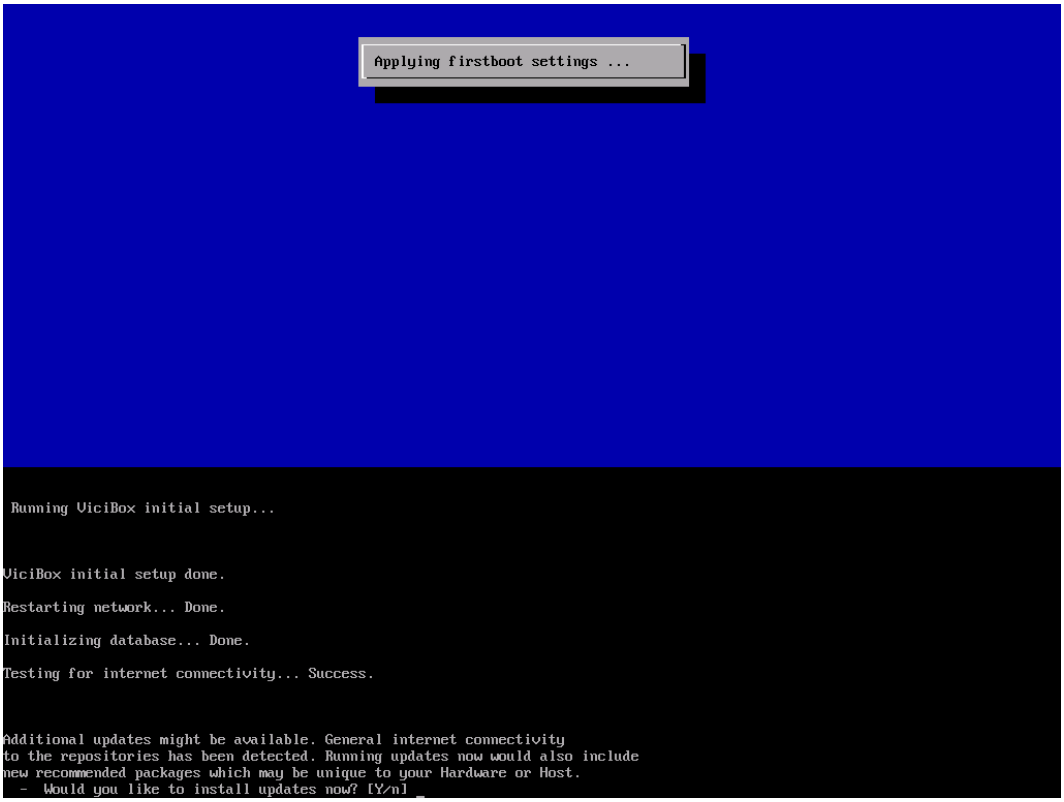
Type in new root password



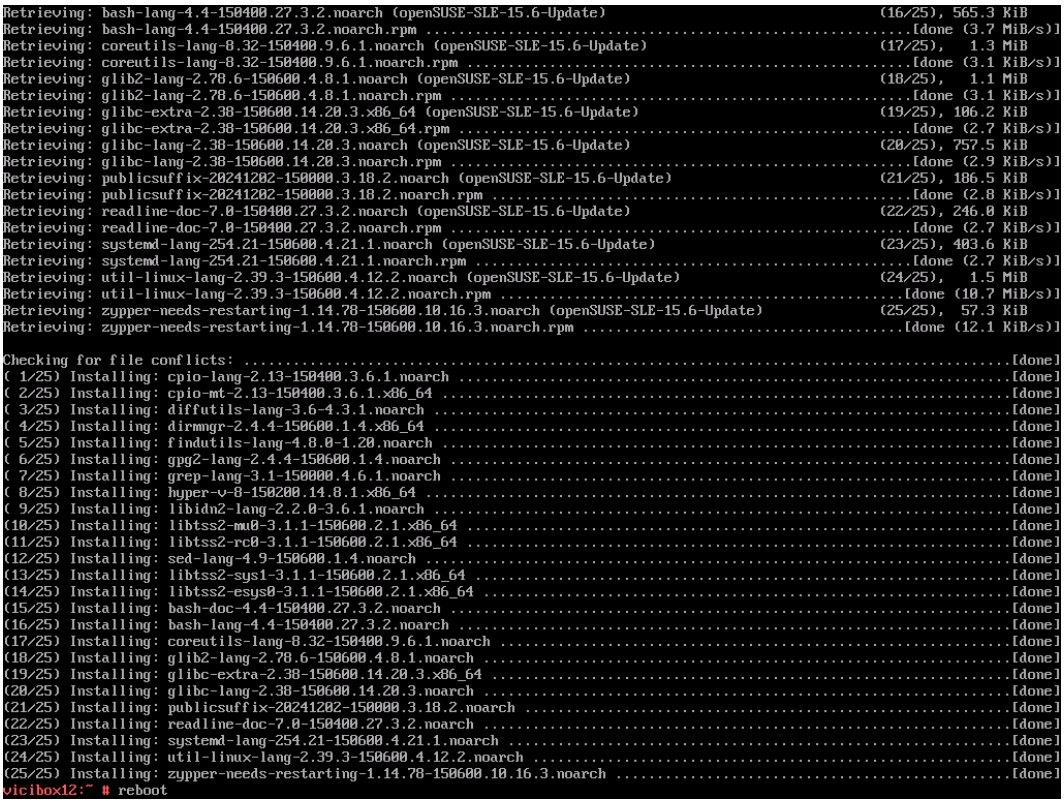
Confirm the new root password



Install updates over internet



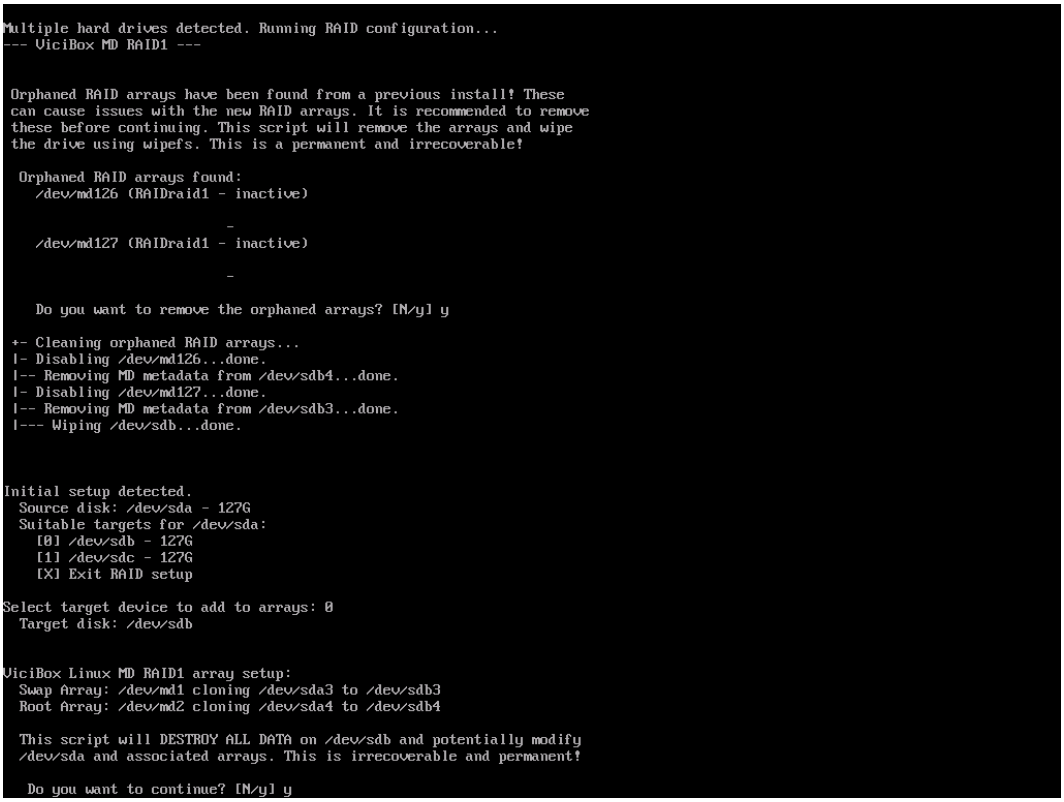
Installation complete without RAID



2.2.4 RAID Specific

The following screenshots show installation sections related to the MD RAID image. This is only ran when multiple-drives are detected in the system and /dev/md2 is being used for root.

Select target drive to add



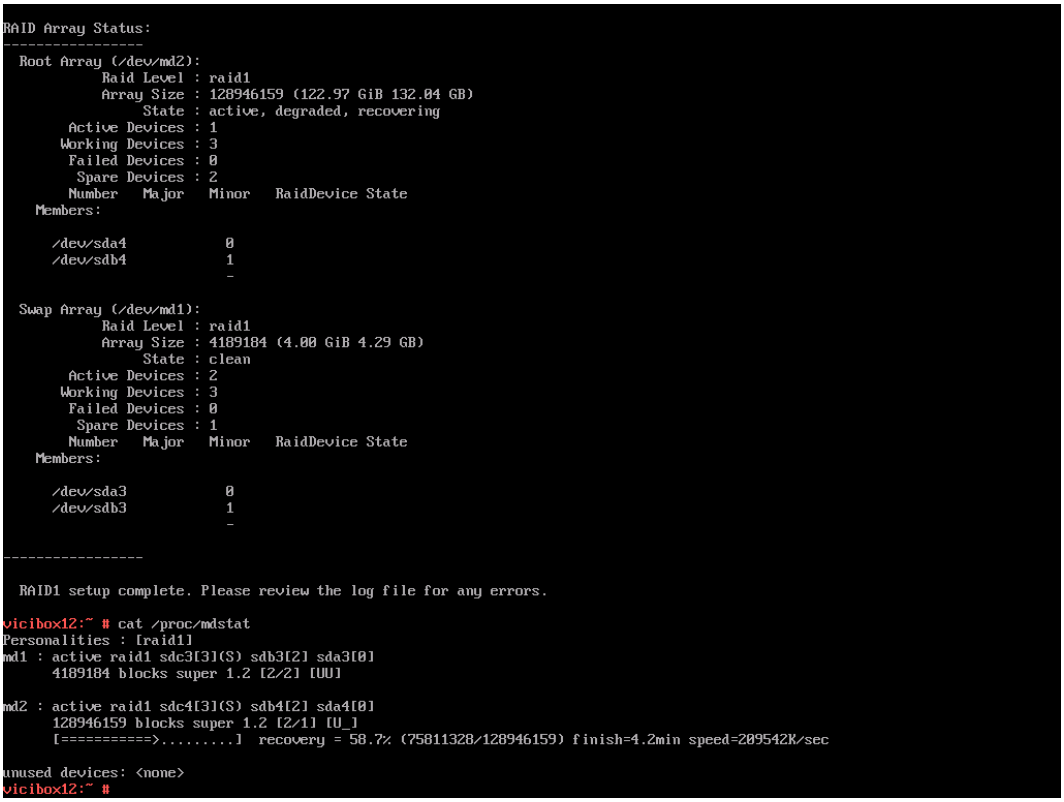
Verify successful setup then reboot

```
  Generating new mdadm.conf... done.
  Installing grub boot loader on /dev/sdb... done.

RAID Array Status:
-----------------
  Root Array (/dev/md2):
           Raid Level : raid1
           Array Size : 128946159 (122.97 GiB 132.04 GB)
                State : active, degraded, resyncing (DELAYED)
       Active Devices : 1
      Working Devices : 2
       Failed Devices : 0
        Spare Devices : 1
       Number   Major   Minor   RaidDevice State
    Members:

      /dev/sda4           0
      /dev/sdb4           1

  Swap Array (/dev/md1):
           Raid Level : raid1
           Array Size : 4189184 (4.00 GiB 4.29 GB)
                State : clean, degraded, recovering
       Active Devices : 1
      Working Devices : 2
       Failed Devices : 0
        Spare Devices : 1
       Number   Major   Minor   RaidDevice State
    Members:

      /dev/sda3           0
      /dev/sdb3           1

-----------------

  RAID1 setup complete. Please review the log file for any errors.

vicibox12:~ # cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sdb3[2] sda3[0]
      4189184 blocks super 1.2 [2/2] [UU]

md2 : active raid1 sdb4[2] sda4[0]
      128946159 blocks super 1.2 [2/1] [U_]
      [==>..................]  recovery = 10.4% (13429440/128946159) finish=9.5min speed=200833K/sec

unused devices: <none>
vicibox12:~ # reboot
```

Add a new or spare drive to the array

```
vicibox12:~ # vicibox-mdraid1
--- ViciBox MD RAID1 ---
RAID Array Status:
-----------------
  Root Array (/dev/md2):
           Raid Level : raid1
           Array Size : 128946159 (122.97 GiB 132.04 GB)
                State : clean, degraded, recovering
       Active Devices : 1
      Working Devices : 2
       Failed Devices : 0
        Spare Devices : 1
       Number   Major   Minor   RaidDevice State
    Members:

      /dev/sda4           0
      /dev/sdb4           1

  Swap Array (/dev/md1):
           Raid Level : raid1
           Array Size : 4189184 (4.00 GiB 4.29 GB)
                State : clean
       Active Devices : 2
      Working Devices : 2
       Failed Devices : 0
        Spare Devices : 0
       Number   Major   Minor   RaidDevice State
    Members:

      /dev/sda3           0
      /dev/sdb3           1

-----------------
Do you want to add another device to the arrays? (N/y) : y

  Source disk: /dev/sda - 127G
  Suitable targets for /dev/sda:
    [0] /dev/sdc - 127G
    [X] Exit RAID setup

Select target device to add to arrays: 0_
```

Verify spare (S) drive is added to array



2.3 Phase 1.5

Before ViciDial is installed and set up on the servers, it is necessary to configure the network. Since this is a convenient stopping point, it is also a good time to do other things like install updates. It's recommended to do both of these where possible.

2.3.1 Static IP

While not necessary, it is highly recommended to use a static IP. Once ViciDial is installed, its configuration will be tied to the current LAN and WAN IP. If those IPs change, then ViciDial's configuration must also change to match. While not usually a problem with a LAN, a static IP is very important for the WAN. This static WAN IP is what will allow ViciDial to work reliably behind firewalls and with SIP carriers.

This might not be a problem if the ISP doesn't rotate the IPs that often. My residential cable modem ISP seems to rotate the IP every 30 days. Still, the cost to get a static IP is usually worth what a few hours of unexpected downtime in the middle of the day will be.

The IP address, net mask, and default gateway will be unique to your network and is beyond the scope of this document. While the DNS servers listed in the below example can be used safely it might be better to use the local router or ISP for DNS instead.

If there is a LAN and WAN network connected to the server then the WAN's default gateway should be used. There should only ever be one default gateway on the server no matter how many networks it is connected to.

If this server is to be used in a ViciDial cluster then each server must have a unique hostname. The recommended convention is 'DBX', 'webX', and 'dialerX'. For example, a basic three server cluster would use the hostnames 'DB1',

'web1', and 'dialer1'. An additioner Telephony server would be 'dialer2', etc. Please limit the hostname to 16 characters or less.

Network Settings

Table 1: Example Network Configuration

Setting	Value
Host Name	vicidocs
IP Address	192.168.50.4
Subnet Mask	255.255.255.0 (/24)
Default Gateway	192.168.50.1
Name Server 1	208.67.222.222
Name Server 2	208.67.220.220

Note: While the server supports IPv6 ViciDial itself has not been extensively tested with it. Therefore the documentation will assume IPv4 only for all networking.

YaST Network Configuration

1. If not already, login as the `root` user to get to the `#` command prompt.
2. Type `yast lan` to start the network configuration.
3. Press the `TAB` key until the network interface is highlighted.
4. If there are multiple network interfaces, use the up and down arrow key to highlight the correct network interface
5. Press `ALT-I` to edit the highlighted network interface.
6. Press `ALT-T` to select **Statically Assigned IP Address**
7. Press `TAB` or `ALT-I` to move to the **IP Address** field.
8. Type in the static IP address for this network interface, I.E. `192.168.50.4`.
9. Press `TAB` or `ALT-S` to move to the **Subnet Mask** field.
10. Type in the subnet mask for this network interface, I.E. `255.255.255.0`. CIDR formats are also supported and can be typed in directly, I.E. `/24`.
11. Press `ALT-N` to continue back to the network Overview.
12. If you have multiple networks repeat steps 3 through 11 for any additional network interfaces needed
13. Press `ALT-S` to change to the Hostname/DNS configuration.
14. Press `ALT-T` or `TAB` to move to the **Static Hostname** field.
15. Type in the server name for this server, I.E. `vicibox-docs`
16. Press `ALT-1` or `TAB` to move to the **Name Server 1** field.
17. Type in the primary DNS server IP, I.E. `208.67.222.222`.
18. Press `ALT-2` or `TAB` to move to the the **Name Server 2** field.
19. Type in the secondary DNS server IP, I.E. `208.67.220.220`.
20. If you have a tertiary DNS server you can add it in the **Name Server 3** field.

21. Press ALT-R to change to the Routing configuration.
22. You will likely receive a notification about adapting the network configuration for the new hostname. Press ALT-Y to make sure **Yes** is selected and then press ENTER.
23. Press ALT-D to add a gateway to the server. The **Default Route** option should be checked.
24. Press ALT-G or TAB to move to the **Gateway** field
25. Type in the default gateway to use for this server, I.E. `192.168.50.1`
26. Press ALT-O or TAB to select the **OK** button. You should see the newly added gateway listed as default
27. Press ALT-O or TAB to select the **OK** button to accept the network configuration and make changes. If you are connected via SSH you might be disconnected during this process and will need to connect to the new static IP in the next step.
28. Before continuing it is necessary to log out and back in as root for the hostname change to take full effect. In the below screenshots the command prompt goes from **vicibox11:~ #** to **testBox1:~ #**.
29. At this point the network should be connected. Verify by pinging some hosts, I.E. `ping -4 google.com`.
30. Press CTRL-C to cancel the ping.

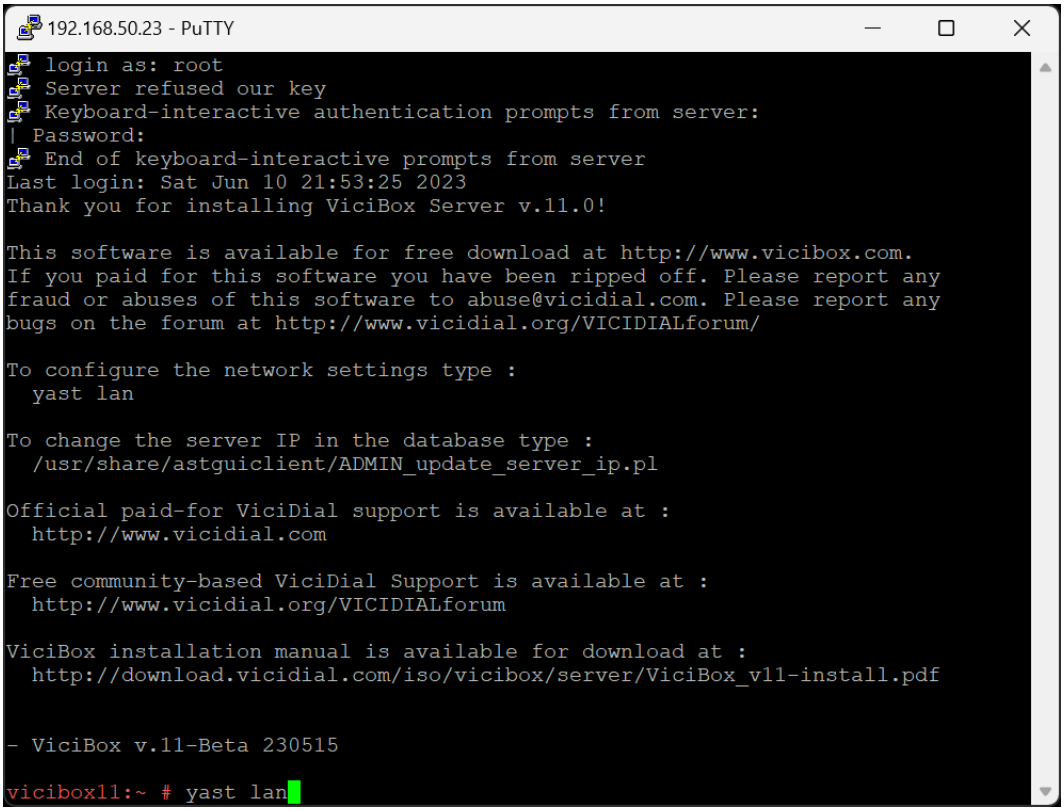
    If only certain aspects of the network need to be modified, for instance changing the hostname or DNS servers, then only the instructions related to that setting need to be ran.

    For Example, to change the hostname

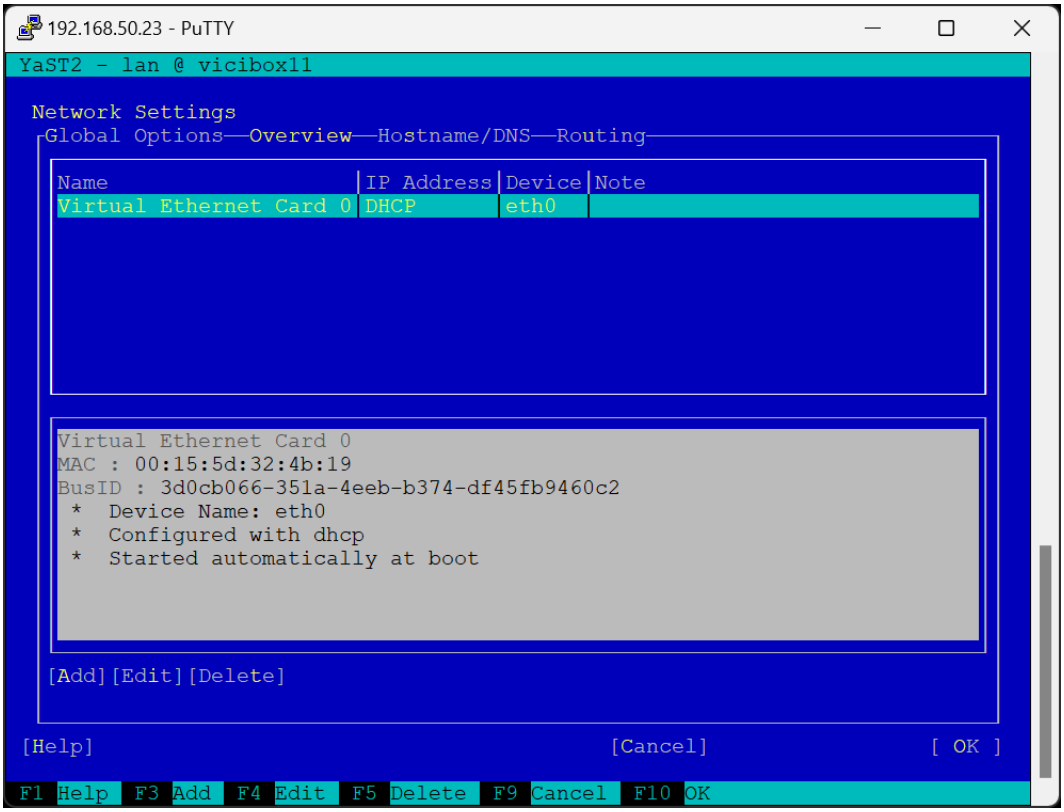
    1. If not already, login as the `root` user to get to the # command prompt.
    2. Type `yast lan` to start the network configuration.
    3. Press ALT-S to change to the Hostname/DNS configuration.
    4. Press ALT-T or TAB to move to the **Static Hostname** field.
    5. Type in the server name for this server, I.E. `vicibox-docs`.
    6. You will likely receive a notification about adapting the network configuration for the new hostname. Press ALT-Y to make sure **Yes** is selected and then press ENTER.
    7. Press ALT-O or TAB to select the **OK** button to accept the network configuration and make changes.
    8. Before continuing with the rest of the setup it is necessary to log out and back in as root for the hostname change to take effect on the command line. In the below screenshots the command prompt goes from **vicibox11:~ #** to **testBox1:~ #**

Screenshots

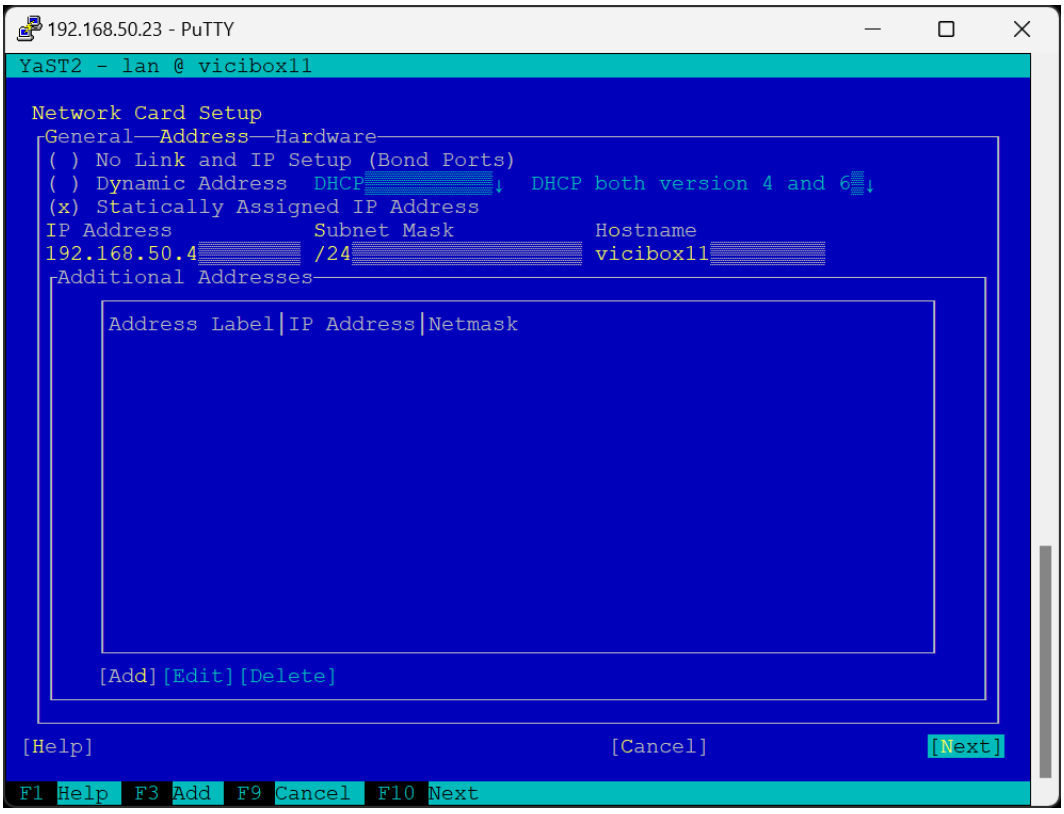
Run yast lan



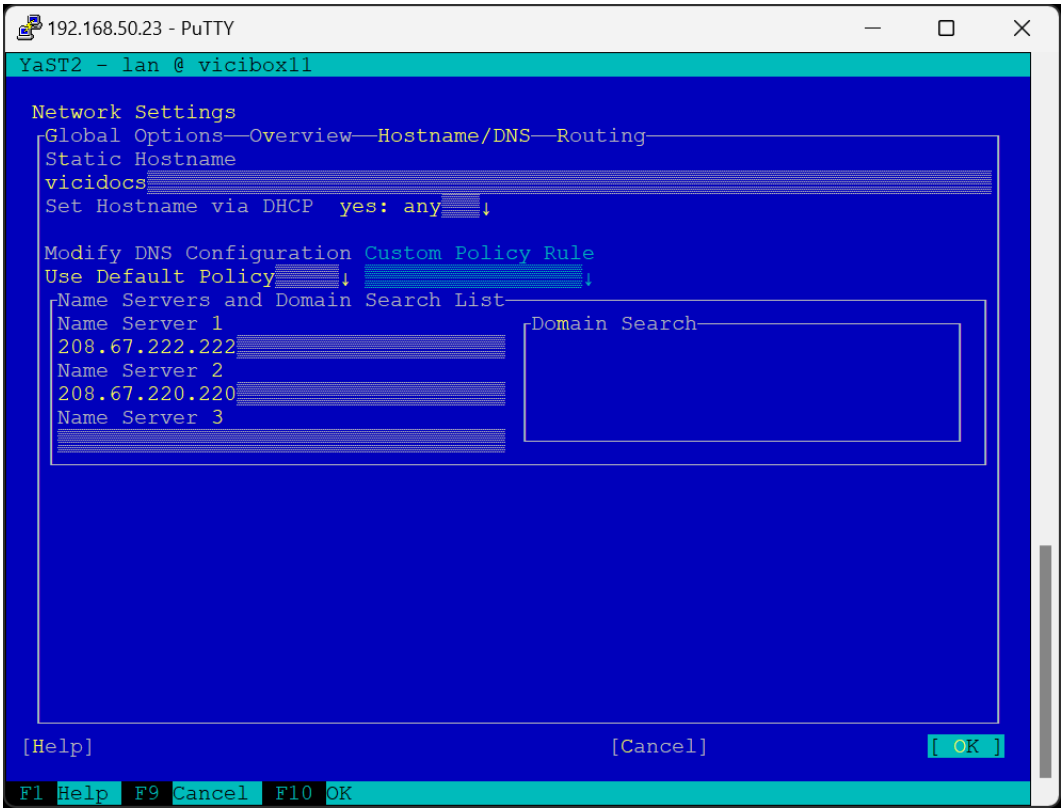
Select network interface



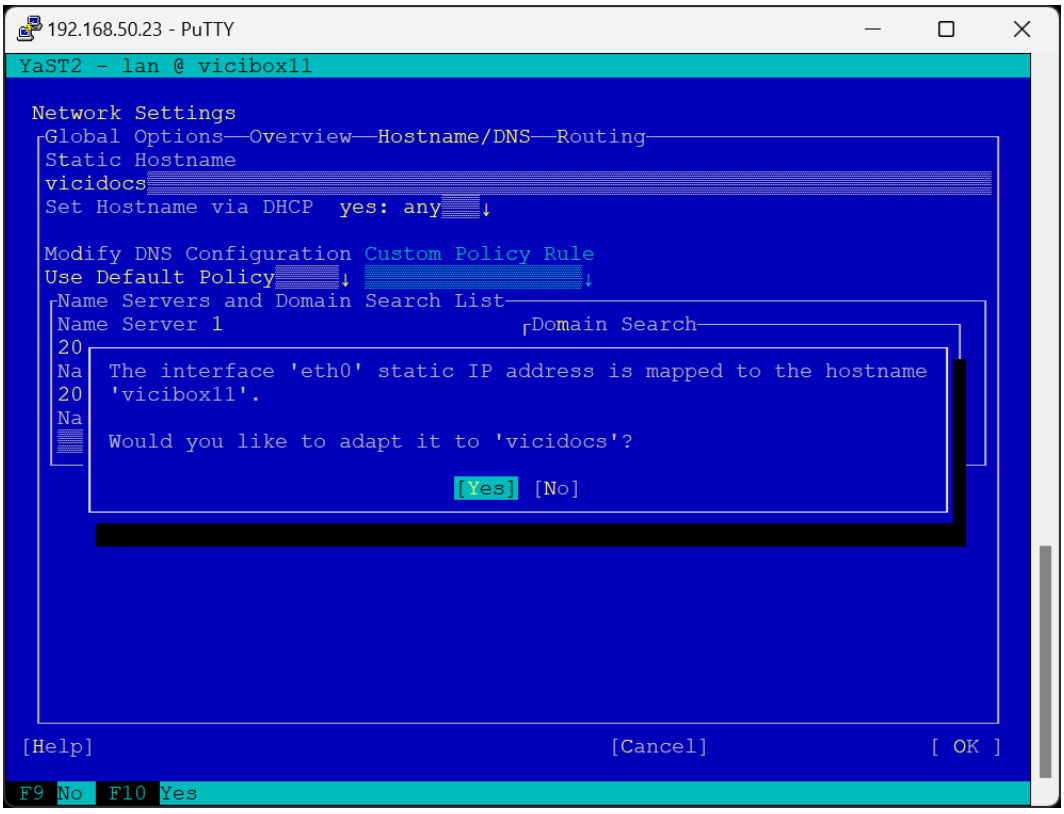
Assign static IP



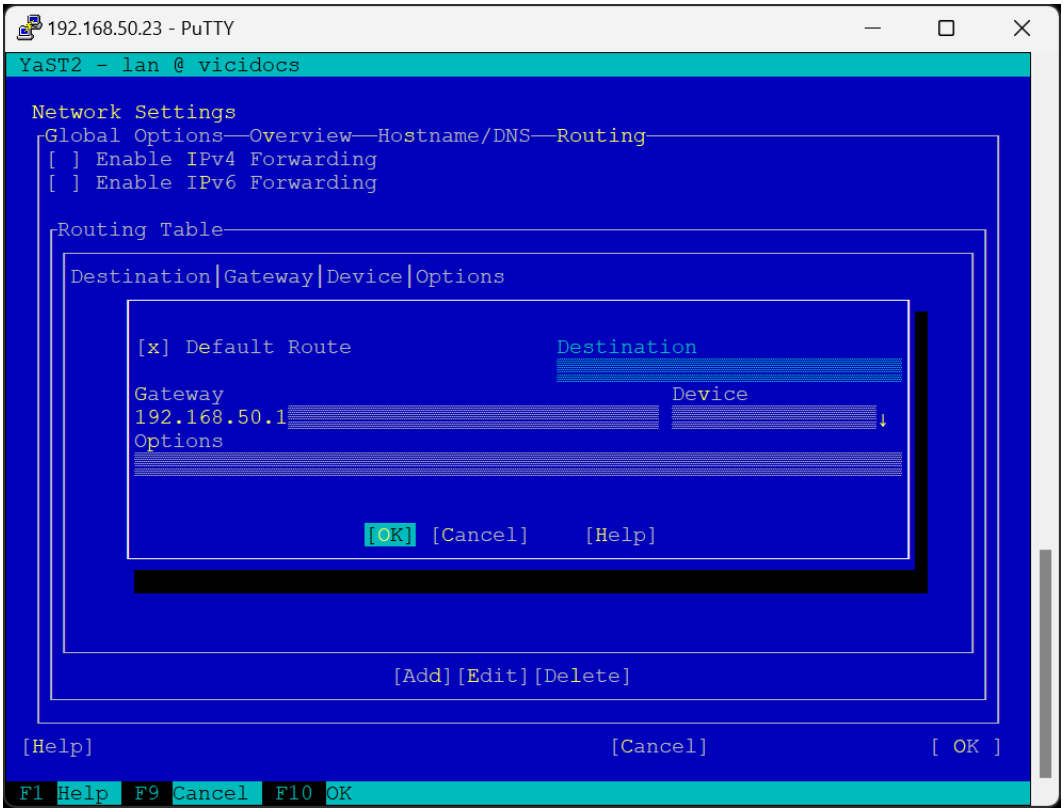
Configure DNS



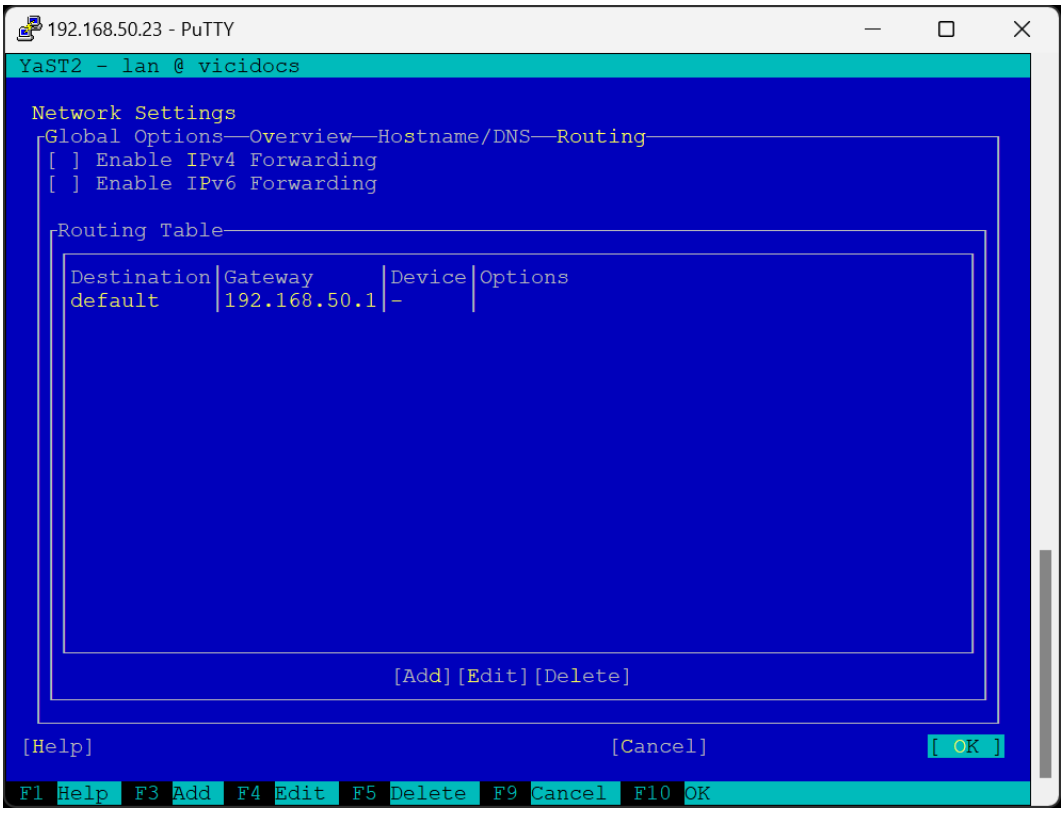
Accept hostname change



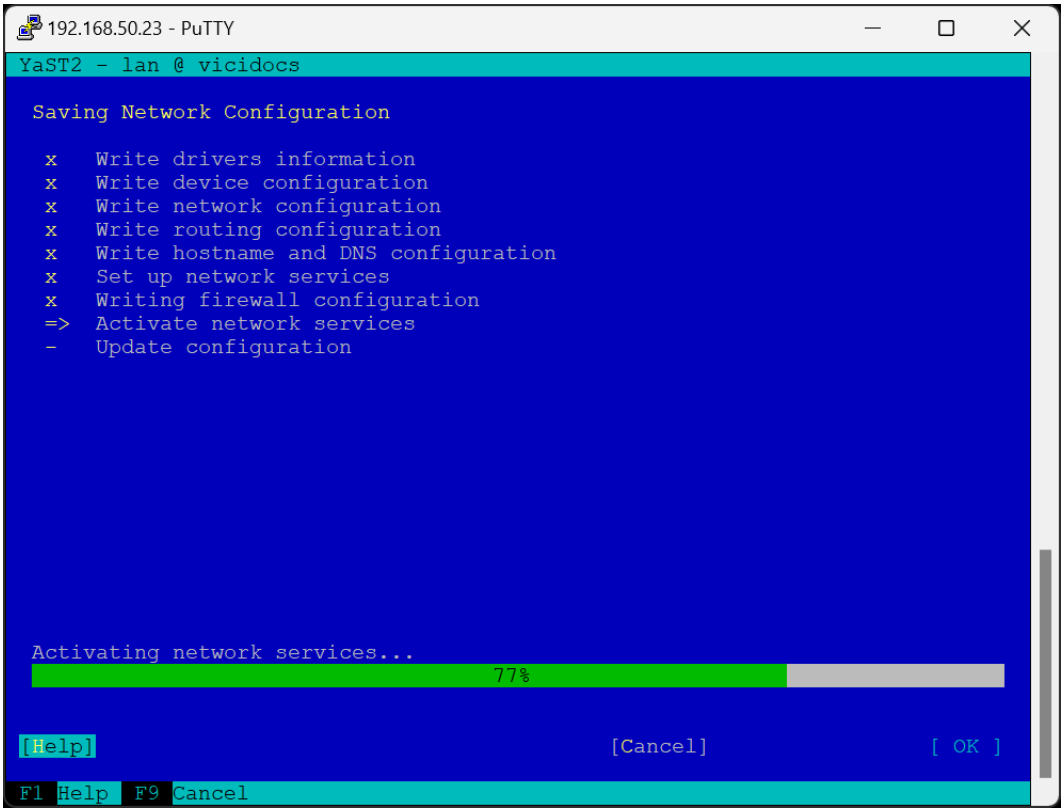
Add a Default Route



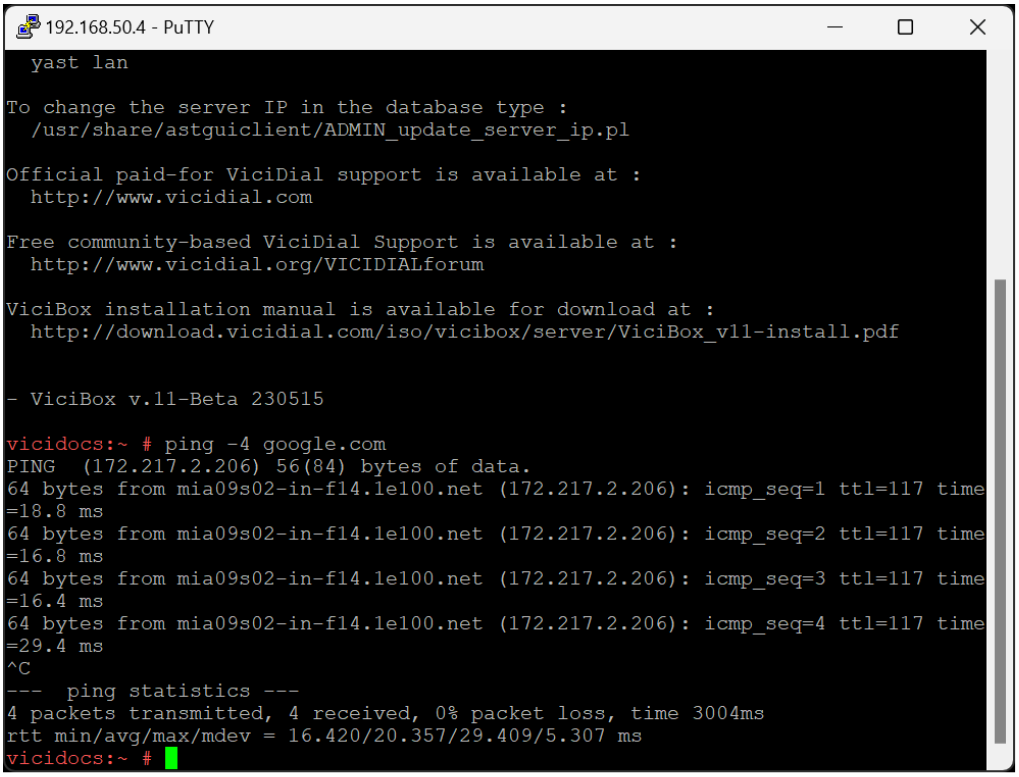
Single Default Route



Save changes



Verify connectivity and hostname change



2.3.2 Install Updates

While not required, it is *highly* recommended to install updates. This will update the ViciBox installer used in phase 2 as well as any new bug fixes or security updates. Internet connectivity is required to install updates. If the server is used in a secured network without internet access, updates can be skipped. It's still recommended to at least install updates when the OS is first installed prior to securing the server.

Installing Updates

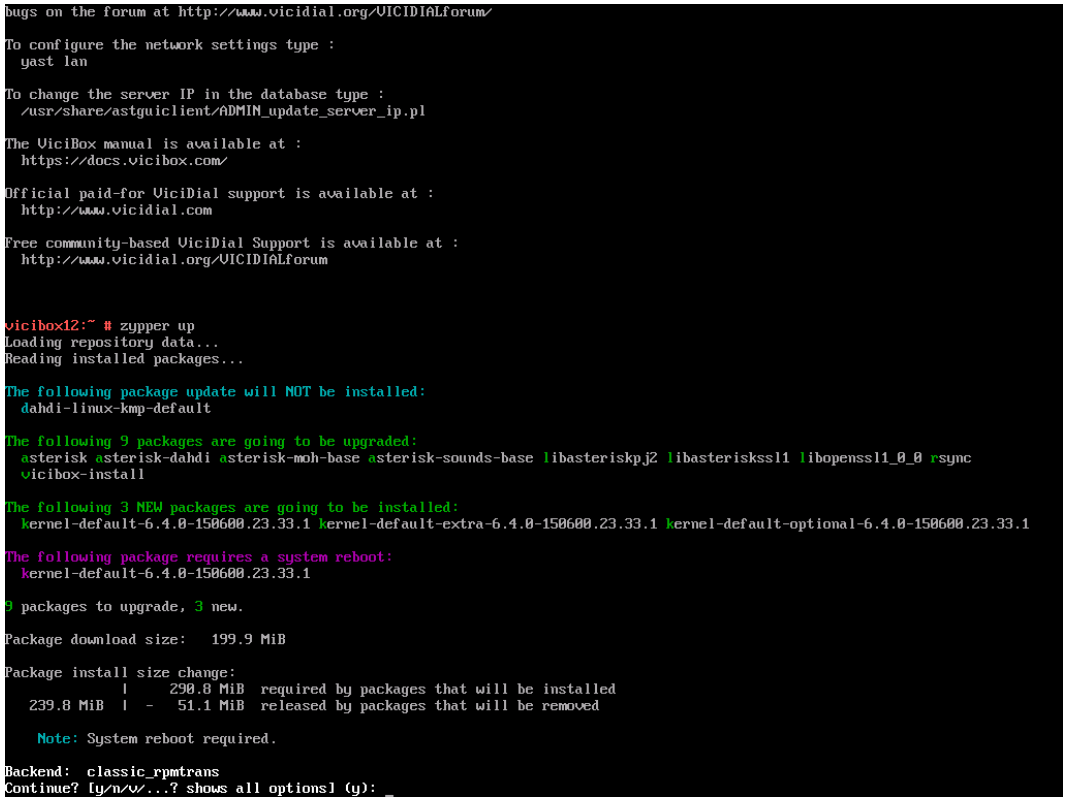
1. If not already, login as the `root` user to get to the # command prompt.
2. Type `zypper up` and press `ENTER` to start the update process.
3. A list of updates and a summary of them will be shown. Type `Y` and press `ENTER` to start downloading and installing updates.
4. Occasionally an update will ask if you want to view it's update notice. Press `ENTER` to continue if this happens.
5. While not strictly necessary, it's advised to reboot the server at this time. Type `reboot` and press `ENTER` to reboot the server.

Some alternative commands for `zypper up` is `zypper inr` and `zypper dup`. The `zypper inr` variant installs recommended packages most likely specific for the hardware or host. The `zypper dup` one installs packages that require repository changes like when adding a new repository.

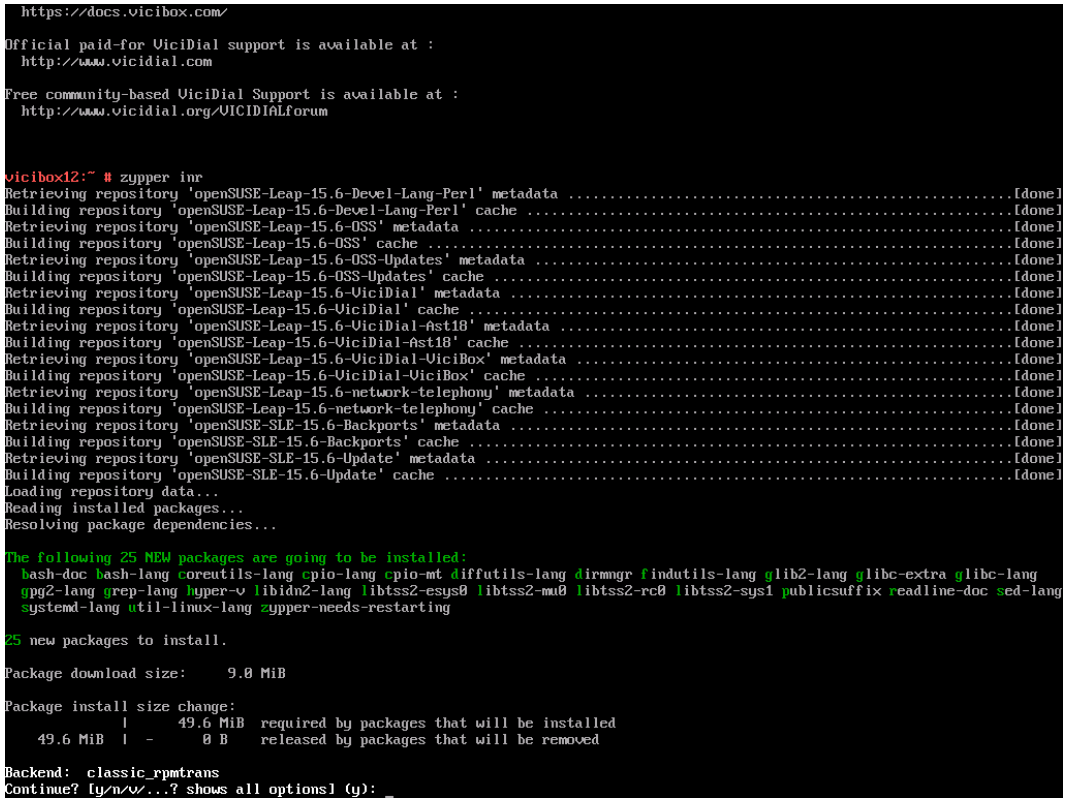
Note: It's not unusual for there to be up to 300 megs of updates depending on how old the system is. This can take a while to download and install depending upon the internet connection speed.

Screenshots

Installing normal updates



Installing recommended updates



2.3.3 RAID Setup

These instructions only apply if the *MultiDevice ISO* installation media was used. If the two drives are not the exact same size, then the smaller drive must be the drive selected during installation. There is no way to add a second drive to a RAID array if it's not at least the same size or bigger than the first drive.

> **Warning:** MD RAID setup can be temperamental. If there are any problems during the installation it's recommended to wipe all drives and start over. That can be done with wipefs, I.E. `wipefs -fa /dev/sda` or `wipefs -fa /dev/nvme0`, prior to installing.

Setup Instructions

1. If not already, login as the `root` user to get to the # command prompt.
2. Type `vicibox-mdraid1` and press `ENTER` to start the setup process.
3. If there are any orphaned RAID arrays, they will be shown. To remove them press `Y` and then `ENTER`. This will destroy the data on these drives.
4. If this is not the first time running the script, a summary of the current RAID arrays will be shown.
5. If there are any suitable target drives in the system, they will be shown. Select the appropriate drive number from the list and press `ENTER`.
6. A confirmation prompt will be shown to confirm the destruction of the target drive. Press `ENTER` to confirm the target drive.

7. The drive will be partitioned and added to the RAID arrays. A summary of the arrays will be shown when complete.
8. To check the status of the MD RAID arrays, type `cat /proc/mdstat` and press `ENTER`. md1 is the swap array and md2 is the root array.
9. While not strictly necessary, it's advised to reboot the server at this time. Type `reboot` and press `ENTER` to reboot the server.

For more screenshots of these steps, see *RAID Specific*.

Filesystem Layout

Table 2: System Mounts

Mount	MD Array
/ (root)	/dev/md2
swap	/dev/md1

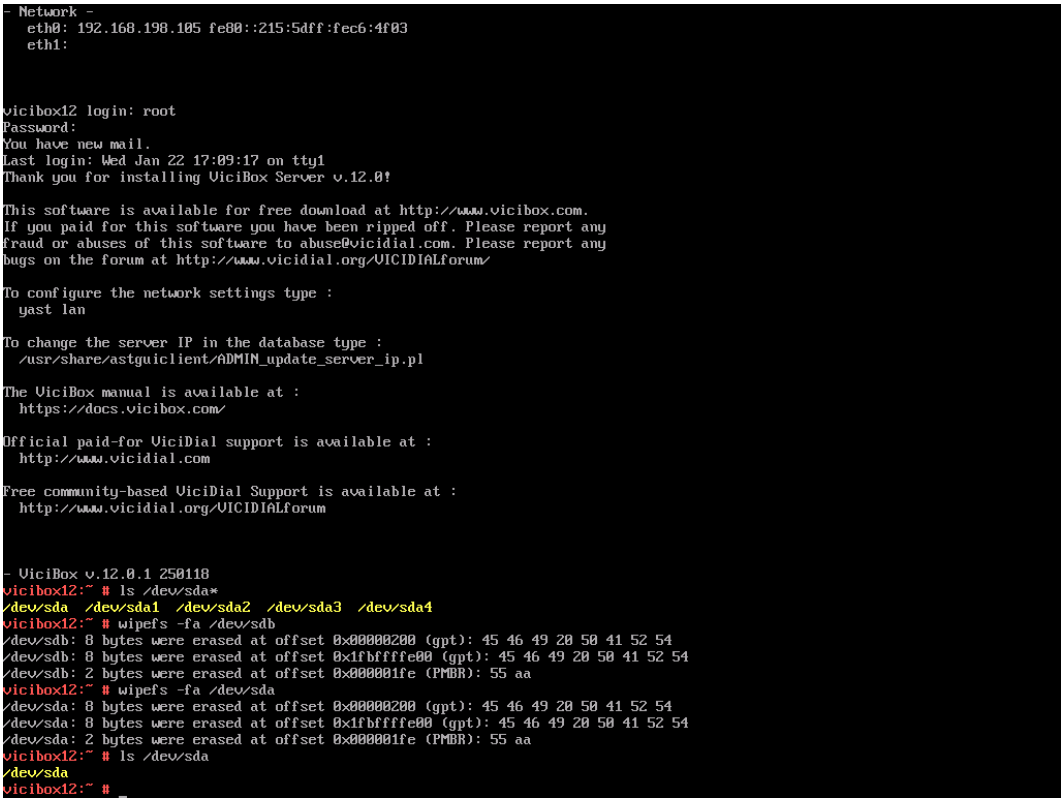
Table 3: Drive Layout

MD Array	Partition
/dev/md2	/dev/sda4 or /dev/nvme0n1p4
/dev/md1	/dev/sda3 or /dev/nvme0n1p3

Note: When initially installed, the swap MD array is not setup. The drive layout shows only a single drive, but you can replace sda with sdb or nvme0 with nvme1 for the second drive that gets added to the array. /dev/md0 is not used by ViciBox and available for end users to use as they see fit.

Screenshots

Use wipefs to clear target drives



2.4 Phase 2

ViciDial is installed through the `vicibox-install` command. This command will ask a series of questions in order to determine how to install. A ViciDial cluster will use this command when setting up new servers.

An alternative to this is the mostly automated *Express Box* install. This actually runs the same program but with pre-defined settings. It is an all-in-one approach to ViciDial that can later be turned into a cluster if needed.

ViciDial is broken down into three main server roles with an optional fourth role:

- Database server with MariaDB
- Web server with Apache
- Telephony server with Asterisk
- Archive server with VSFTPd (Optional)

Once installed, ViciDial and the server's configuration will be tied to the current LAN and WAN IP. If the network environment changes, then those changes will need to be made in ViciDial and the server to match. This usually happens when migrating to a new ISP or moving to a different location.

Dimensioning, specifications, and clustering examples can be found in the *Hardware* section.

Attention: It is highly recommended to *Phase 2* before continuing.

2.4.1 Express Box

With `vicibox-express` all three ViciDial roles will be installed onto a single server. This is best suited for contact centers with fewer than 20 agents or as a proof of concept. It is the recommended starting point for first-time users of ViciBox as it's the easiest option.

Different roles can later be split off and moved to different servers. After all, an express box is just all three roles running on a single server. These roles can be moved to different servers on the network as needs change.

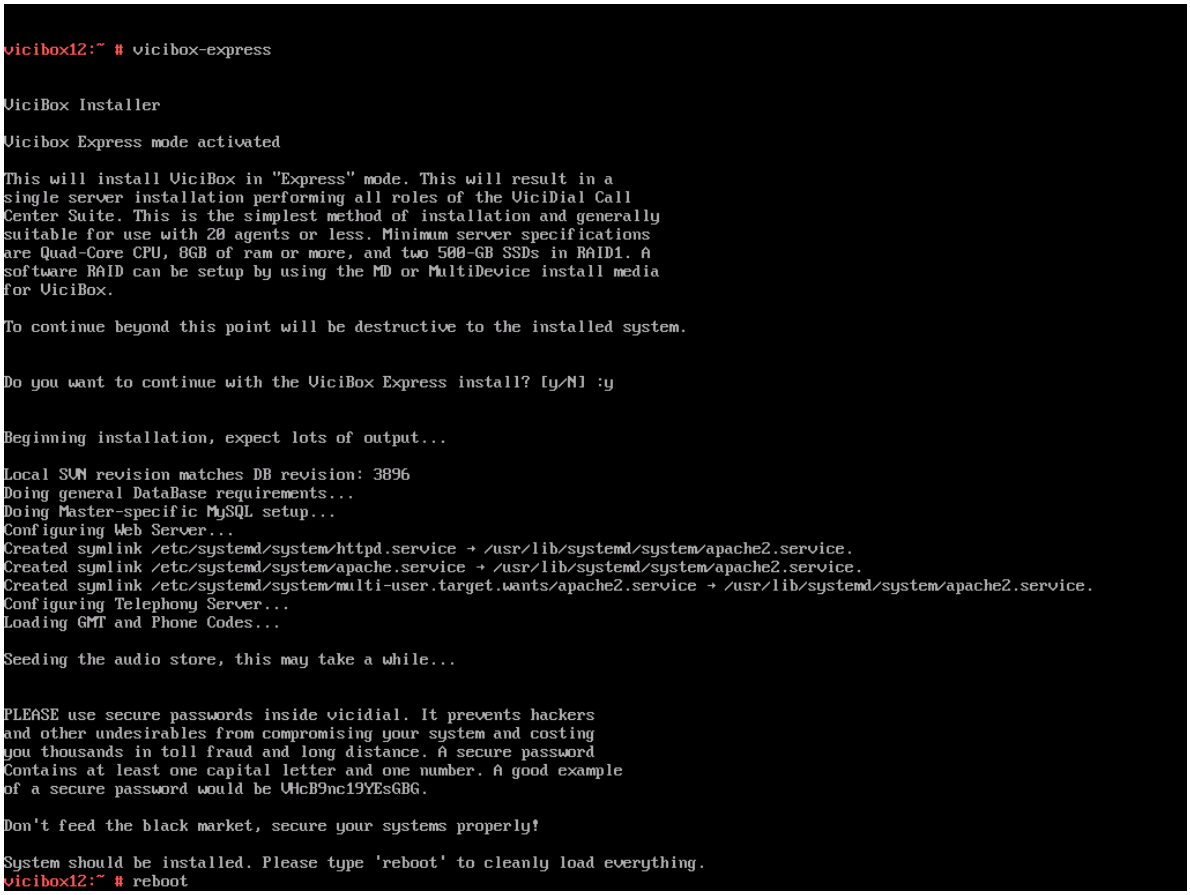
Installation Steps

1. If not already, login as the `root` user to get to the **#** command prompt.
2. Type `vicibox-express` and press `ENTER`.
3. Type `Y` and press `ENTER` to start the installation.
4. Once you are back at the **#** command prompt, the installation is complete. Type `reboot` and press `ENTER`.
5. Once the reboot is complete, log back in as root to get to the **#** command prompt.
6. Type `screen -ls` and press `ENTER`. While it might take upwards of 5 minutes, eventually there should be **11 Sockets in /run/screens/S-root** shown before returning to the **#** command prompt
7. Type `asterisk -r` and press `ENTER` to connect to the Asterisk console. There should be different processes like **sendcron** logging on and off.
8. Type `quit` and press `ENTER` to exit back to the **#** command prompt.
9. In a web browser, type in the servers IP address, I.E. `192.168.50.4`, and press `ENTER`
10. Click on **Administration** and login. The default **Username** is `6666` with **Password** `1234`. Upon login you should see the ViciDial Initial Setup screen.

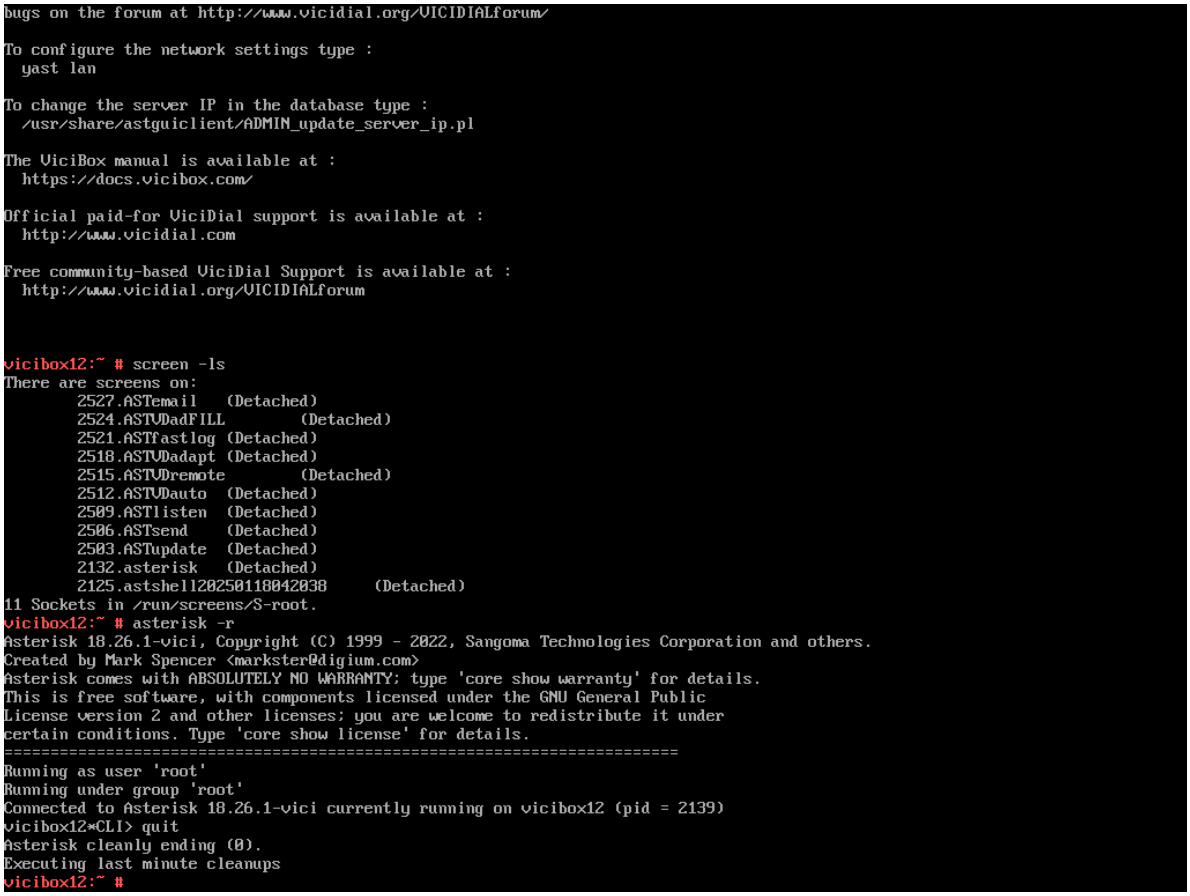
ViciDial is now successfully installed and running. It's recommended to continue with the initial ViciDial setup and then give the **6666** user all Admin permissions.

Screenshots

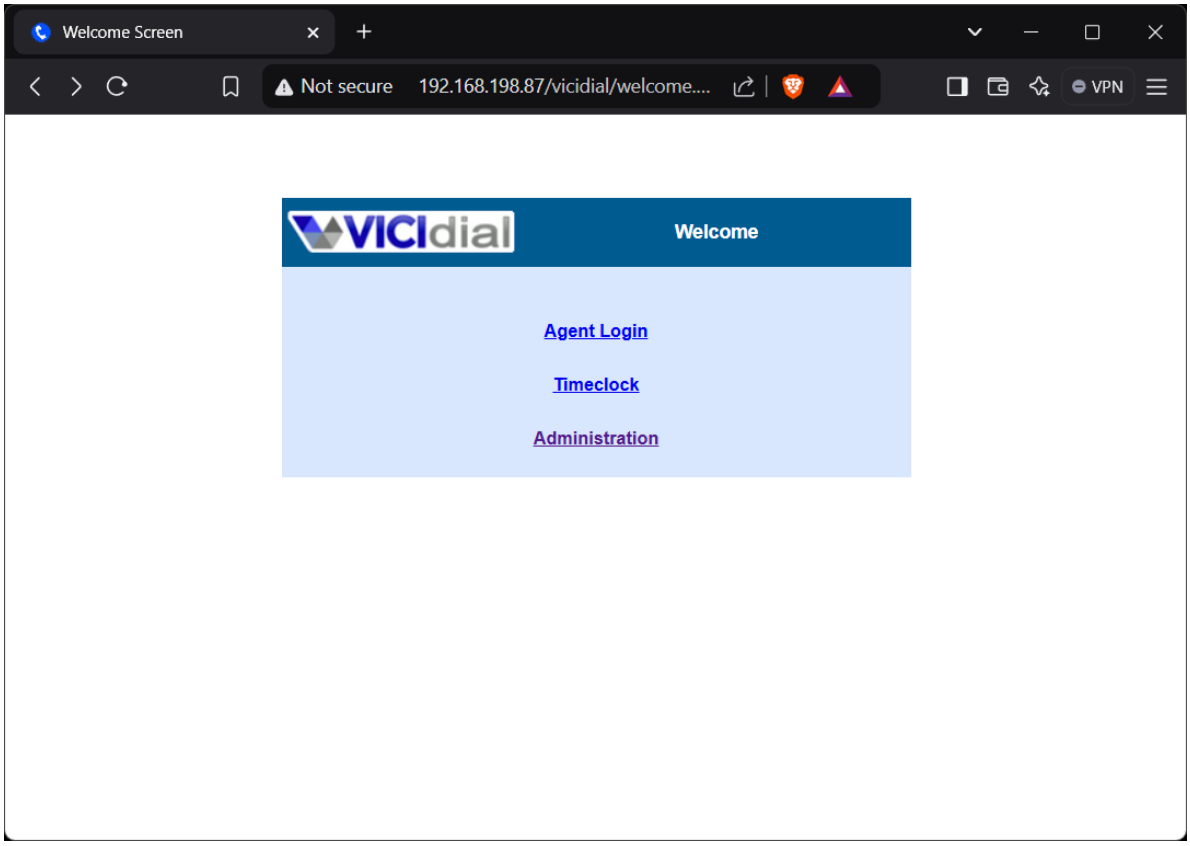
Run vicibox-express and reboot



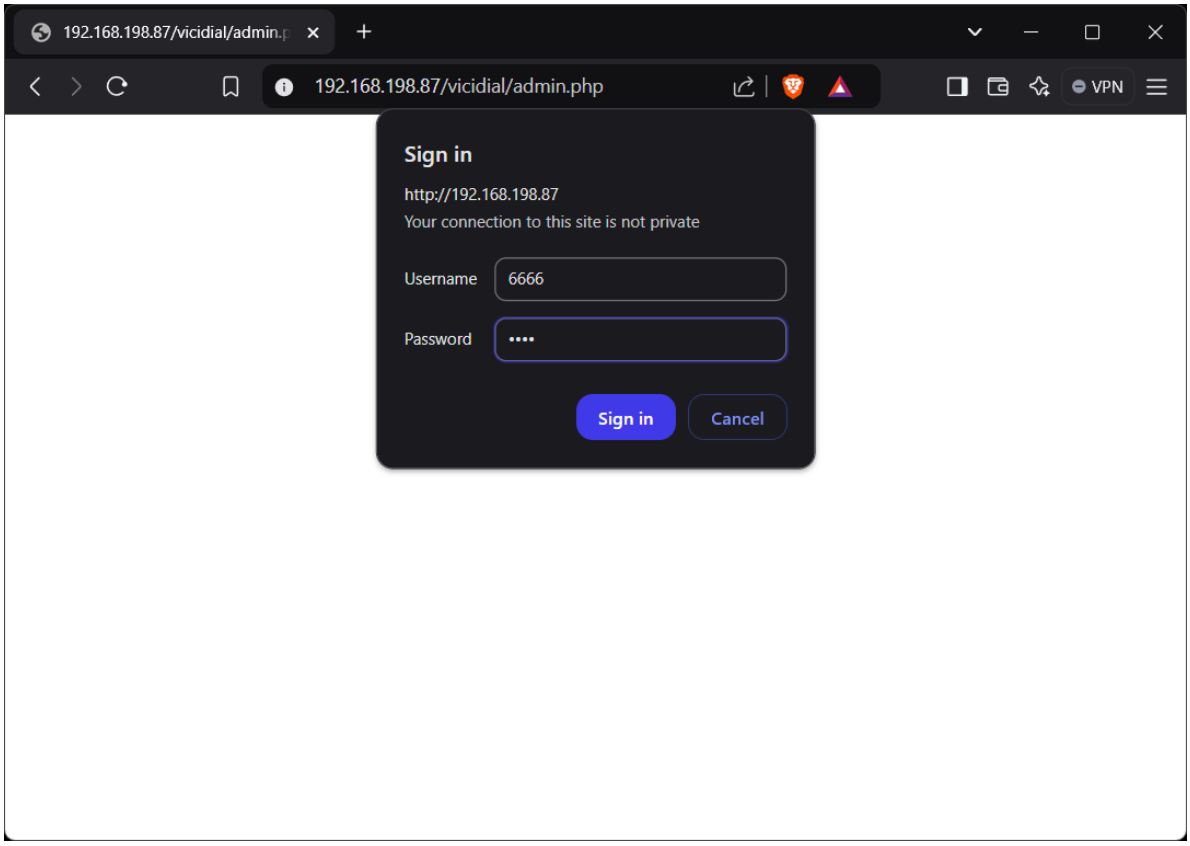
Verify that ViciDial started (may take up to 5 minutes)



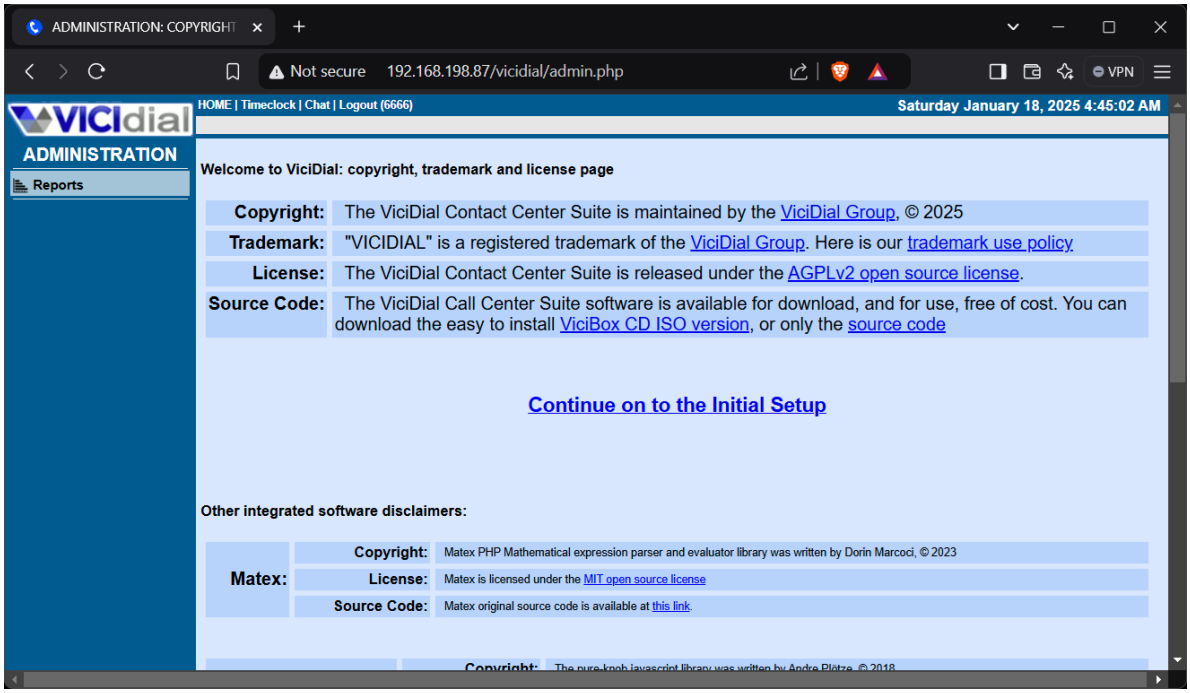
Verify that the web interface is working



Login as default user (password is 1234)



Continue with the ViciDial setup



2.4.2 Cluster

ViciDial Setup Order

- Database server
- Web server
- Telephony server

All clusters start with the primary Database server since everything starts there. Afterwards, the web server is installed to provide services needed by the Telephony server. Lastly, the Telephony server is installed and will set up portions of ViciDial needed by other servers. Any additional servers can be set up after these three are working together as a cluster.

The hostname for each server in a cluster is used as that server's name in the ViciDial database. Because of this, each server must have a unique hostname. The recommended naming convention is to use 'DBX', 'webX', and 'dialX' as the prefix for the hostname, e.g. 'DB1', 'web1', 'dial1', etc. This designates the server's role as well as which one it is if there are multiple of that type in the cluster. How to change the hostname can be found in the *Cluster* section.

Tip: While it might sound good to use Greek gods, Disney characters, or Transformers for the hostname of your servers, don't. Being told that Optimus Prime went down but Megatron is handling it now is just confusing. And yes, that is based on a true story of an 11-server cluster. Optimus Prime was the primary database, Megatron was the replicated backup. Bumblebee was the web server and Starscream was their primary telephony server. No numbers either, so the second telephony server was Skywarp I think. Don't be that guy.

Planning

With `vicibox-install` the different roles of ViciDial can be run on multiple servers. These servers can then connect with each other across the network to scale. By doing this, a ViciDial Cluster can scale up to 500 agents.

The examples in this section will be for the three initial servers needed to make a ViciDial Cluster. This is the starting point upon which any size cluster can be built. To add more servers, just repeat the install as needed.

If there are only two servers available for a cluster, it is advised to have the Database and Web server role running on the more powerful of the two servers. To accomplish this, the Web server role would also be selected during the setup of the Database. Fun fact: if you were to select all 3 roles on the same server you would end up with an *Express Box*.

A ViciDial cluster can only have one primary Database server. The primary Database server is what all Web and Telephony servers will connect to. More information on the Database server role is available in the *Hardware* section.

Table 4: Cluster Information

Server	IP Address
DB1	192.168.50.4
web1	192.168.50.6
dial1	192.168.60.10

2.4.3 Database

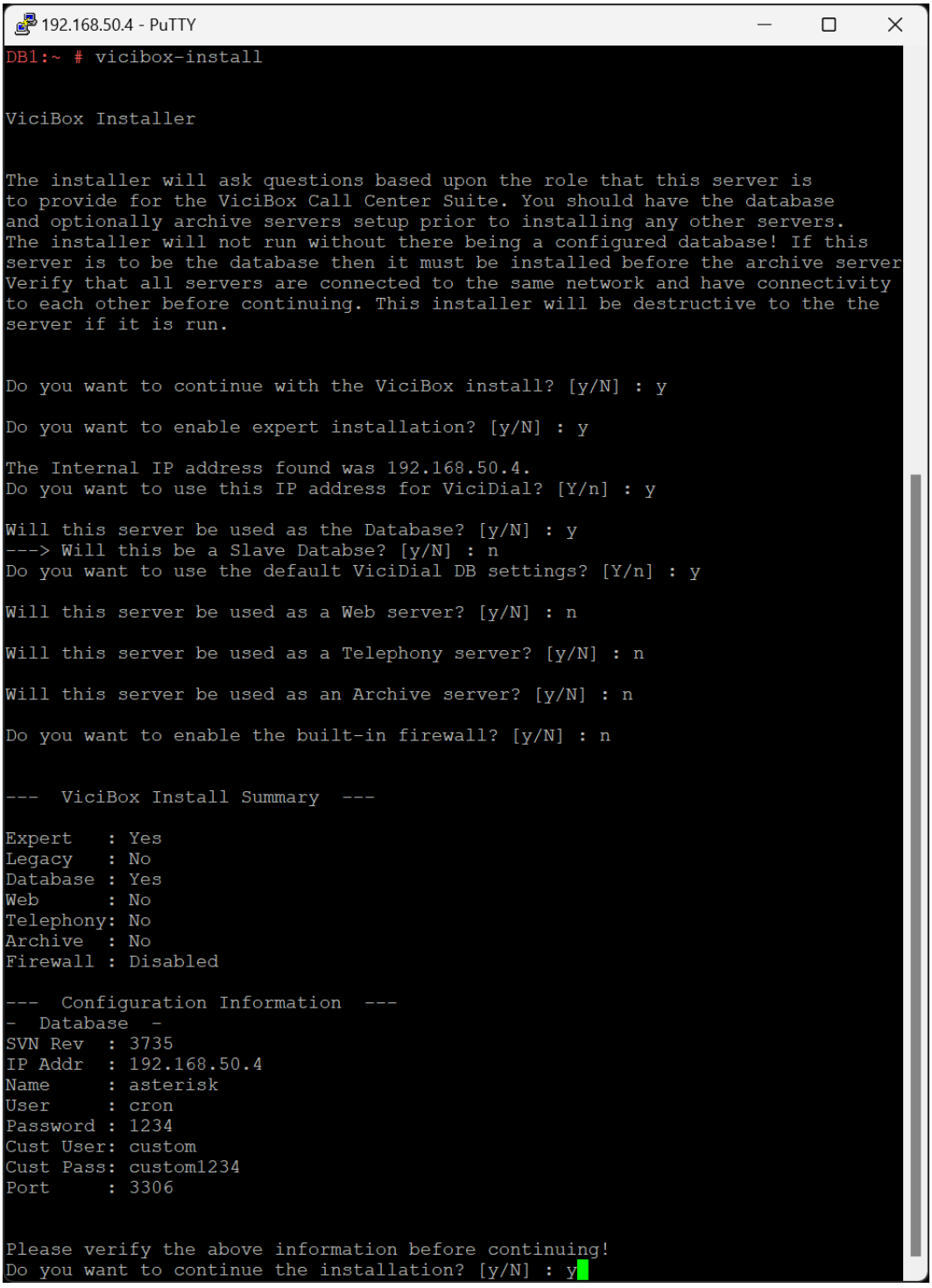
Follow these steps to install and configure the database server for a ViciDial cluster:

1. If not already, log in as the `root` user to get to the # command prompt.
2. Type `vicibox-install` and press `ENTER` to start the ViciBox installer.
3. Type `Y` and press `ENTER` at the **ViciBox install** prompt.
4. Type `Y` and press `ENTER` at the **expert installation** prompt.
5. The installer will attempt to find a LAN IP address to use for the cluster. If the IP shown is correct, type `Y` and press `ENTER`. If not, type `N` and press `ENTER` and follow the prompts.
6. Type `Y` and press `ENTER` at the **the Database** prompt.
7. Type `N` and press `ENTER` at the **Slave Database** prompt.
8. Type `Y` and press `ENTER` at the **DB settings** prompt. If you want to use different database settings, type `N` and press `ENTER` to follow those prompts.
9. Type `N` and press `ENTER` at the **Web server** prompt.
10. Type `N` and press `ENTER` at the **Telephony server** prompt.
11. Type `N` and press `ENTER` at the **Archive server** prompt.
12. Type `N` and press `ENTER` at the **built-in firewall** prompt.
13. A summary will be listed of all selected options. Type in `Y` and press `ENTER` to accept and install.
14. Type `reboot` and press `ENTER` to reboot and cleanly load vicidial.
15. Log in as the `root` user to get to the # command prompt.
16. Type `screen -ls` and press `ENTER` to show running screen sessions. There should be three listed like in the screenshot.

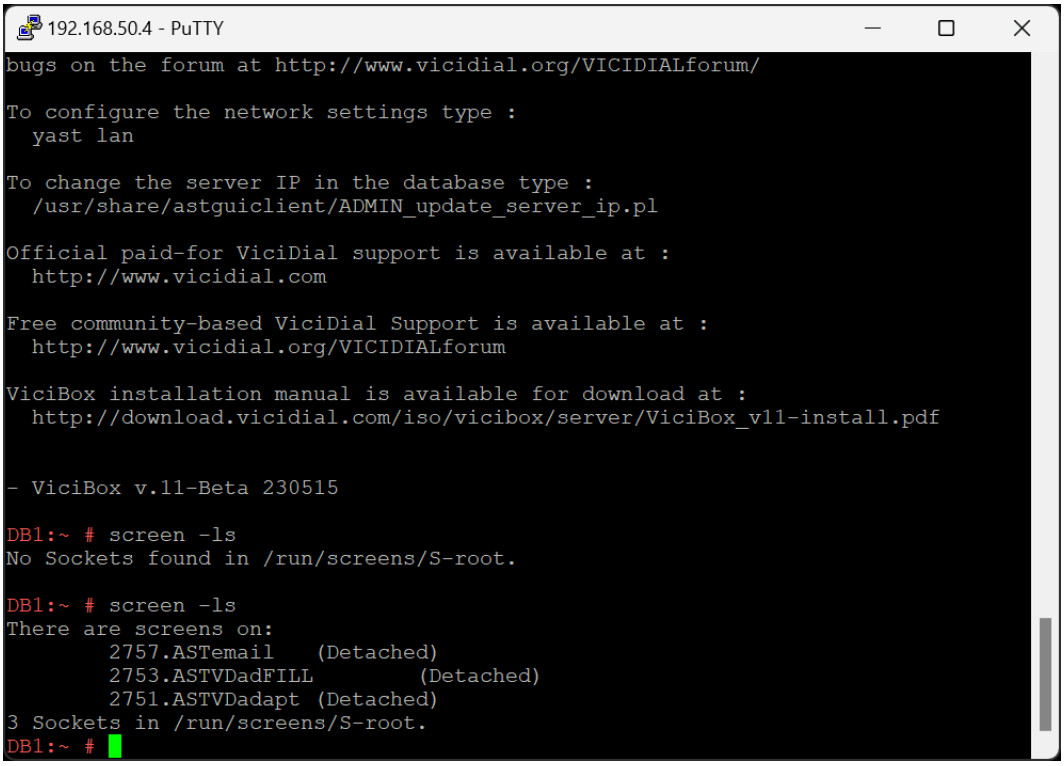
This will create an entry under *Admin* → *Servers* called **DB1**. Do not delete this entry as it's needed for ViciDial to function properly.

Screenshots

Install Database



Verify screen sessions



2.4.4 Web Server Setup

Follow these steps to install and configure the web server for a ViciDial cluster:

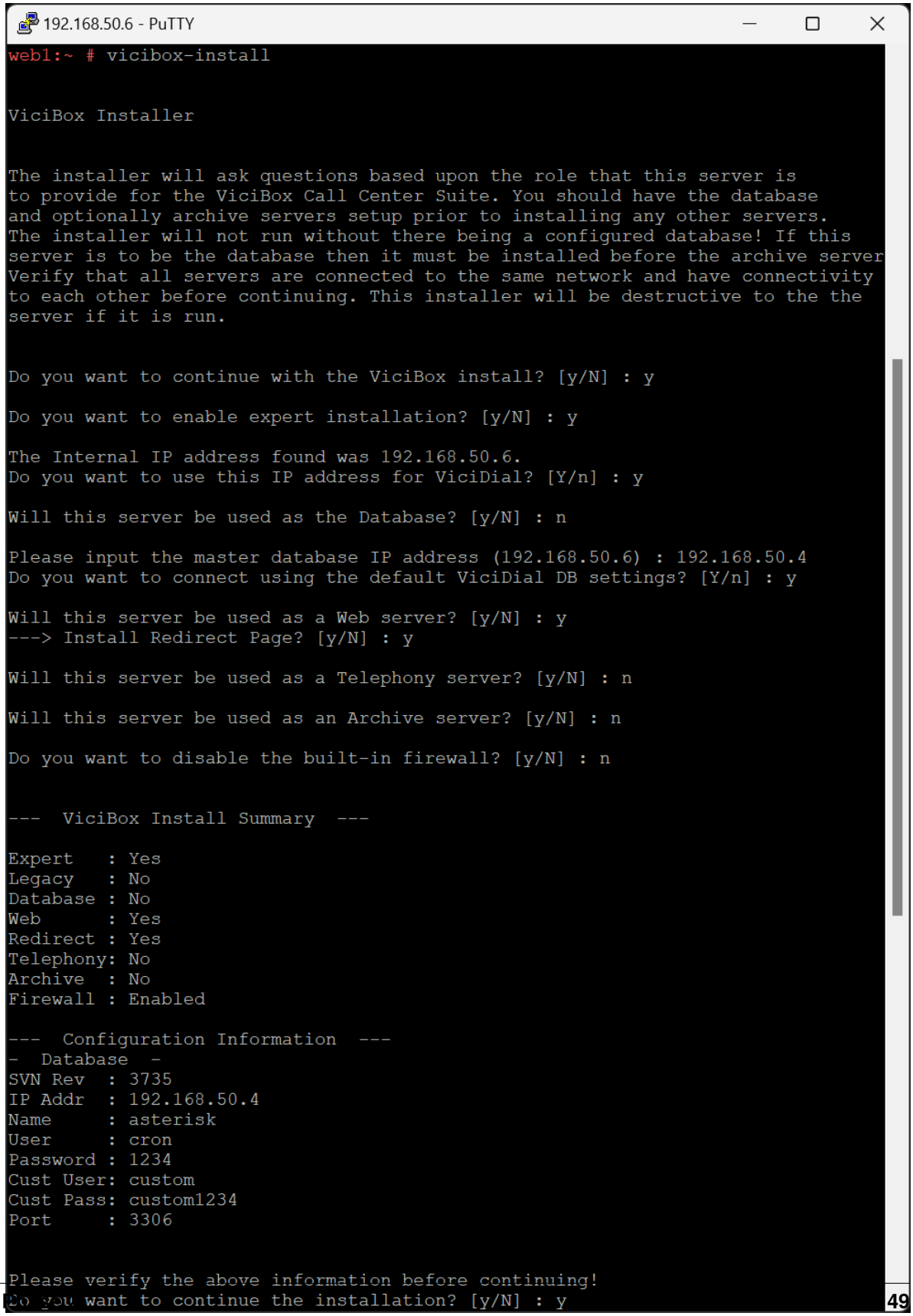
1. If not already, log in as the `root` user to get to the # command prompt.
2. Type `vicibox-install` and press `ENTER` to start the ViciBox installer.
3. Type `Y` and press `ENTER` at the **ViciBox install** prompt.
4. Type `Y` and press `ENTER` at the **expert installation** prompt.
5. The installer will attempt to find a LAN IP address to use for the cluster. If the IP shown is correct, type `Y` and press `ENTER`. If not, type `N` and press `ENTER` and follow the prompts.
6. Type `N` and press `ENTER` at the **the Database** prompt.
7. Type in the Database IP address and press `ENTER`, e.g. `192.168.50.4`. If the installer is unable to connect to the Database server it will error out. Correct any issues and run the installer again.
8. Type `Y` and press `ENTER` at the **Web server** prompt.
9. Type `Y` and press `ENTER` at the **Redirect Page** prompt.
10. Type `N` and press `ENTER` at the **Telephony server** prompt.
11. Type `N` and press `ENTER` at the **Archive server** prompt.
12. Type `N` and press `ENTER` at the **built-in firewall** prompt.
13. A summary will be listed of all selected options. Type in `Y` and press `ENTER` to accept and install.
14. Type `reboot` and press `ENTER` to reboot and cleanly load vicidial.
15. Once the server has rebooted, verify you can reach the web interface by going to the server's IP address in a browser, e.g. `192.168.50.6`, and press `ENTER`.

16. Click on **Administration** and log in with **Username** `6666` and **Password** `1234` to continue with the ViciDial Initial Setup.

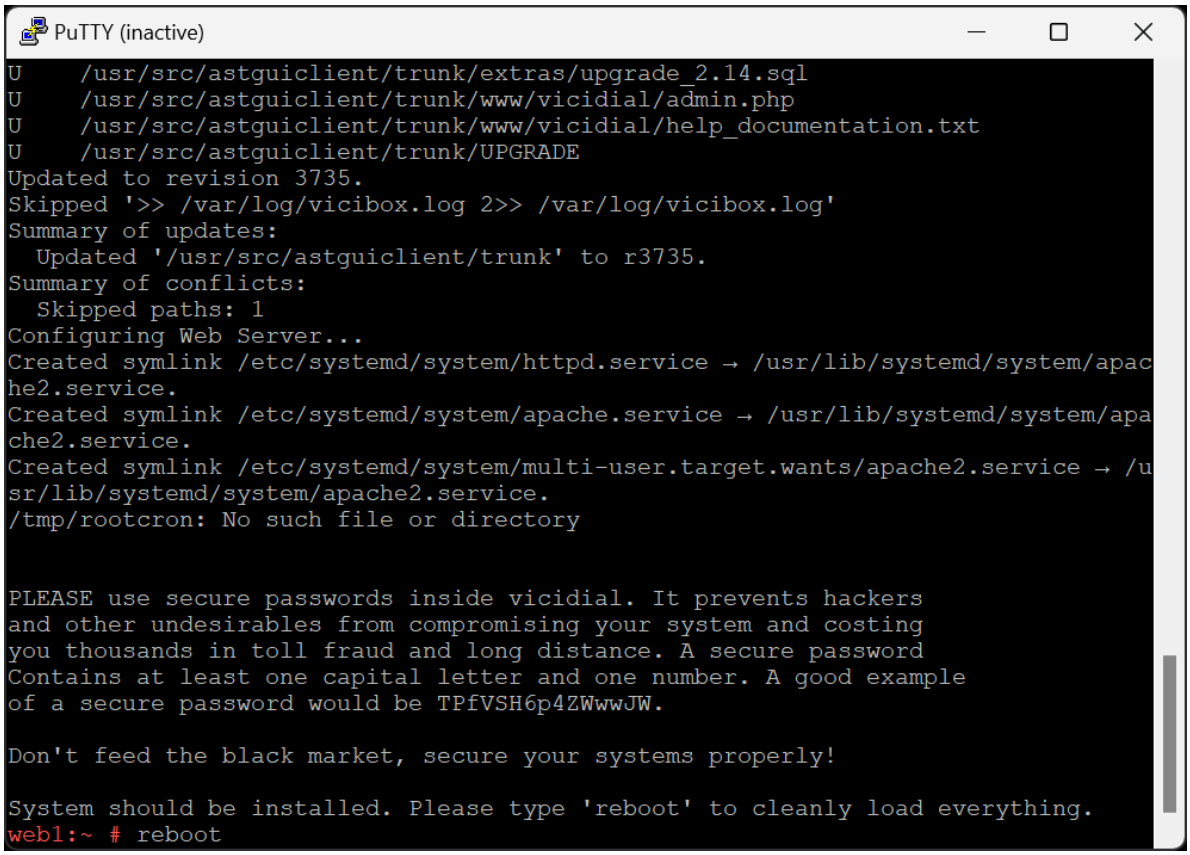
It is recommended to give the **6666** user all Admin permissions before continuing. If there are multiple web servers in the cluster, these instructions can be repeated on any additional servers.

Screenshots

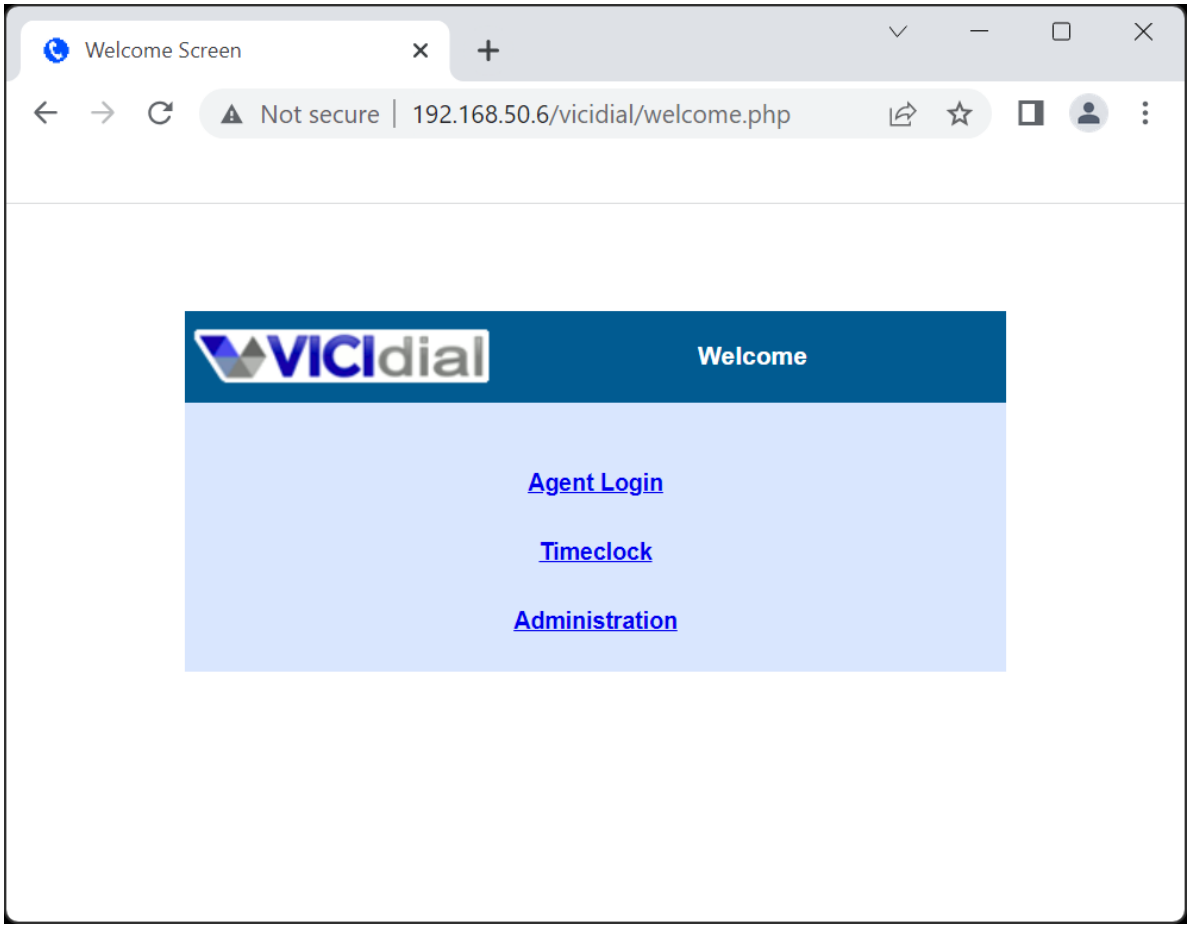
Install Web



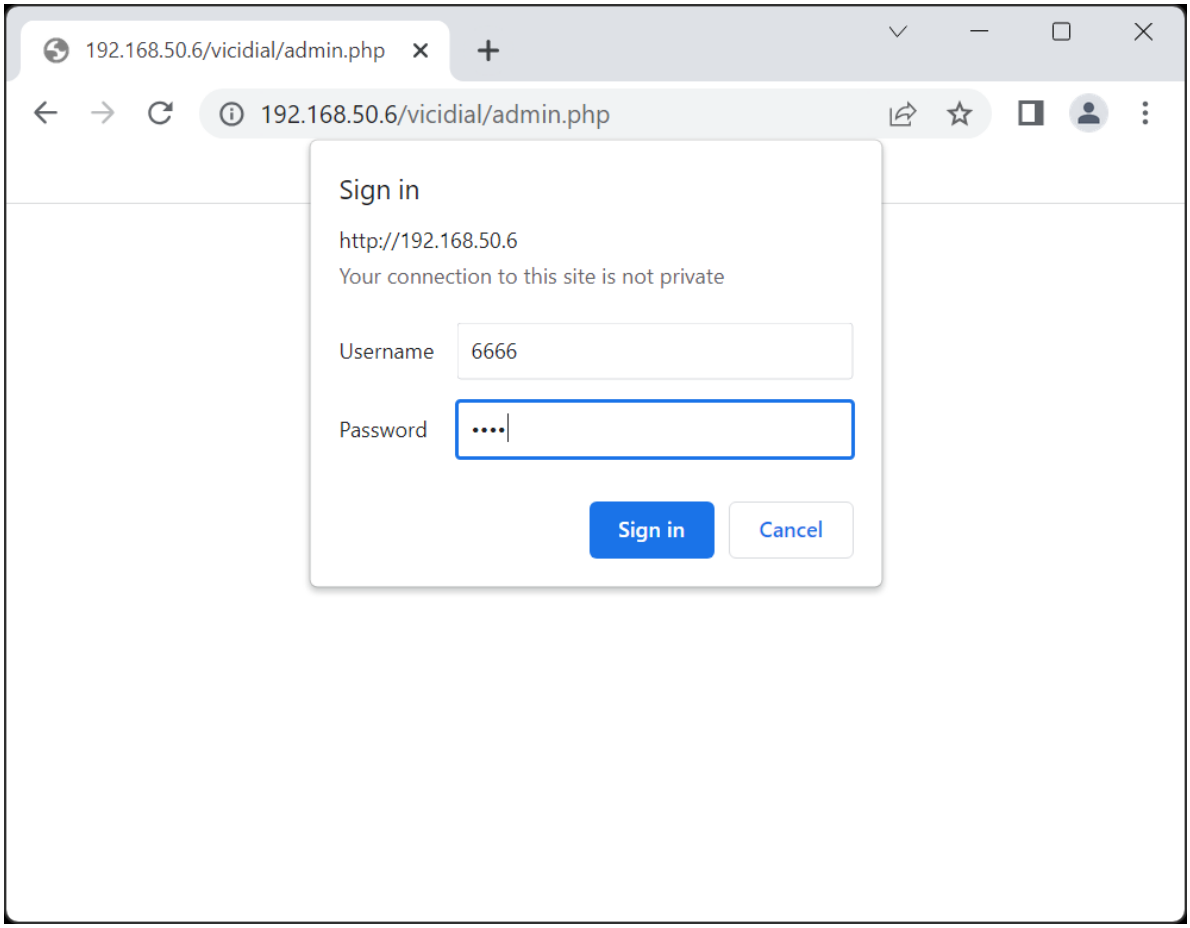
Reboot



Verify web interface



Login with default user



Continue to ViciDial Initial Setup

2.4.5 Telephony

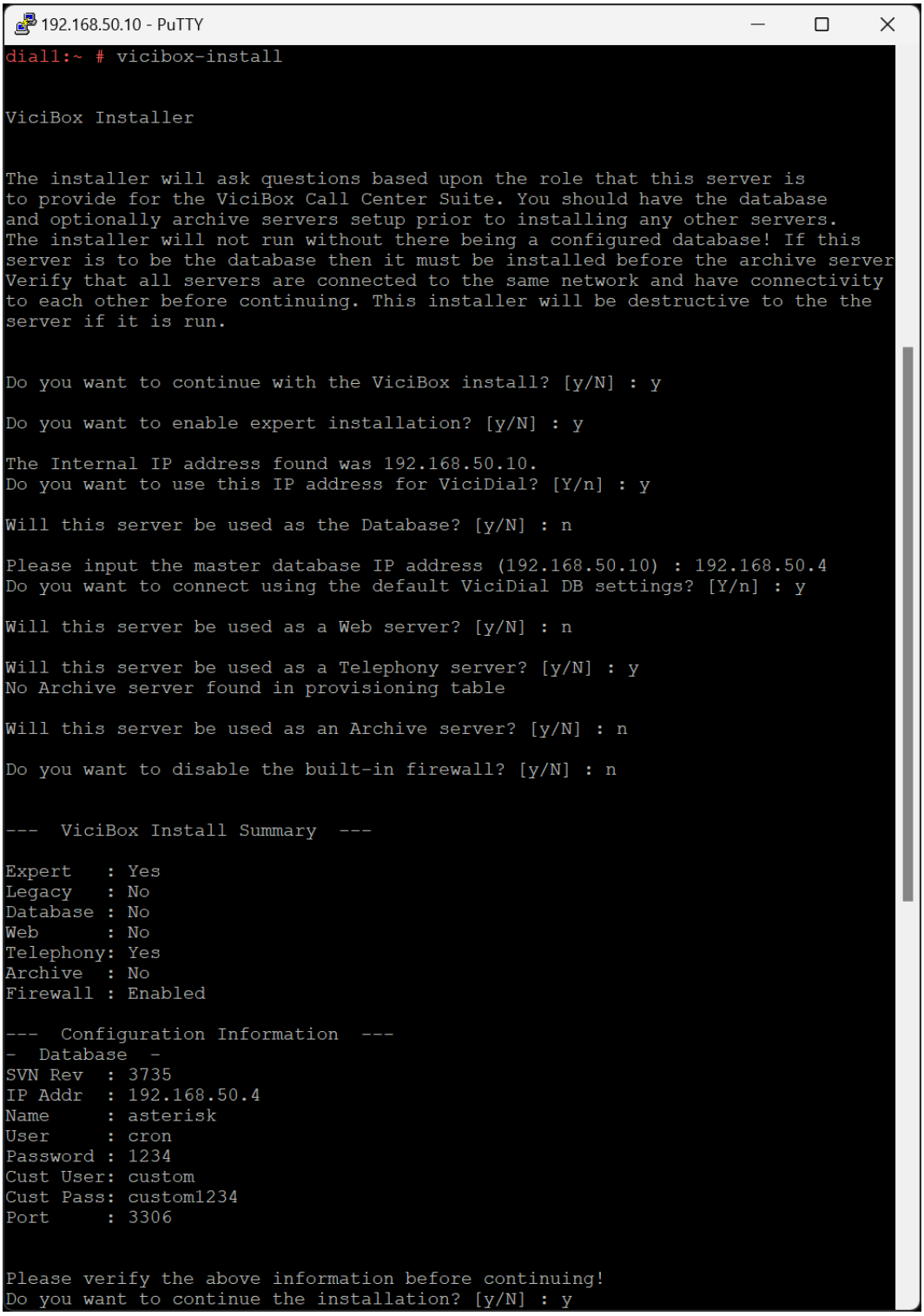
Follow these steps to install and configure the telephony server for a ViciDial cluster:

1. If not already, log in as the `root` user to get to the # command prompt.
2. Type `vicibox-install` and press `ENTER` to start the ViciBox installer.
3. Type `Y` and press `ENTER` at the **ViciBox install** prompt.
4. Type `Y` and press `ENTER` at the **expert installation** prompt.
5. The installer will attempt to find a LAN IP address to use for the cluster. If the IP shown is correct, type `Y` and press `ENTER`. If not, type `N` and press `ENTER` and follow the prompts.
6. Type `N` and press `ENTER` at the **the Database** prompt.
7. Type in the Database IP address and press `ENTER`, e.g. `192.168.50.4`. If the installer is unable to connect to the Database server it will error out. Correct any issues and run the installer again.
8. Type `N` and press `ENTER` at the **Web server** prompt.
9. Type `Y` and press `ENTER` at the **Telephony server** prompt.
10. (Follow any additional prompts as needed.)
11. Type `N` and press `ENTER` at the **Archive server** prompt.
12. Type `N` and press `ENTER` at the **built-in firewall** prompt.
13. A summary will be listed of all selected options. Type in `Y` and press `ENTER` to accept and install.
14. Type `reboot` and press `ENTER` to reboot and cleanly load ViciDial.
15. Once the reboot is complete, log back in as root to get to the # command prompt.
16. Type `screen -ls` and press `ENTER`. While it might take upwards of 5 minutes, eventually there should be **8 Sockets in /run/screens/S-root**
17. Type `asterisk -r` and press `ENTER` to connect to the Asterisk console. There should be different processes like **sendcron** logging on and off.
18. Type `quit` and press `ENTER` to exit back to the # command prompt.

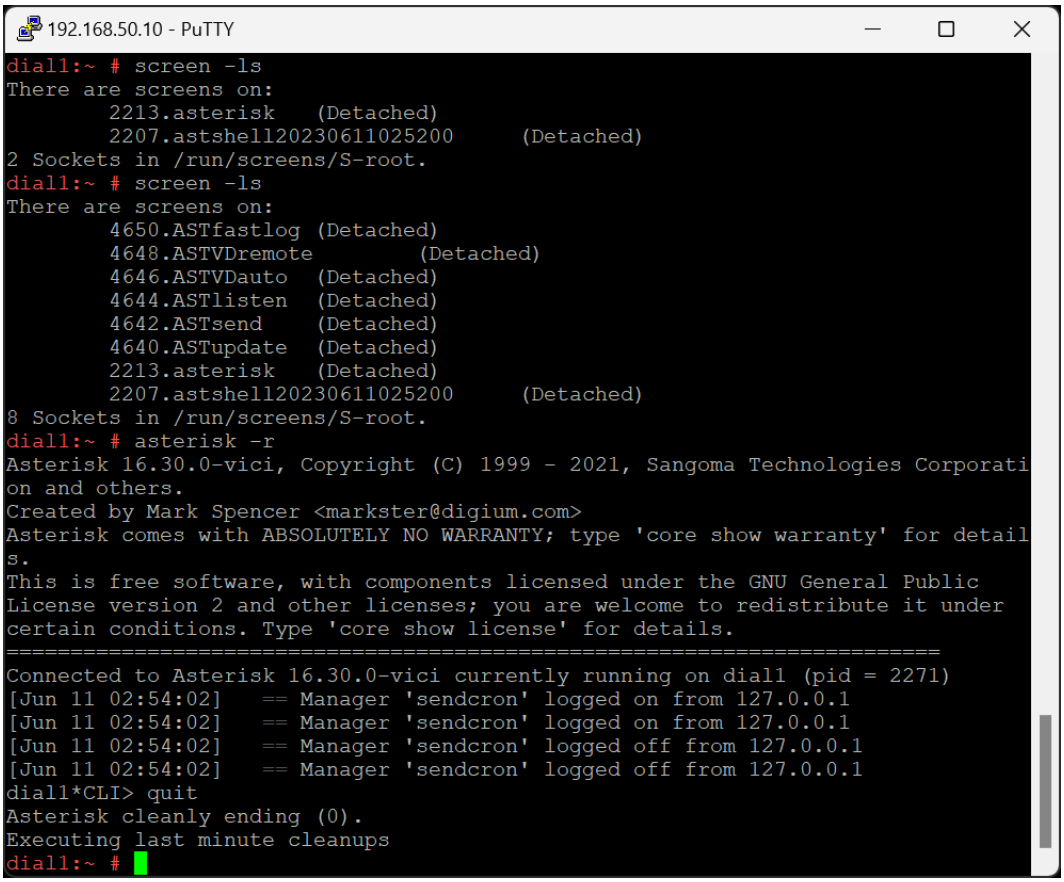
The Telephony server is now installed. If there are multiple telephony servers in the cluster, these instructions can be repeated on any additional servers.

Screenshots

Install Telephony server



Reboot and verify Asterisk running


192.168.50.10 - PuTTY
dial1:~ # screen -ls
There are screens on:
2213.asterisk (Detached)
2207.astshell20230611025200 (Detached)
2 Sockets in /run/screens/S-root.
dial1:~ # screen -ls
There are screens on:
4650.ASTfastlog (Detached)
4648.ASTVDremote (Detached)
4646.ASTVDauto (Detached)
4644.ASTlisten (Detached)
4642.ASTsend (Detached)
4640.ASTupdate (Detached)
2213.asterisk (Detached)
2207.astshell20230611025200 (Detached)
8 Sockets in /run/screens/S-root.
dial1:~ # asterisk -r
Asterisk 16.30.0-vici, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
Connected to Asterisk 16.30.0-vici currently running on dial1 (pid = 2271)
[Jun 11 02:54:02] == Manager 'sendcron' logged on from 127.0.0.1
[Jun 11 02:54:02] == Manager 'sendcron' logged on from 127.0.0.1
[Jun 11 02:54:02] == Manager 'sendcron' logged off from 127.0.0.1
[Jun 11 02:54:02] == Manager 'sendcron' logged off from 127.0.0.1
dial1*CLI> quit
Asterisk cleanly ending (0).
Executing last minute cleanups
dial1:~ #

CHAPTER

THREE

NETWORKING

By default ViciBox will attempt to use DHCP on the first network interface. Any IP obtained will be shown on the server's display.

Table 1: Network Definitions

Term	Definition
WAN	Wire Area Network, the Internet
LAN	Local Area Network, private network
ISP	Internet Service Provider
NAT	Network Address Translation, the firewall

3.1 Deployments

This section describes common network deployment scenarios for ViciBox and their typical considerations.

3.1.1 LAN and WAN

In this deployment, the ViciDial Web and Telephony server is directly connected to both the LAN for agents and the WAN/ISP. This eliminates potential issues with routers not handling SIP properly. The only limit to scaling is how many static IPs can be obtained.

Common Drawbacks:

- Multiple static IPs may be expensive or hard to get from your ISP
- Requires two separate switches or one that can do VLANs
- Firewall must be managed on the server itself
- Might not be allowed under corporate network security policy

3.1.2 WAN Only

Mostly used by remote or work-from-home contact centers, this deployment is commonly done in a data center or colocation provider. Here, the servers are only connected to the Internet. This deployment is the most complicated with a cluster, as firewall rules need to be created to allow the cluster to communicate. If the IP addresses are not contiguous, then each server will need individual firewall rules to every other server. It is also much more likely that any network changes or issues can easily result in the server being unreachable. This is a more advanced network deployment than any of the others and is not recommended if you are not experienced with Linux and networking.

Common Drawbacks:

- Multiple static IPs may be expensive or hard to get from your ISP
- Using a data center or colocation provider can be quite costly
- Firewall configuration in a cluster can get burdensome if the static IPs aren't contiguous
- Requires a bit of networking and Linux experience to handle

3.2 Firewall

ViciBox uses firewalld for its firewall. The firewall is configured through different operational modes that can be combined together. Each mode is designed to handle specific use cases that come up in a VoIP environment.

By default ViciBox is configured to use the VoIP Black List mode of operation. This mode downloads and maintains a list of known SIP abusers. While effective, it's important to understand what the firewall is doing and how to configure it properly.

Attention: There is a known issue between the default VoIP Black List mode of operation and firewalld. The problem is that the size (50K+ entries) of the list can cause firewalld to enter a race condition. This most commonly happens after making network changes in `yast lan`. The recommended action is to stop firewalld with `service firewalld stop`, make any needed network changes, then `reboot` to cleanly load the list back in. If the VoIP Black List is not needed then just disable it. While this is not ideal it is better then nothing at all.

3.2.1 Ports

This section describes the collection of ports that need to be exposed to agents and the internet depending on your installation.

SIP and RTP Traffic

SIP signalling is on UDP port 5060. This is the control port and should primarily be limited to the networks, carriers, and agents that need it. If you have multiple dialers behind a firewall, this can only be forwarded to one dialer behind the firewall and that dialer will be responsible for all inbound calls. When a carrier gives you a list of IPs for their network, you want to ask them what the 'signalling' or 'SIP' IPs are. This is what you specifically want to allow in on a firewall.

RTP traffic is an ephemeral pool of ports as defined in `/etc/asterisk/rtp.conf`. By default, this port range is UDP 10000-20000. These ports are used for audio only and should generally be open to all of the public internet. Since there is no control protocol, there is no attack vector on these ports. That, coupled with the inevitable fact that carriers, despite their best efforts, will inevitably send audio from an IP outside of their published ranges due to adding new peers and aggregates.

With multiple dialers behind a firewall, you will need to assign a unique port range to each one. The recommendation is to break up the port pool into 5000 port chunks, starting with port 10000. For example:

Table 2: Example RTP Port Ranges

Dialer	UDP Port Range
dialer1	10000-14999
dialer2	15000-19999
dialer3	20000-24999

HTTP and HTTPS

The standard ports for HTTP is TCP 80 and for HTTPS is TCP 443. The recommendation is to set up a valid SSL certificate and force all HTTP connections to HTTPS. See the *SSL* section for more information. If you are using the web phone, then it is required that a valid SSL certificate be set up on the server.

Web Sockets

The standard port for Web Sockets (WSS) is TCP 8089. This requires a valid SSL certificate that matches the server's FQDN. Please see the *SSL* section for more information on how to install an SSL certificate. This port is a control port, so some care should be taken to restrict who has access to it. While it does not currently have the same level of vulnerability as an exposed SIP port, it will eventually.

3.2.2 Zones

This section explains the concept of zones in firewalld, the underlying firewall in ViciBox, and how they apply to network interfaces and traffic.

The concept of zones in firewalld is applied globally to all connections. Any network traffic received on any network interface can be moved to a specific zone if it matches a rule. The default zone assigned to the network interface is only used when no other matching rule is found.

For example, even though `eth0` on the server has IP `192.168.50.4/24` and is in the **Trusted** zone by default, it's possible to have IP `192.168.50.40` be sent to the **External** zone if it's included on the *ViciDial Whitelist*. Haphazardly adding IP addresses to things without understanding this concept is the biggest cause of "The whitelist/portal isn't working", "I can't access the server anymore", and other timeless classics.

Public

This is the public zone, also known as the Internet. Anything attached or in the public zone will be available to anyone. In general, the RTP ports will be publicly available along with potentially the HTTPS web server.

Trusted

This zone is where the LAN network interface should be placed. Everything in this zone is allowed to connect to anything on the server. There is no need to add or remove services from this zone as it allows everything by default. It is functionally equivalent to turning the firewall completely off.

External

This zone is for allowed or authenticated access. The *ViciDial Whitelist* and *Dynamic Portal* will assign IP addresses to this zone. Any services you want remote or work-from-home agents to have access to will need to be listed in this zone. By default, all needed services for ViciDial are already added.

3.2.3 ViciDial Whitelist

The ViciDial White List mode is designed to only allow known good IP addresses to connect to the server. This is accomplished by integrating with the ViciDial Remote Agent interface to dynamically allow connections from agents as they connect. This mode also allows for static entries to be added for things like SIP carriers and other trusted sources.

Configuration Steps

1. If not already, log in as the `root` user to get to the `#` command prompt.
2. Type `vicibox-firewall` and press `ENTER`.
3. Using the arrow keys, select **ViciDial White List** and press `ENTER`.
4. Type `Y` and press `ENTER` to confirm the change.
5. Review the output to ensure the change was successful.

Static Entries

Static entries can be added to the white list by editing the `/etc/firewalld/whitelist.conf` file. Each entry should be on its own line and can be either an IP address or a network in CIDR notation.

Example `whitelist.conf`:

- 192.168.1.0/24
- 10.0.0.0/8
- 1.2.3.4

Setup

The White List is only compatible with the Dynamic Portal. Below are the changes you would make to the ViciBox crontab entry. The recommendation is to delete the old entries and copy-paste these in. The crontab entries shown are for White List Only and White List with Dynamic Portal.

Listing 1: White List only crontab

```
### ViciBox integrated firewall, using whitelist only, and check once every minute
@reboot /usr/bin/VB-firewall --white --quiet
* * * * * /usr/bin/VB-firewall --white --quiet
```

Listing 2: White List with Dynamic Portal crontab

```
### ViciBox integrated firewall, using whitelist and dynamic portal, and check once␣
↪every minute
@reboot /usr/bin/VB-firewall --white --dynamic --quiet
* * * * * /usr/bin/VB-firewall --white --dynamic --quiet
```

The IP List feature must be enabled under *Admin* → *Settings*.

All services under the **Public** zone should be removed except **dhcpv6-client** and **rtp**.

Any IP address on the White List will be handled through the **External** zone in `yast firewall`. By default, all the services needed for ViciDial are already listed in this zone.

Control

The White List can be controlled through the `ViciWhite` IP list. This can be found by going to *Admin* → *IP Lists*. The format is simple, with one IP or CIDR network per line. Any changes made may take up to 2 minutes to apply.

Listing 3: Sample White List entries

```
157.240.14.35
142.250.217.206
64.233.160.0/19
66.102.0.0/20
```

3.2.4 Black List

The Black List blocks specific IP address' from accessing the server. This is controlled through an IP List inside ViciDial called **ViciBlack**. This allows for easy administration as the firewall can be controlled from the Admin interface.

Setup

The Black List needs to be setup in the crontab first.

Listing 4: Black List only crontab

```
### ViciBox integrated firewall, using blacklist only, check once every minute
@reboot /usr/bin/VB-firewall --black --quiet
* * * * * /usr/bin/VB-firewall --black --quiet
```

Listing 5: Black List with VoIP BL

```
### ViciBox integrated firewall, using blacklist and VoIPBL, check VoIPBL␣
↪every 6 hours and blacklist every minute
```

(continues on next page)

(continued from previous page)

```
@reboot /usr/bin/VB-firewall --black --voipbl --quiet
0 */6 * * * /usr/bin/VB-firewall --voipbl --quiet
* * * * * /usr/bin/VB-firewall --black --dynamic --quiet
```

The IP List feature must be enabled under *Admin* → *Settings*.

Control

The White List can be controlled through the `ViciWhite` IP list. This can be found by going to *Admin* → *IP Lists*. The format is simple with one IP or CIDR network per line. Any changes made may take up to 2-minutes to apply.

Listing 6: Sample White List entries

```
157.240.14.35
142.250.217.206
64.233.160.0/19
66.102.0.0/20
```

3.2.5 Dynamic Portal

The dynamic portal allows for remote or work-from-home agents to authenticate with their ViciDial logins on a separate web portal. This portal is standalone outside the framework of ViciDial and restricts how fast authentication attempts can be made. It allows agents to dynamically add their IP to the firewall for ViciDial.

Setup

The dynamic portal is only compatible with the White List and is often ran in conjunction with it.

Listing 7: Dynamic Portal only crontab

```
### ViciBox integrated firewall, using whitelist only, and check once every␣
↪minute
@reboot /usr/bin/VB-firewall --dynamic --quiet
* * * * * /usr/bin/VB-firewall --dynamic --quiet
```

Listing 8: White List with Dynamic Portal crontab

```
### ViciBox integrated firewall, using whitelist only, and check once every␣
↪minute
@reboot /usr/bin/VB-firewall --white --dynamic --quiet
* * * * * /usr/bin/VB-firewall --white --dynamic --quiet
```

All services under the **Public** zone should be removed except **dhcpv6-client** and **rtp**.

Any IP address from the Dynamic Portal will be handled through the **External** zone in `yast firewall`. By default all the services needed for ViciDial are already listed in this zone.

Enable Portal

The dynamic portal needs to be exposed to the Public zone. While the portal works with standard HTTP it's recommended to only use HTTPS. This will require a properly setup DNS and SSL certificate. If the SSL certificate is handled outside of `vicibox-ssl` then /etc/apache2/vhosts.d/dynportal-ssl.conf needs to be updated to point to the correct SSL certs.

Listing 9: Enable SSL Dynamic Portal

```
firewall-cmd --permanent --zone=public --add-port=446/tcp
firewall-cmd --reload
```

The portal should now be reachable by going to https://your.server.com:446/valid8.php

Obscurity

Since security by obscurity can be a good thing, it's also possible to change the dynamic portal to run on another port besides 446. To do that two files will need to be modified as well as the above firewall rule. References to port '446' will need to be changed to your own random port of choice.

Table 3: Dynamic Portal Config Files

File	Modification to make
/etc/apache2/vhosts.d/dynportal-ssl.conf	First line change 446 to preferred port
/etc/apache2/listen.conf	Change all references of 446 to preferred port

Apache and firewalld will need to be restarted after making those changes. That can also be accomplished through a quick `reboot`.

Listing 10: Restart apache and firewalld

```
service apache2 restart
firewall-cmd --permanent --zone=public --add-port=<preferred-port>/tcp
firewall-cmd --reload
```

3.2.6 VoIP Black List

This mode of operation downloads the VoIP Black List and loads it into the firewall. This is a community-submitted list that contains over 55,000 IP entries of known SIP abusers.

Default Operation

This mode of operation is the ViciBox default for new server installations. It is enabled through the root's crontab.

Listing 11: Default crontab entry

```
### ViciBox integrated firewall, by default just load the VoIP Black list and reload it␣
↪every 4 hours
### You can lock everyone out of your server if you set this wrong, so understand what␣
↪you are doing!!!
@reboot /usr/bin/VB-firewall --voipbl --noblack --quiet
0 */6 * * * /usr/bin/VB-firewall --voipbl --noblack --quiet
```

To disable the VoIP Black List, just comment out the last two lines above in the crontab.

Listing 12: Commented crontab entry

```
### ViciBox integrated firewall, by default just load the VoIP Black list and reload it␣
↪every 4 hours
### You can lock everyone out of your server if you set this wrong, so understand what␣
↪you are doing!!!
#@reboot /usr/bin/VB-firewall --voipbl --noblack --quiet
#0 */6 * * * /usr/bin/VB-firewall --voipbl --noblack --quiet
```

3.3 SSL

ViciBox supports SSL out of the box with a self-signed certificate. While functional, it is not recommended to use this certificate at all. It is merely a placeholder for a real SSL certificate.

For clusters, it is recommended to use a wildcard SSL certificate. These are available from several Certificate Authorities, including free providers. Commercial SSL providers tend to be less problematic and require yearly renewals. Free SSL providers generally require that the certificate be renewed every 30 to 90 days through an automated process. This automated process, in conjunction with firewalls, tends to be an issue.

Attention: Before SSL can be set up, the server needs a Fully Qualified Domain Name (FQDN). For example, if `your.domain.com` is the FQDN for the server, then the ViciDial web interface should be accessible at `http://your.domain.com` in a web browser. Until this is correctly working, no SSL certificate will ever work.

3.3.1 Common Files

To help SSL certificates work across a cluster without requiring multiple webRTC templates, there is a common file location that Apache and Asterisk are configured to use. By default, the self-signed certificate is located there. To install your own certificates, a symlink should be created from the actual SSL certificate to the common one.

Table 4: Common SSL files

File Location	Purpose
/etc/apache2/ssl.crt/vicibox.crt	SSL Certificate
/etc/apache2/ssl.key/vicibox.key	SSL Private Key
/etc/apache2/ssl.crt/vicibox-chain.crt	SSL Certificate Chain

3.3.2 ViciBox SSL Script

The `vicibox-ssl` script automates the process of requesting and installing an SSL certificate from Let's Encrypt. This includes setting up automated renewal and configuring both Apache and Asterisk to use the certificate.

Table 5: Example SSL settings

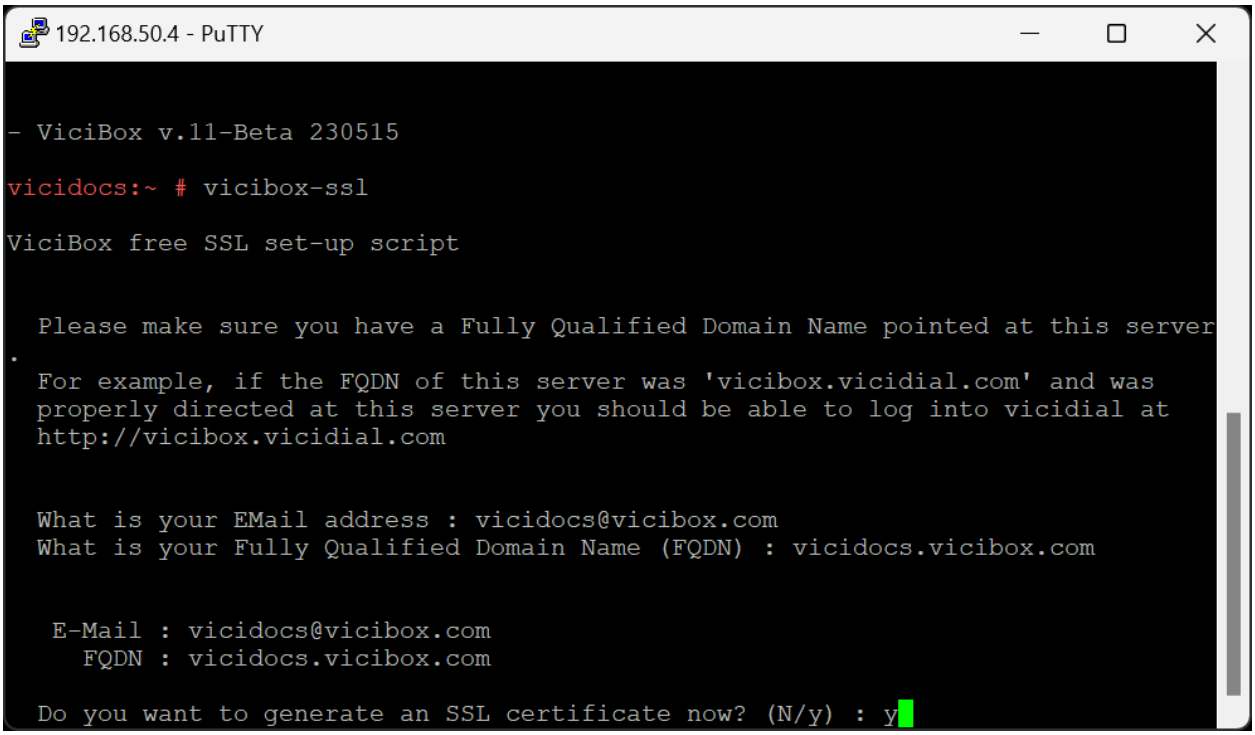
Setting	Value
Fully Qualified Domain Name (FQDN)	vicidocs.vicibox.com
EMail Alert Address	vicidocs@vicibox.com

3.3.3 Setup Instructions

1. If not already, log in as the `root` user to get to the # command prompt.
2. Type `vicibox-ssl` and press `ENTER` to start the setup process.
3. Type in the EMail address to use for the SSL certificate, e.g. `vicidocs@vicibox.com`
4. Type in the FQDN to use for the SSL certificate, e.g. `vicidocs.vicibox.com`
5. After reviewing the typed in information, press `Y` and then `ENTER` to start the automated setup process.
6. After an SSL certificate is generated, press `Y` and press `ENTER` to enable the new certificate.
7. Press `Y` and `ENTER` to set up the needed crontab entry for cert renewal.
8. Verify Asterisk loaded the SSL certs: `asterisk -rx "http show status"`
9. Test by visiting `https://your.domain.com` in a browser.

3.3.4 Screenshots

Run vicibox-ssl


192.168.50.4 - PuTTY
- ViciBox v.11-Beta 230515
vicidocs:~ # vicibox-ssl
ViciBox free SSL set-up script
Please make sure you have a Fully Qualified Domain Name pointed at this server
.
For example, if the FQDN of this server was 'vicibox.vicidial.com' and was
properly directed at this server you should be able to log into vicidial at
http://vicibox.vicidial.com
What is your EMail address : vicidocs@vicibox.com
What is your Fully Qualified Domain Name (FQDN) : vicidocs.vicibox.com
E-Mail : vicidocs@vicibox.com
FQDN : vicidocs.vicibox.com
Do you want to generate an SSL certificate now? (N/y) : y

CHAPTER

FOUR

MAINTENANCE

Common maintenance items on ViciBox

4.1 Change Time Zone

The timezone of the server should match the timezone for its physical location. These instructions will modify the timezone settings of the underlying operating system. If these instructions are followed after ViciDial has been installed, you will still need to modify the GMT Offset of the server in the admin interface. This can be found under *Admin* → *Servers* in ViciDial.

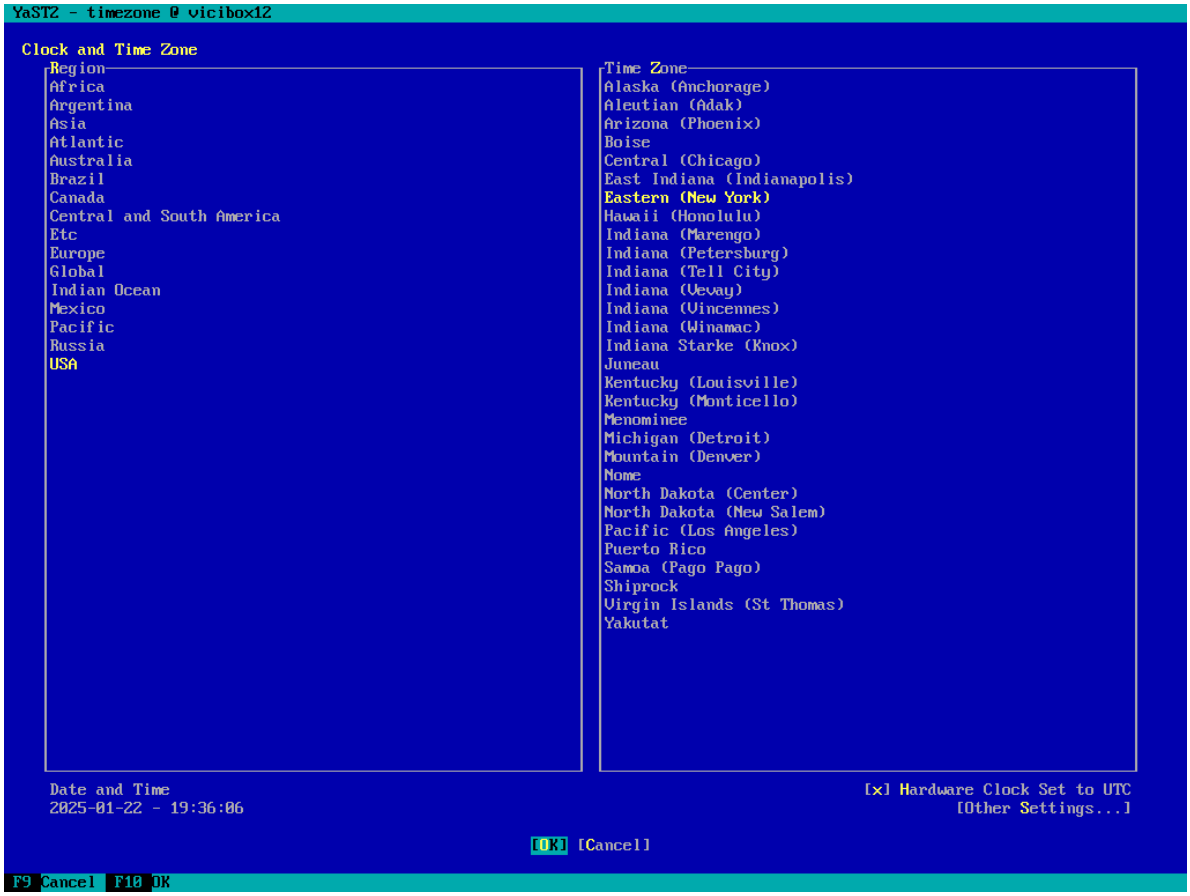
4.1.1 Change Time Zone Steps

1. If not already, log in as the `root` user to get to the `#` command prompt.
2. Type `vicibox-timezone` and press `ENTER` to start the time zone setup.
3. Using the up and down arrow keys, select the appropriate region and press `ENTER`.
4. Using the up and down arrow keys, select the appropriate time zone and press `ENTER`.
5. The selected time zone should be shown on the output. Type `reboot` at the `#` command prompt to reboot the server.

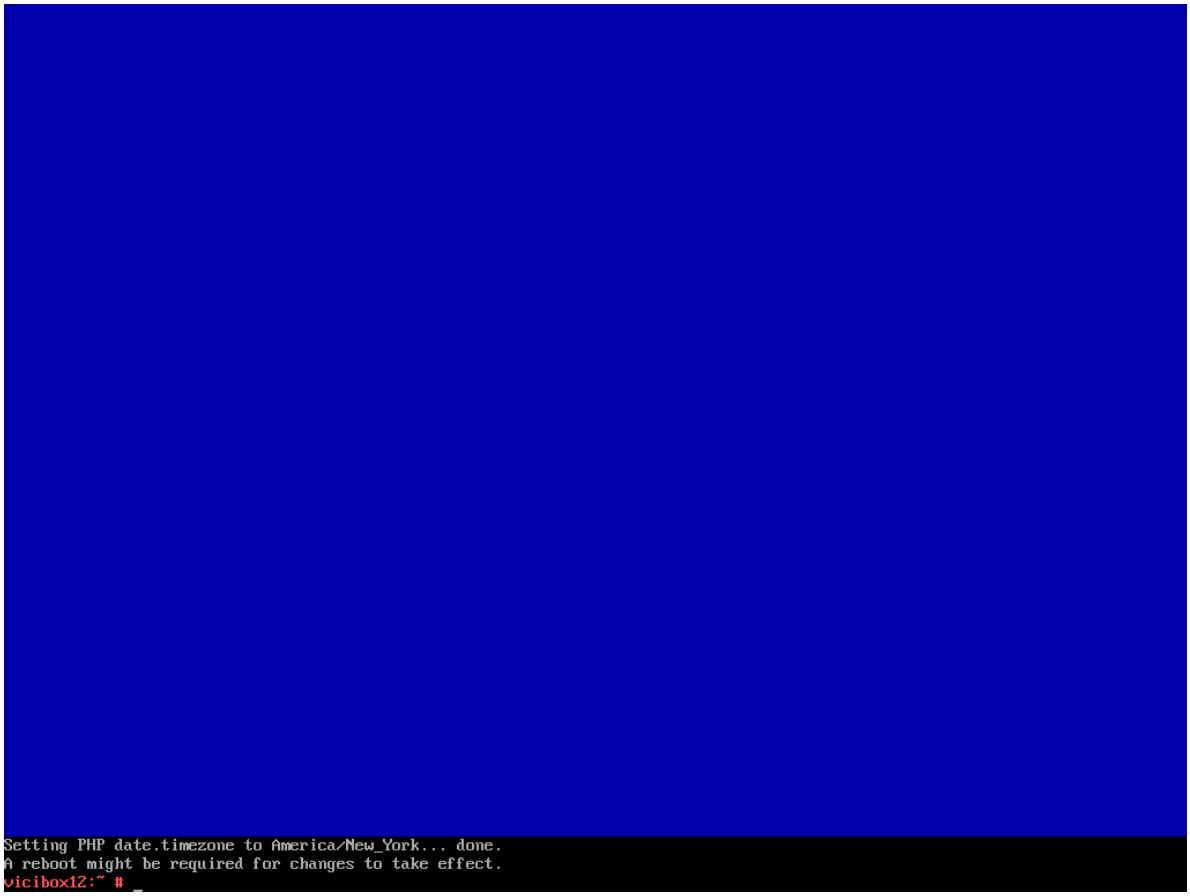
4.1.2 Screenshots

Run vicibox-timezone

Select Region and time zone



Verify output



4.2 Change Root Password

Please try to pick a root password you will remember. Recovering a lost or forgotten root password is not overly trivial. Lastly, if there is no root access to the server then ViciDial and ViciBox cannot be maintained. You have been warned!

4.2.1 Password Guidelines

The root user is everything in Linux. It's highly recommended to change the root users password to something secure. While everyone will have their own preferences for passwords, here are some rough guidelines to help create a more secure password:

- At least 14 characters in length
- Contains at least one upper case (ABC)
- Contains at least one lower case (abc)
- Contains at least one number (123)
- Contains at least one special character (@%!)
- Does NOT contain 'vicidial', 'vici', 'password', or 'pass'

Tip: While a truly random password is the most secure, a password you can remember is more useful. I recommend basing the password around a 'phrase' to help. As an example, albeit a bad one, of this is the password 'ViciPass4U!'.

4.2.2 Change Password Steps

1. If not already, login as the `root` user to get to the **#** command prompt
2. Type `passwd` and press `ENTER` to change the root password
3. At the **New password:** prompt type in your new root password and press `ENTER`
4. At the **Retype new password:** prompt type in the new root password again and press `ENTER`

4.2.3 Screenshots

Change root password

4.3 Change External IP

When the external IP is changed, a few settings need to be updated in ViciBox to match. To help facilitate this, the `vicibox-externip` script was added. This script will attempt to auto-detect the correct external IP and insert it into Asterisk. Alternatively, you can provide the new IP to the script when you run it.

Using vicibox-externip

1. If not already, log in as the `root` user to get to the # command prompt.
2. Type `vicibox-externip` and press `ENTER`. Alternatively, type in the IP address to use as well, e.g. `vicibox-externip 1.2.3.4`.
3. Review the IP summary information, and press `Y` and press `ENTER` to make the change and update Asterisk.

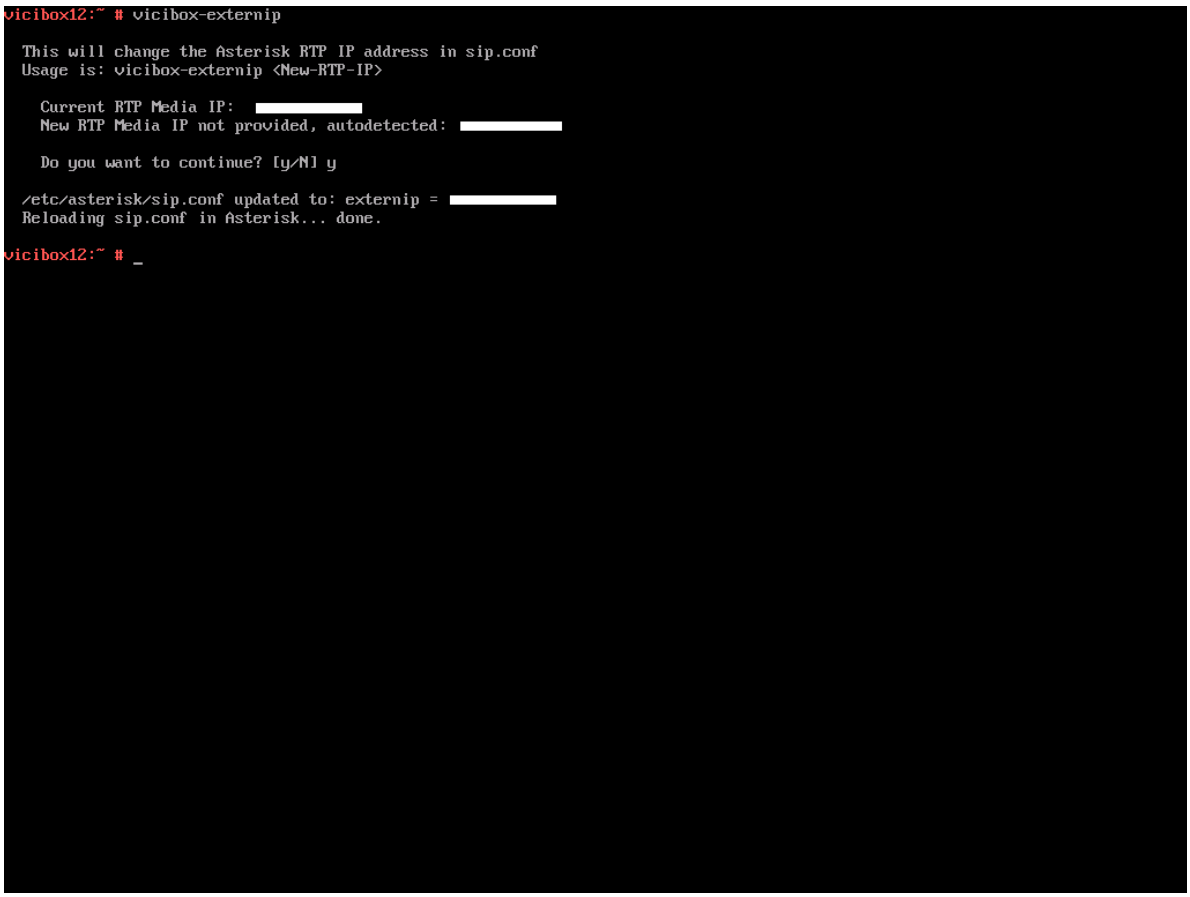
Additional Changes

In addition to modifying the Asterisk configuration, the following items will also need to be checked and possibly adjusted:

- **External Server IP** under *Admin* → *Servers*
- DNS entries that pointed to the old server IP
- **Sounds Web Server** under *Admin* → *System Settings*

4.3.1 Screenshots

Run vicibox-externip



CHAPTER

FIVE

BUG FIXES

Bug fixes are rolled up into later realeases. So a ViciBox v.12.0.1 system does not need any of the updates listed for ViciBox v.12.0.0. You only need to apply updates that are equal to or greater then your ViciBox install media version.

The version of ViciBox used to install the server is shown just above the # command prompt after logging in as `root`, I.E. **- ViciBox v.12.0.1 250118**. Most of the fixes are done through the CLI by logging in as the root user. This can be done over SSH or through a directly attached keyboard and monitor.

As a general rule the fixes are mainly for issues that can't reasonably be applied through a standard package update. The following sections are separated by ViciBox version and then the specific issue.

5.1 ViciBox 11.0

This section contains bugfixes, errata, and patch notes related to the ViciBox v.11.0 release. You only need to run the fixes that apply to your version or newer. For example, if you are running ViciBox v.11.0.1, you only need to run the fixes for v.11.0.1 and later, not the fixes for v.11.0.0.

5.1.1 ViciBox 11.0.0 AGI Module Bug

This bug affects ViciBox v.11.0.0 installations where the res_agi.so module fails to load due to an outdated modules.conf file. The `res_speech.so` module is required for `res_agi.so` to load, but the packaged configuration prevents this, causing ViciDial to malfunction. Removing the `noload => res_speech.so` line from `/etc/asterisk/modules.conf` and rebooting resolves the issue.

Note: This fix is only needed for servers already installed with ViciBox v.11.0.0. If you ran `zypper up` before `vicibox-install`, you do not need to apply this fix.

Symptoms

Telephony servers with this issue will show log output stating that no application can be found for the AGI extension.

Listing 1: Example Log Output

```
[Jun 28 12:47:30] == Using SIP RTP CoS mark 5
[Jun 28 12:47:30] > 0x7fd550024340 -- Strict RTP learning after remote address set to:␣
↪192.168.1.106:12722
[Jun 28 12:47:30] WARNING[25228][C-00000006]: pbx.c:2928 pbx_extension_helper: No␣
↪application 'AGI' for extension (defaultlog, 9684, 1)
```

(continues on next page)

(continued from previous page)

```
[Jun 28 12:47:30] == Spawn extension (defaultlog, 9684, 1) exited non-zero on 'SIP/145-
↪00000008'
[Jun 28 12:47:30] WARNING[25228][C-00000006]: pbx.c:2928 pbx_extension_helper: No␣
↪application 'AGI' for extension (defaultlog, h, 1)
[Jun 28 12:47:30] == Spawn extension (defaultlog, h, 1) exited non-zero on 'SIP/145-
↪00000008'
```

The Fix

To resolve this issue, follow these steps:

1. Log in as the `root` user to access the # command prompt.
2. Run the following command to comment out the problematic line:

```
sed -i 's/^noload => res_speech.so/;noload => res_speech.so/' /etc/asterisk/modules.
↪conf
```

3. Reboot the server:

```
reboot
```

Alternatively, you can restart Asterisk without rebooting:

```
asterisk -rx "core restart now"
```

5.1.2 ViciBox 11.0.0 MD Image Bug

This bug affects ViciBox v.11.0.0 installations using the MD image, where the /boot directory is only 200 MB. This prevents newer kernel updates from installing. The fix is to remove the separate /boot partition and use the root filesystem for /boot. This was corrected in ViciBox v.11.0.1. Only follow these instructions if you have already run vicibox-mdraid1 on a ViciBox v.11.0.0 system.

Symptoms

When attempting to update the system using `zypper up` you will get an error when a new kernel attempts to install. This results in no new kernel updates being installed.

Listing 2: Example zypper Output

```
(167/212) Installing: kernel-firmware-amdgpu-20230724-150500.3.3.1.noarch␣
↪[done]
(168/212) Installing: kernel-firmware-all-20230724-150500.3.3.1.noarch ...
↪[done]
  installing package kernel-default-5.14.21-150500.55.12.1.x86_64 needs 26MB␣
↪on the /boot filesystem
(169/212) Installing: kernel-default-5.14.21-150500.55.12.1.x86_64 ......
↪[error]
Installation of kernel-default-5.14.21-150500.55.12.1.x86_64 failed:
Error: Subprocess failed. Error: RPM failed: Command exited with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

The Fix

To resolve this issue, follow these steps:

1. Log in as the `root` user to access the # command prompt.
2. Copy and paste the following commands to remove the separate /boot partition:

Listing 3: Remove /boot partition

```
cd /
umount /boot/efi
mkdir boot-orig
rsync -ravv /boot/ /boot-orig/
umount /boot
rsync -ravv /boot-orig/ /boot/
mount /boot/efi
cp /etc/fstab /etc/fstab.orig
sed -i '/boot ext4/c\' /etc/fstab
```

5.1.3 ViciBox 11.0.1 MariaDB Limits Bug

This bug affects ViciBox v.11.0.1 installations where the MariaDB limits config file was mistakenly placed in `/etc/security` instead of `/etc/security/limits.d`. The fix is to move the file to the correct directory. This issue primarily affects larger cluster setups, but single ViciBox Express setups may also be impacted.

Symptoms

You may see MariaDB logs stating that they cannot open a table, create a tmp file, can't spawn a process, or that a limit has been reached.

The Fix

To resolve this issue, follow these steps:

1. Log in as the `root` user to access the # command prompt.
2. Move the MariaDB limits config file to the correct directory:

```
mv /etc/security/mysql.conf /etc/security/limits.d/mysql.conf
```

3. Reboot the server to load the new settings:

```
reboot
```

5.2 ViciBox 12.0

This section contains bugfixes, errata, and patch notes related to the ViciBox v.12.0 release. You only need to run the fixes that apply to your version or newer. For example, if you are running ViciBox v.12.0.1, you only need to run the fixes for v.12.0.1 and later, not the fixes for v.12.0.0.

5.2.1 ViciBox 12.0 php.ini overwritten

It appears that in preparation for OpenSuSE 16.0 and the long overdue update of some of it's core components that SuSE has pushed out some PHP updates which overwrite the vicidial specific options in php.ini. This also applies to all releases of ViciBox12 since the update is for the OpenSuSE 15.6 distro itself and not any specific ViciBox release. The solution is to re-enable these settings in php.ini.

Symptoms

The primary tell-tale sign of this is extremely large error and optionally access logs from apache with PHP warnings as well as slow or increased web server load.

The Fix

The below commands will restore the vicibox optimized settings in php.ini

Listing 4: Required fix and restart

```
sed -i "s/^error_reporting = E_ALL.*/error_reporting = E_ALL \& \~E_NOTICE \& \
↪~E_DEPRECATED \& \~E_STRICT \& \~E_WARNING/" /etc/php8/apache2/php.ini
sed -i 's/;opcache.enable=1/opcache.enable=1/g' /etc/php8/apache2/php.ini
sed -i 's/;opcache.memory_consumption=128/opcache.memory_consumption=128/g' /
↪etc/php8/apache2/php.ini
sed -i 's/;opcache.interned_strings_buffer=8/opcache.interned_strings_
↪buffer=16/g' /etc/php8/apache2/php.ini
sed -i 's/;opcache.max_accelerated_files=10000/opcache.max_accelerated_
↪files=20000/g' /etc/php8/apache2/php.ini
sed -i 's/;opcache.max_wasted_percentage=5/opcache.max_wasted_percentage=5/g' /
↪etc/php8/apache2/php.ini
sed -i 's/;opcache.validate_timestamps=1/opcache.validate_timestamps=1/g' /etc/
↪php8/apache2/php.ini
sed -i 's/;opcache.revalidate_freq=2/opcache.revalidate_freq=10/g' /etc/php8/
↪apache2/php.ini
service apache2 restart
```

5.2.2 ViciBox 12.0.0 RAID Tool Bug

If you applied updates before running the RAID setup during the first login, you likely do not have this issue.

The ViciBox MDRAID1 tool (`vicibox-mdraid1`) had an issue where previous MD RAID arrays could interfere with the expected partitioning layout. The Linux kernel autoassembles any MD RAID arrays it finds from leftover metadata, resulting in orphaned arrays like /dev/md126, /dev/md127, etc. The fix is to temporarily stop all orphaned RAID arrays on the system during RAID setup.

A second issue relates to reinstalling the OS. If you don't wipe the metadata from the drives, you may get zombie arrays—previous OS arrays mounted under the new OS. For example, after installing ViciBox 12, only /dev/md2 (the root array with /dev/sda4) should exist under `/proc/mdstat`. With a zombie array (e.g., from a previous ViciBox 11 install), you would see /dev/md1 also listed as read-only with /dev/sdb3 as the device. This is mitigated by checking if /dev/sdb3 (the target swap partition) already exists in /dev/md1 (the swap array). If it does, the swap array is stopped and the script can create it properly.

Symptoms

With the version of vicibox-mdraid1 included with the ViciBox v.12.0.0 image, you can potentially end up with an improperly set up swap array. If you look at the output of `/proc/mdstat` and see /dev/md1 listed as (auto-read-only), that is a good indication you have this issue. The screenshot below shows an example: on a newly installed ViciBox v.12.0.0 system without updates, the root array contains /dev/sda4 and the swap array contains /dev/sdb3.

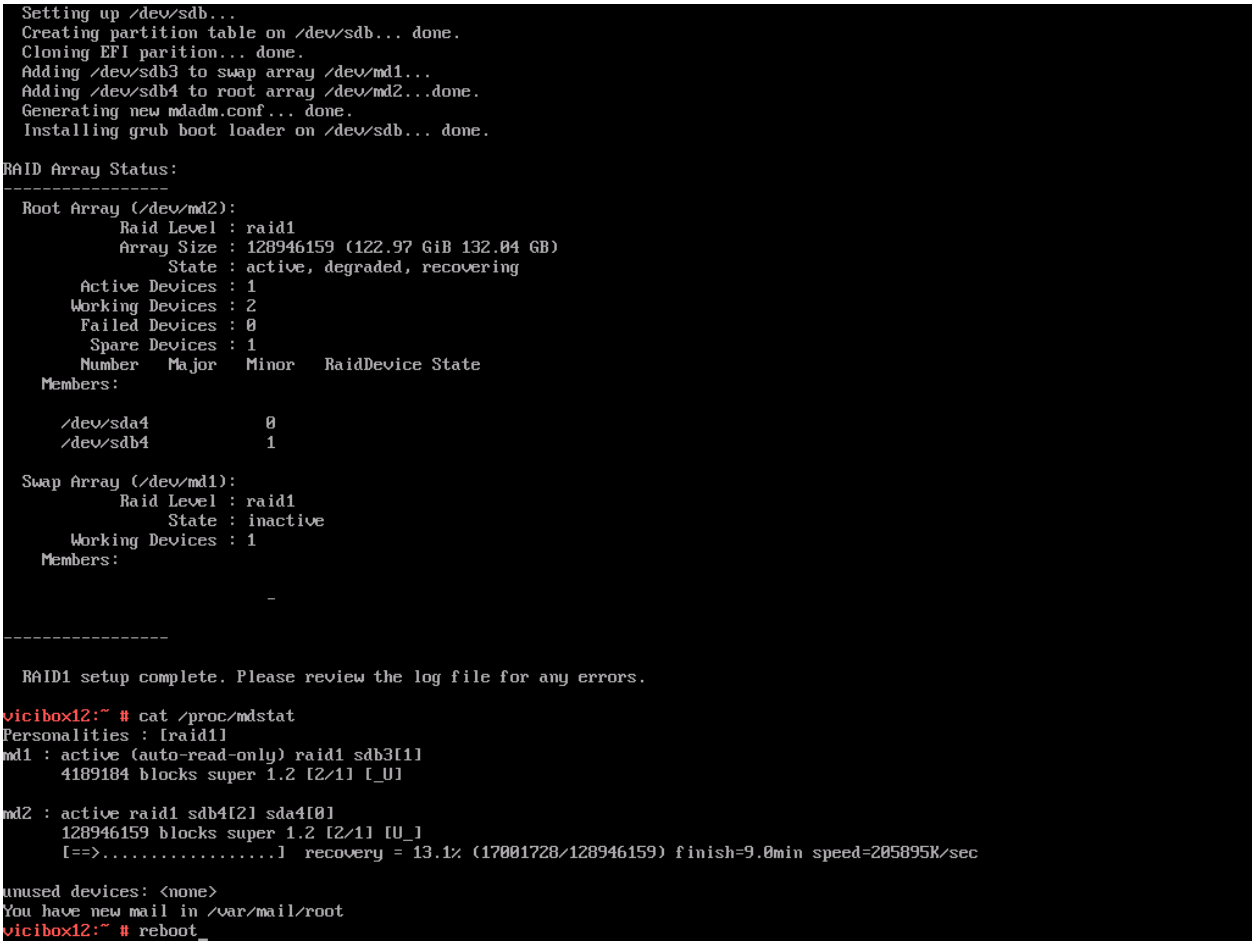


Fig. 1: Zombie RAID from previous ViciBox install

The Fix

It is important to determine the correct partitions to be used for the swap array. By default, the third partition in the image is used for swap. In the above screenshot, /dev/sda3 and /dev/sdb3 would be the swap partitions since we have /dev/sda and /dev/sdb shown. If you have NVMe drives then it would most likely be /dev/nvme0n1p3 and /dev/nvme1n1p3 for swap partitions. This will **highly** depend on your install and drives used. Below are the commands that would be used to fix the above screenshot.

Listing 5: Create proper swap partition

```
swapoff -a
mdadm --stop /dev/md1
mdadm --create --force /dev/md1 --level=1 --raid-devices=2 --metadata=1.2 /dev/
↪sda3 /dev/sdb3
mkswap /dev/md1
sed -i '/swap/ s/^/#/' /etc/fstab
echo "UUID=$(blkid -s UUID -o value /dev/md2) swap swap defaults 0 0" >> /etc/
↪fstab
swapon -a
cat /proc/mdstat
```

5.2.3 ViciBox 12.0.0 Firewall Disabled Bug

In ViciBox v.12.0.0, the firewall (firewalld) is not started by default. This is a security policy issue: by default, the network should be assumed hostile and must be firewalled until configured otherwise. This prevents accidentally attaching an open host to the internet.

Symptoms

You will see tons of noise in the logs about all sort of random IPs hitting you. You'll see them showing up in mysql logs and in places they never should be. For the low hanging fruit that is the 'script kiddie', you are now their new best friend.

The Fix

To resolve this issue, simply enable the firewall. You can do this through YaST or with the following commands. It is recommended to reboot after enabling the firewall to cleanly load the firewall and the default VoIP block lists.

Listing 6: Enable the firewall

```
systemctl enable firewalld.service
reboot
```

5.2.4 ViciBox 12.0.1 YaST Error Bug

In `/etc/firewalld/zones/external.xml`, the 'ssh' service is listed twice. While FirewallD ignores this, YaST will hang or error when opening the firewall module. This is a bug in the YaST firewall module, not in ViciBox. The fix is to remove the duplicate 'ssh' service from the external zone so YaST doesn't get confused.

Symptoms

The general symptom is that when you launch `yast firewall` or enter the firewall module, it hangs for a while before eventually presenting the error shown below.

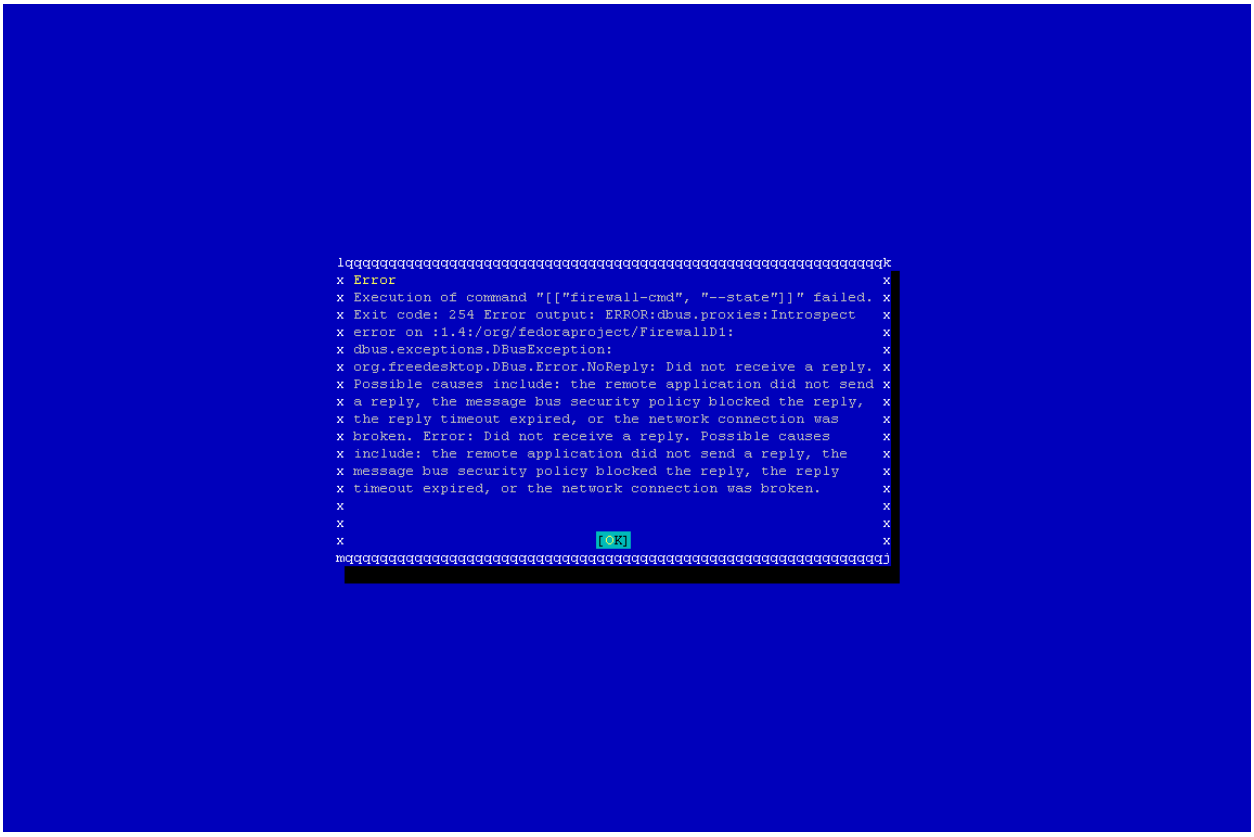


Fig. 2: YaST firewall issue

The Fix

If you apply updates with `zypper up` and do not have customized firewall settings, you can simply copy the new external.xml zone file over the old one. If you have custom firewall settings, manually edit the external.xml file to remove the duplicate 'ssh' service, or update the new file as needed.

Listing 7: Copy replacement file over old one

```
zypper ref && zypper up
cp /etc/firewalld/zones/external.xml.rpmnew /etc/firewalld/zones/external.xml
```

5.2.5 ViciBox 12.0.1 MariaDB TIMESTAMP Bug

If you are migrating a database from an older server to ViciBox v.12.0, you are not affected by this issue. This only applies to newly created databases loaded from the MySQL_AST_CREATE_tables.sql or through updates.

So MariaDB/MySQL finally changed a deprecated behavior that affects all TIMESTAMP fields in the database. The old behavior was to add default ON UPDATE CURRENT_TIMESTAMP clauses to all timestamps unless defined otherwise. Since this allowed for SQL to have hidden functionality not apparent in the source, it was deprecated and finally turned off by default somewhere between MariaDB 10.6 (ViciBox 11) and 10.11 (ViciBox 12). The new behavior is that all clauses must be explicitly defined. This means that all TIMESTAMP fields in the database that don't have an ON UPDATE CURRENT_TIMESTAMP clause will no longer update the timestamp when the row is updated. This is a problem for ViciDial because it relies on this behavior for the db_time field in the server_updater table amongst others.

There are portions of the ViciDial schema that existed before a TIMESTAMP field type was even available. These sections will need the SQL code updated to handle this new behavior. Once the schema is updated in SVN and the ViciBox ISO is updated, this will no longer be an issue. Until then, you'll need to manually fix this issue.

The official MariaDB documentation for this is here.

Symptoms

Symptoms vary, but basically all sorts of weird behavior will happen and ViciDial won't work right. The good news is that there's a setting to enable the old deprecated behavior.

The Fix

To resolve this issue, add the following line to your MariaDB configuration file and restart MariaDB:

Listing 8: Required fix and restart

```
echo "explicit_defaults_for_timestamp = Off" >> /etc/my.cnf.d/general.cnf
systemctl restart mariadb.service
```

If you set up a new ViciBox v.12.0 database using vicibox-express, vicibox-installer, or have applied updates, you may also need to run the optional fix below. Alternatively, if your database contains no important data, you can drop the database and re-run the installer. If you reinstall ViciBox and start over, only the required fix above is needed.

Listing 9: Optional export and import to fix fields

```
screen -s "DBFIX" # Optional, but recommended
cd /root # Go somewhere safe with lots of storage space
```

(continues on next page)

(continued from previous page)

```
mysqldump -B asterisk | gzip > asterisk-notimestamps.sql.gz
#mysql -u root -p -e "RENAME DATABASE asterisk TO asterisk_old;" # Uncomment␣
↪to rename the database instead of dropping it
mysql -u root -p -e "DROP DATABASE asterisk;" # If you renamed the database,␣
↪you can skip this line
mysql -u root -p -e "create database asterisk default character set utf8␣
↪collate utf8_unicode_ci;"
pv asterisk-notimestamps.sql.gz | gunzip | mysql -u root -p asterisk
```

5.2.6 ViciBox 12.0.2 FirewallD Crashing

It appears that in preparation for OpenSuSE 16.0 and the long overdue update of some of it's core components that SuSE has pushed out some firewallD updates that break. The solution seems to be to reinstall firewallD to fix it.

Symptoms

When running *yast firewall* it will either not load or give an error.

The Fix

To resolve this issue simply reinstall firewallD

Listing 10: Required fix and restart

```
zypper in --force firewalld
reboot #optional, but recommended
```

This also applies to all releases of ViciBox12 since the update is for the OpenSuSE 15.6 distro.

5.2.7 ViciBox 12.0.2 dynamic portal inaccessible

It appears that in preparation for OpenSuSE 16.0 and the long overdue update of some of it's core components that SuSE has pushed out some Apache updates which overwrote listen.conf. This prevents the dynamic portal from properly being accessible

Symptoms

The dynamic portal will be inaccessible even after enabling it in the firewall

The Fix

To resolve this issue re-enable the listen ports in Apache

Listing 11: Required fix and restart

```
sed -i 's/^Listen 80/Listen 80\nListen 81/' /etc/apache2/listen.conf
sed -i 's/^\t\tListen 443/\t\tListen 443\n\t\tListen 446/' /etc/apache2/listen.
↪conf
service apache2 restart
```

This also applies to all releases of ViciBox12 since the update is for the OpenSuSE 15.6 distro.