DOWNLOAD PDF LINUX SERVER CONFIGURATION TUTORIAL

Chapter 1 : How To Set Up A Linux Cloud Server - Written Tutorial

Linux Internet Web Server and Domain Configuration Tutorial HowTo Create an Apache based Linux website server. Create a web server with Linux, Apache, FTP and bind DNS: This tutorial covers the Linux server configuration required to host a website.

Ubuntu Apparmor community wiki Enable ExecShield: ExecShield is a Linux kernel feature which protects the system against buffer overflow exploits. This feature is performed by random placement of stack memory, prevention of execution of memory used to hold data and text buffer handling. Install a Linux kernel 2. The boot loader will also have to specify the PAE kernel for boot. The BIOS will also have to be configured to support it as well. This kernel should only be installed on a system with a x86 32 bit processor which offers this support. It is well known that there are various blocks of IP addresses where nefarious hackers and spam bots reside. These IP blocks were often once owned by legitimate corporations and organizations but have fallen into an unsupervised realm or have been hijacked and sold to criminal spammers. These IP blocks should be blocked by firewall rules. There are various friendly services which seek and discover these IP blocks to firewall and deny and they share this information with us. The Spamhaus drop list: This is a script to download the total drop list and generate an iptables filter script to block these very IP addresses: Done" To block the IP addresses just execute the script on each of your servers: Block or allow by country: One can deny access by certain countries or the inverse, allow only certain countries to access your server. See these sites to generate lists: CIDR lists Block forum and comment list spammers: Use the list generated from honeypots operated by StopForumSpam. It is also a rapidly changing list which is updated constantly. You may get the following error: Unknown error I found that by slowing down the execution of the script, I can avoid this error. I added a bash echo to write each line to the screen and it behaved much better although also much slower. Use the following to identify and geolocate an IP address InfoSniper. Turn off modules you are not going to use. If your web site does not serve https, turn it off. With past ssl exploits, those using this philosophy did not get burned. Red Hat Apache 2. This file is picked up from the line Include conf. Comment out the use of the ssl module by placing a " " in the first column. The Ubuntu distribution has a fairly frugal use of modules by default. The default configuration has SSL turned off. One can also block the https port using firewall rules: Attacks are often version specific. Spammers also trigger errors to find email addresses. ServerAdmin webmaster at megacorp dot com ServerSignature Off The response may be meaningless anyway if you are using the web server as a proxy to another. Block hackers and countries which will never use your website. Use the Apache directive Deny from to block access. Order allow,deny Block form bots Deny from Secure Shell SSH protocol suite of network connectivity tools are used to encrypt connections across the internet. SSH encrypts all traffic including logins and passwords to effectively eliminate network sniffing, connection hijacking, and other network-level attacks. In a regular telnet session the password is transmitted across the Internet un-encrypted. Note that SSH1 does have a major vulnerability issues. The "woot-project" web site cracking and defacing gang uses this vulnerability.

Chapter 2 : Linux Server Configuration Tutorial

LDAP Server Configuration and tutorial? Hello all. I like to know the LDAP(Light Weight Directory Access Protocol) its use,importance, usage and how to setup LDAP server on Redhat Linux, please help and if any one have tutorial or documentation regarding the above subject please give to me My email ID shaji_sivan@calendrierdelascience.com

If you get the following error: No route to host This means you have firewall issues most probably on the FTP server itself. Start by removing the firewall "iptables" rules: Passive mode can also help one past the rules: This toggles passive mode on and off. When on, FTP will be limited to ports specified in the vsftpd configuration file: This will also load the dependency: As root, grant access with the following command: File transfer directory browsing and compare. Ability to limit upload and download speed. Connect to multiple servers, transfer files, directory browsing, file content browsing. When hosting web sites, there is no need to grant a shell account which only allows the server to have more potential security holes. It requires users to have a real user shell. If it works for you, use it, as it is more secure to deny the user shell access. You can always deny telnet access. You should NOT be using this problem ridden version of ftpd. Use the latest wu-ftpd One must create the shell "ftponly" as defined below to allow vsftp access with no shell. Disable remote telnet login access allowing FTP access only: Protection set to -rwxr-xr-x 1 root root with the command: For more on Linux security see the: See DNS caching server In a purely web hosting configuration, Bind will only resolve for the IP addresses of the domains which are being hosted. This is the configuration which will be discussed and is often called an "Authoritative-only Nameserver". This is typically two separate computer systems hosted on two different IP addresses. It is not necessary that the Linux servers be dedicated to DNS as they may run a web server, mail server, etc. Note on Bind versions: Red Hat versions 6. Security jail for operation of bind. Utility commands like nslookup, host, dig system-config-bind: We will not be covering this as it is not required for web hosting. This is used by internet providers so their clients can cache the DNS entries of the sites they are visiting.

Chapter 3 : Linux Internet Server Security and Configuration Tutorial

Linux Internet Server Security and Configuration Tutorial. Security configuration and set-up for Linux servers exposed to the internet: Any computer connected to the internet will require steps and precautions to be taken to reduce the exposure to hacker threats.

Log In to your account Log In to your account. You are now in the control panel. Here you can set up, stop and start servers, and create and manage the drives that you install the servers on to. Add a server and a hard drive. Wait a few seconds until the image processing has finished. On your server, click the Start icon. In your server, you will see an IP address and VNC password which you will require for the next step. Connect to your server Connect via VNC: Congratulations you now have a Linux Cloud Server! Now your server is running, it is a fully-functional Debian Linux system. You can shut it down and the data will be stored on the drive. You can add a server or a drive only. When you add a drive, you just get the drive. Then we have a range of installation types: We have Debian, Ubuntu, a variety of Linux and Windows images. You install from the CD to the drive. We have a wide variety of Linux options as well as FreeBSD and a variety of Windows trial CDs that you can install as a trial or activate with your own licence keys. Boot from live CD: Boot from existing drive: Alternatively, follow this link to find more tutorials. Read more posts by this author.

Chapter 4 : Configure SQL Server replication on Linux | Microsoft Docs

Linux Servers Paul Cobbaut Publication date CEST Abstract This book is meant to be used in an instructor-led training. For self-study, the intent is to read.

Linux bit and bit. On the host machine, a new Hamachi network is created. The host installs and configures the Minecraft server software: The server IP field in server. The host passes the newly created Hamachi network credentials to each of the players. Each player connects using this IP as per the usual Minecraft multiplayer screen. Configuring the Minecraft server Configure the server by editing the server. Be certain to edit the file with a text editor that does not add formatting e. Additional configuration may not be necessary as many servers run fine from the default values. Operator status will not be changed if you change your username due to the use of UUID. Administrators and operators may execute commands. In other words, operator op privileges allow you to control certain aspects of the game e. Due to the transition to the UUID system, it is not recommended to directly edit whitelist. Connect to the Minecraft server If you are playing on the same machine on which the server is running, select the "Multiplayer" option in the game client, click direct connect, and then type in "localhost" instead of an IP address. Both hosting and playing on the same machine is not a recommended practice unless you have a powerful computer e. Users within your local network i. The internal IP address of a specific network adapter can be found by typing "ipconfig" into command prompt and looking for the ipv4 address. People connecting from the Internet i. You must port forward for someone outside your network to connect to the server. IP address notes Unless you set a static IP for the computer that is hosting the game, the internal IP address can change. This affects port forwarding rules, and can make them invalid. Each modem or router has a different way of setting a static IP address. You should refer to the manual for your device s or online documentation for further instruction. If you are having players connect to your external IP, your external IP can change if you do not have a static IP from your internet service provider. You may also search "my ip address" on Google and it will show your IP address. Alternatively, you can look into a DNS service that will allow you to have a name, rather than an IP address, that will remain the same. The name will point to your external IP address, regardless of whether or not it changes the DNS is updated when changes occur. For troubleshooting purposes you can try running Minecraft on the server machine and connect locally. You can connect through either localhost, your home network IP If for some reason you have trouble with connecting publicly over your IPv4, try connecting over IPv6. This should only be done for testing whether your server is online, external players should still use IPv4. Select your router from that list, skip the ad that comes after selecting the device, and you will see instructions for setting up port forwarding. Alternatively, you can read the documentation supplied with your router, modem, or other ISP related hardware. Verify the port is open, and note your external IP by using a port checker tool, such as You Get Signal. The default port you should test is , unless you specified something else. Have the Minecraft server running when you test the port. Local network dedicated servers This only applies to Classic v0. A common problem for server administrators is the inability to connect to your own server via another machine on your local network. A typical scenario for this is that you have a Classic server running on a dedicated machine, and you have your own machine which you play on. Normally, connecting via the URL generated for your server will result in an error message claiming that the server is offline. To correct this, you must add a function to the end of your URL, bookmarks, or whatever else you connect by. This situation does not effect Beta servers, and you should be able to connect via an internal or external IP. FAQ frequently asked questions Q: I have a problem which is not answered in here! What should I do to? Go to the Minecraft Forums and post your problem there. To help you, they need the following information: Operating system One machine or multiple computers Exact description of the problem Steps you have taken to solve the problem Any errors you encountered Screenshots of the problem if possible Anything else that might help us to solve your problem - there almost never is too much information passwords would be too much information! And please, if we were able to help you, post where the problem was exactly and what the fix was for that. Other people will appreciate that and we will be able to get a grip on the common problems! On a Windows

computer, when I double click the batch file it opens a command prompt window, but quickly disappears and the server does not start. If it says invalid path, it is probably due to an incorrect path for javaw. Or search your system for javaw. Also, you must have the offline version of Java installedâ€”not just the Java plug-in for your browser. You can also try replacing the contents of the. Whenever I try to get the server up, it says "Failed to bind to port! The most common reason this happens is because you put an IP address in the server-ip field in your server. By leaving it blank, you let it bind to all interfaces. You can try a different port by changing it in your server. Operation interrupted at java. For whatever reason, out of all of the operating systems, only Solaris throws that exception when a thread interrupts a connection. A workaround is to change the default behavior on the command line: When I try to connect to my server this is what it says: Connection lost The server responded with an invalid server key A: This is most usually caused by interacting with blocks in a protected area. If you are trying to interact near spawn, most likely it has been protected, by the minecraft server software; either build away from it or get operator status. My server runs fine, but I cannot connect to it! This could be caused by a series of issues. Please post a thread using the template provided above. How do you give a. Change the numbers in the server launch command "-Xmx1G -Xms1G". The -Xms part specifies how much memory the server starts with, and the -Xmx part is the maximum amount of memory the server can use. Why is the server CPU constantly at full load? Some users are experiences full CPU load on the server. This may be caused by the GUI graphic user interface window. Run the server with the nogui option to disable this window. Read Connect to the Minecraft server Q: I port forwarded and allowed java. Your modem might be acting as a router as well.

Chapter 5 : Get started with SQL Server on Ubuntu | Microsoft Docs

Tutorial: Getting Started with Ansible for Linux Server Configuration Management Lawrence Systems / PC Pickup. Loading Unsubscribe from Lawrence Systems / PC Pickup? Tutorial: Getting.

This will increase the security and usability of your server and will give you a solid foundation for subsequent actions. If you have not already logged into your server, you may want to follow the first tutorial in this series, How to Connect to Your Droplet with SSH , which covers this process in detail. If it is your first time logging into the server, with a password, you will also be prompted to change the root password. About Root The root user is the administrative user in a Linux environment that has very broad privileges. Because of the heightened privileges of the root account, you are actually discouraged from using it on a regular basis. This is because part of the power inherent with the root account is the ability to make very destructive changes, even by accident. The next step is to set up an alternative user account with a reduced scope of influence for day-to-day work. This example creates a new user called "demo", but you should replace it with a user name that you like: Enter a strong password and, optionally, fill in any of the additional information if you would like. Step Three â€" Root Privileges Now, we have a new user account with regular account privileges. However, we may sometimes need to do administrative tasks. To avoid having to log out of our normal user and log back in as the root account, we can set up what is known as "super user" or root privileges for our normal account. This will allow our normal user to run commands with administrative privileges by putting the word sudo before each command. To add these privileges to our new user, we need to add the new user to the "sudo" group. By default, on Ubuntu As root, run this command to add your new user to the sudo group substitute the highlighted word with your new user: For more information about how this works, check out this sudoers tutorial. Step Four â€" Add Public Key Authentication Recommended The next step in securing your server is to set up public key authentication for your new user. Setting this up will increase the security of your server by requiring a private SSH key to log in. Generate a Key Pair If you do not already have an SSH key pair, which consists of a public and private key, you need to generate one. If you already have a key that you want to use, skip to the Copy the Public Key step. To generate a new key pair, enter the following command at the terminal of your local machine ie. Hit return to accept this file name and path or enter a new name. Next, you will be prompted for a passphrase to secure the key with. You may either enter a passphrase or leave the passphrase blank. If you leave the passphrase blank, you will be able to use the private key for authentication without entering a passphrase. If you enter a passphrase, you will need both the private key and the passphrase to log in. Securing your keys with passphrases is more secure, but both methods have their uses and are more secure than basic password authentication. Remember that the private key should not be shared with anyone who should not have access to your servers! We will cover two easy ways to do this. This is because DigitalOcean disables password authentication if an SSH key is present, and the ssh-copy-id relies on password authentication to copy the key. Use ssh-copy-id If your local machine has the ssh-copy-id script installed, you can use it to install your public key to any user that you have login credentials for. Run the ssh-copy-id script by specifying the user and IP address of the server that you want to install the key on, like this: The corresponding private key can now be used to log into the server. On the server, as the root user, enter the following command to switch to the new user substitute your own user name: Create a new directory called. We will use nano to edit the file: To read more about how key authentication works, read this tutorial: Step Five â€" Configure SSH Daemon Now that we have our new account, we can secure our server a little bit by modifying its SSH daemon configuration the program that allows us to log in remotely to disallow remote SSH access to the root account. Begin by opening the configuration file with your text editor as root: This is generally a more secure setting since we can now access our server through our normal user account and escalate privileges when necessary. Modify this line to "no" like this to disable root login: Type this to restart SSH: We do not want to disconnect until we can confirm that new connections can be established successfully. Open a new terminal window on your local machine. In the new window, we need to begin a new connection to our server. This time, instead of using the root account, we want to use the new account that

we created. For the server that we showed you how to configure above, you would connect using this command. Substitute your own user name and server IP address where appropriate: After that, you will be logged in as your new user. Remember, if you need to run a command with root privileges, type "sudo" before it like this: At this point, you have a solid foundation for your server. You can install any of the software you need on your server now. If you are not sure what you want to do with your server, check out the next tutorial in this series for Additional Recommended Steps for New Ubuntu It covers things like basic firewall settings, NTP, and swap files. It also provides links to tutorials that show you how to set up common web applications. You may also want to check out this guide to learn how to enable fail2ban to reduce the effectiveness of brute force attacks. If you just want to explore, take a look at the rest of our community to find more tutorials.

Chapter 6 : How To Configure the Apache Web Server on an Ubuntu or Debian VPS | DigitalOcean

Tutorial: Configure Apache Web Server on Amazon Linux 2 to Use SSL/TLS Secure Sockets Layer/Transport Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on.

You then connect with sqlcmd to create your first database and run queries. Tip This tutorial requires user input and an internet connection. If you are interested in the unattended or offline installation procedures, see Installation guidance for SQL Server on Linux. Prerequisites You must have a Ubuntu To install Ubuntu on your own machine, go to http: You can also create Ubuntu virtual machines in Azure. Note At this time, the Windows Subsystem for Linux for Windows 10 is not supported as an installation target. Import the public repository GPG keys: Use the following command for SQL Server installations: Evaluation, Developer, and Express. Once the configuration is done, verify that the service is running: The following steps install the SQL Server command-line tools: Use the following steps to install the mssql-tools on Ubuntu. Import the public repository GPG keys. In this tutorial, you are connecting locally, so the server name is localhost. The user name is SA and the password is the one you provided for the SA account during setup. Tip If you later decide to connect remotely, specify the machine name or IP address for the -S parameter, and make sure port is open on your firewall. If successful, you should get to a sqlcmd command prompt: If you get a connection failure, first attempt to diagnose the problem from the error message. Then review the connection troubleshooting recommendations. Create and query data The following sections walk you through using sqlcmd to create a new database, add data, and run a simple query. Create a new database The following steps create a new database named TestDB. From the sqlcmd command prompt, paste the following Transact-SQL command to create a test database: Databases The previous two commands were not executed immediately. You must type GO on a new line to execute the previous commands: Insert data Next create a new table, Inventory, and insert two new rows. From the sqlcmd command prompt, switch context to the new TestDB database: GO Select data Now, run a query to return data from the Inventory table. From the sqlcmd command prompt, enter a query that returns rows from the Inventory table where the quantity is greater than

Chapter 7 : How to Setup a Complete Mail Server (Postfix) using 'SquirrelMail' (Webmail) on Ubuntu/Debia

This allows you to configure your web server in a way that makes sense for your application or website. Linode Guides & Tutorials contains a number of documents regarding the installation and maintenance of various web servers.

We will also install the phpLDAPadmin web-based management tool. Given the appropriate access, clients can search the directory, modify and manipulate records in the directory. OpenLDAP is efficient on both reading and modifying data in the directory. OpenLDAP servers are most commonly used to provide centralized management of user accounts. You can check out its status with: Basic Post-Installation Configuration The installation process installs the package without any configurations. To have our OpenLDAP server running properly, we need to do some basic post-installation configuration. Run the following command to start the configuration wizard. Answer these questions as follows: Omit LDAP server configuration: Enter your domain name like linuxbabe. You will need to set a correct A record for your domain name. You can also subdomains like directory. Enter your organization name like LinuxBabe. Enter the same password set during installation. BDB Berkeley Database is slow and cumbersome. Writes are x faster. So we choose MDB as the database backend. Do you want the database to be removed when slapd is purged? Copy and paste the following text at the end of the file. Replace your-domain and com as appropriate. It tells the client programs where to start their search in the directory. LDAP administrator search result search: If you use Apache The installation will put a configuration file phpldapadmin. Then text Nginx configurations. Configuring phpLDAPadmin We need to do some configurations just like we did with the command-line client. Line specifies that phpLDAPadmin will connect to localhost. Next, you can disable anonymous login. Go to line To disable it, you need to remove the comment character the two slashes and change true to false. When phpLDAPadmin first loads, it looks something like this. You will see the login dialog box. Once you log into phpLDAPadmin, you can manage this directory server.

Chapter 8 : Tutorials/Setting up a server â€“ Official Minecraft Wiki

calendrierdelascience.com team is determined to provide you with simple to follow Linux tutorials, various tips, tricks and programming guides as well as with GNU/Linux system administration tutorials in general to help you to learn Linux faster and use it with ease.

Before we get into it, lets talk about an overview. It is an enterprise Linux distribution that is built by Univention. It is their goal to simplify the access to applications and devices for organizations and Univention heavily uses Open Source software for that. Basically, this involves three core topics: A central identity management system An app store-like environment for applications And, of course, IT infrastructure and device management All this is brought together into one product called Univention Corporate Server. You can also imagine UCS as Android for servers. Like Android UCS offers a marketplace for apps. Univention calls it App Center. Because of the flexibility of UCS, most apps can be operated both on premises or in the cloud. UCS is used by a broad variety of organizations in very different industries ranging from just a few users until up to 30 million users in the directory service. The software packages are taken from the Debian project. Univention builds some packages on their own, because some packages like Samba or OpenLDAP are customized with patches or simply need a newer version than available in Debian stable. It consists of a tree of variable keys and their values that are used in configuration files and scripts. It allows to use the same variable, for example the LDAP base distinguished name, in different places and it is only defined once. With UCR a system administrator does not need to worry about missing settings spread over several configuration files. A value can be changed and is then committed to the relevant configuration files. System administrators are mostly interacting with UCS via the web-based management system. There they take care of the identity management with users, groups and roles and the infrastructure management like IP address leases, name resolution for systems. The UCS system itself is also managed this way and administrators update system packages or install new apps via the web-browser. System administrators usually deal with recurring tasks and they are simplified by the management system. Furthermore, the learning curve for enterprise Linux systems is lowered. The glue ingredients are software craftsmanship, creativity, Python, JavaScript and Dojo, Bash and a bunch of knowledge about Linux and various Open Source Software projects. The Core Edition comes full-featured and free of charge with community support. Enterprise subscription is also available including support and a longer maintenance of five to seven years for a major version. This installation uses the UCS virtual machine image for VirtualBox and walks through the single steps. Download VirtualBox and install it. Select location Customize keyboard, if needed Enter network configuration: Either choose to obtain an IP address automatically default or enter a static IP address. In this tutorial, used a static IP, because UCS system should take care of all the ip address handling. Select the first option. I want setup my own domain and I start with creating a new one. I can later add more systems to this new domain by selecting the second option during the setup. Furthermore, if an existing Active Directory service should be used, select option three. Enter the password for the root and Administrator account. The system needs to have a root password. I postpone the system activation to a later time and leave the other fields empty. Specify the name of the system in the Host settings. I just went with the proposed defaults. Here the system receives its name. You may already want to install additional components, like for example the Active Directory compatible domain controller. UCS will apply the settings. This can last several minutes and depends on the performance of your underlying virtualization host system. Finally the setup is completed. After finishing the setup wizard, the appliance greets with a welcome screen and announces what IP address should be used in the browser to access the UCS management system. This screen comes up after every reboot of the appliance and gently reminds where to reach the system. Heading to the address provided by the welcome page opens the UCS portal page. It looks quite empty yet and offers a login to the management system. The Administrator is the first administrative user having all the rights for the environment. With the first successful login, UCS welcomes the user with a short dialog and asks for the first feedback, if issues occurred during installation and setup. Each section reveals its own modules for different administrator tasks. Frequently used modules can be

put into the Favorites section. After UCS setup, the system should be extended by an additional app and ownCloud is my candidate. In order to use the App Center, the system has to be registered. Afterwards, I can continue with the installation. The registration has to be done only once. A look at the portal now shows some more tiles on it. It offers the login to ownCloud. Before a login with a usual user can be made, the user needs to be created. The admin user can login though with the given credentials shown after the installation. Provide at least a lastname, username and a password. By default, new users are enabled for ownCloud, as soon as the app is installed. If a new user shall not be able to login to ownCloud, the checkbox has to be removed in the Advanced settings section. Summary Univention Corporate Server UCS is very sophisticated operating system for identity and infrastructure management for organizations. The setup is straight forward and easy to make. I like the way how third party solutions extend the platform and that they are integrated with the identity management. This makes testing and even production operation very easy.

Chapter 9 : Getting Started with Amazon EC2 Linux Instances - Amazon Elastic Compute Cloud

Enter network configuration: Either choose to obtain an IP address automatically (default) or enter a static IP address. In this tutorial, used a static IP, because UCS system should take care of all the ip address handling.

Install the Apache web server. For step-by-step instructions, see Tutorial: If you plan to use your EC2 instance to host a public website, you need to register a domain name for your web server or transfer an existing domain name to your Amazon EC2 host. Numerous third-party domain registration and DNS hosting services are available for this, or you may use Amazon Route Note A self-signed certificate is acceptable for testing but not production. If you expose your self-signed certificate to the internet, visitors to your site are greeted by security warnings. This process may take a few minutes, but it is important to make sure that you have the latest security updates and bug fixes. Note The -y option installs the updates without asking for confirmation. If you would like to examine the updates before installing, you can omit this option. During installation, OpenSSL used this key to generate a self-signed host certificate, and you can also use this key to generate a certificate signing request CSR to submit to a certificate authority CA. Try running sudo ls -al inside the directory. You can call a certificate cert. Reboot your instance and reconnect to it. Because you are connecting to a site with a self-signed, untrusted host certificate, your browser may display a series of security warnings. Override the warnings and proceed to the site. All data passing between the browser and server is now encrypted. To prevent site visitors from encountering warning screens, you need to obtain a trusted certificate that not only encrypts, but also publicly authenticates you as the owner of the site. Obtain a CA-signed Certificate This section describes the process of generating a certificate signing request CSR from a private key, submitting the CSR to a certificate authority CA , obtaining a signed host certificate, and configuring Apache to use it. The difference is social, not mathematical. Each web browser contains a list of CAs trusted by the browser vendor to do this. When a browser connects to a web server over HTTPS, the server presents a certificate for the browser to check against its list of trusted CAs. If the signer is on the list, or accessible through a chain of trust consisting of other trusted signers, the browser negotiates a fast encrypted data channel with the server and loads the page. Certificates generally cost money because of the labor involved in validating the requests, so it pays to shop around. A list of well-known CAs can be found at dmoztools. A few CAs offer basic-level certificates free of charge. Underlying the host certificate is the key. As of , government and industry groups recommend using a minimum key modulus size of bits for RSA keys intended to protect documents through The default modulus size generated by OpenSSL in Amazon Linux 2 is bits, which means that the existing autogenerated key is suitable for use in a CA-signed certificate. An alternative procedure is described below for those who desire a customized key, for instance one with a larger modulus or using a different encryption algorithm. If you prefer to use your existing host key to generate the CSR, skip to Step 3. Optional Generate a new private key. Here are some sample key configurations. Any of the resulting keys work with your web server, but they vary in the degree and type of security that they implement. As a starting point, here is the command to create an RSA key resembling the default host key on your instance: To create a stronger RSA key with a bigger modulus, use the following command: To create a bit encrypted RSA key with password protection, use the following command: Important Encrypting the key provides greater security, but because an encrypted key requires a password, services depending on it cannot be auto-started. Each time you use this key, you need to supply the password "abcde" over an SSH connection. RSA cryptography can be relatively slow, because its security relies on the difficulty of factoring the product of two large two prime numbers. Keys based on the mathematics of elliptic curves are smaller and computationally faster when delivering an equivalent level of security. Here is an example: The commands would be as follows: Create a CSR using your preferred key. The example below uses custom. All of the fields except Common Name are optional for a basic, domain-validated host certificate.