Document to build a node on lonos

Step 1: Purchasing a plan

Website URL : https://www.ionos.com/servers/vps



Click on see servers to see the plans.



These are the plans available. The specifications for running a \$DAG node is 8 vCores CPU, 16 GB RAM and Disk space varies depending on the snapshots. We have to choose VPS XL here. Once you select this plan, you will be asked to fill in all your personal details and do the payment.

You can also place an order by calling to the customer support. Phone no - +1-484-254-5555 Once the payment is done, you will get the customer id details to your email id.

Step 2: Getting the details of root password

Go to my.ionos.com and give your customer id or email id and password to login to your account. Once you login you will see as below



Select IONOS VPS Linux XL

SS



You can see your vps here

e a	A CONTRACTOR OF THE OWNER OF THE						
	Type - Name -		Status	IP -	Size -	OS▼	Datacenter
0	😭 My VPS		•	_	vps 8 16 480	o Ubuntu 24.04	¢
1y '							On +
	,						
eat	ures						
î	Login Data:						
	Host:	65.38.96.90					
E.	User:	root					
N.	Initial Password:	View password					o
	Image:						
	Source:	IONOS Images					
	Operating System:	Ubuntu 24.04					

Click on the Radio button beside My VPS so that you can view User which is root and click on view password for password

Step3: Create a Firewall

10	NOS MENU~		${\bf Q}_{\rm c}$ Search for features, domains, and help	Ą	*	Ø Ę 4° L
(† 	Infrastructure Servers Images Network Firewall Policies Dublic ID	Servers		Last login: 04/03/2	025 12:03:16 from 49.207.206.73 (India) * * * * *	Recommended help topics > Overview: Server (VPS) > VPS: Getting Started > Using the Remote Console for Server Access (VPS Linux and VPS Windows) > Installing Pleak (VPS Windows) and VPS Linux A
0	Backup	Type * Name *	Status - IP -	Size * vps 8 16 480	OS - Datacenter -	 Important Security Information for Your Server
0	Management					

On the left side click on Firewall policies

Firewall Policies	14 🌣 😡
Create Delete	Filter 🔻

Click on firewall to create a firewall

Network	For security reasons, all incoming ports are closed by default.	
Firewall Policies Public IP	Firewall Policies	
Backup	Create firewall policy	x
Management	Name:	Summary
	DAG-Mainnet-Firewall	Name DAG-Mainnet-Firewall
Help 🖸	Configuration Action ~ Allowed IP - Protocol ~ Port(s) ~ Description ~	Configuration: Protocols / Ports
	Allow all O TCP V	Create
	Add Predefined Values	

Give the name of your choice and add the rules

Configuration

Incoming				
Action -	Allowed IP	Protocol	Port(s)	Description ~
Allow	All	ТСР	9000 - 9001	0 0
Allow	All	ТСР	9010 - 9011	0 0
Allow	49.207.206.73	ТСР	22	0 0

These are the rules to be added. To get your local ip address, go to **whatismyip.com** and paste your ip address

Properties		Assigned IP
Created on:	04/02/2025 13:16:32	
	(Assign

Click on Assign to add firewall to the vps

Step 4: Create an SSH Key pair using PuTTYgen

Open PuTTYgen			
😴 PuTTY Key Generator			? ×
<u>F</u> ile <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp			
Key No key.			
Actions			
Generate a public/private key pair			Generate
Load an existing private key file			Load
Save the generated key		Save p <u>u</u> blic key	<u>S</u> ave private key
Parameters Type of key to generate: <u>R</u> SA Number of <u>b</u> its in a generated key:	⊜ <u>e</u> cdsa	○ EdD <u>S</u> A	O SSH-1 (RSA) 4096

By default it will be 2048. Change the Number of bits in a generated key to 4096.

💽 I	PuTTY	Key Generator					?	\times
File	Key	Conversions	Help					
Ke	у							
P	lease g	enerate some ra	ndomness	by moving the mouse over	er the blank area.			
Ac	tions							
G	enerate	e a public/private	key pair			Gener	ate	
	and an	evisting private k	evfile				langer and a	
	Jau an	existing private k	eyme			LUat		
S	ave the	generated key			Save public key	Save priva	ate key	
Pa	ramete	rs						
Т	ype of I	key to generate:		- ECDSA				
N	umber	of bits in a denor	ated key:	ECDSA	EdDSA	4096	(134)	
IN	umber	or bits in a genera	ateu key.			4030		

Click on Generate and move the mouse around to complete the process

Eile Key Public key for pasting into OpenSSH authorized_keys file: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC9Pd1SLxLM7RIVkeLSEZFaXloLDIdEpHy86uhJAEn3xkFFUEUxRzB: nvWrNr4JEDVyu4uCSbcBcICNSsVRnoApLbDHVn2irbS4aDki6029deGTwq7hal/ZJkStN3DeD9/E0AVsW3SIFRhz 4zd080fKyLfk/YPbv4rsvllf/UViKnpjnnt4I3CG0gJzShDkWF7P6scEx5gYOaf9l6R0jWhMlw/DaueLk93qUZg1VAnrdhr LbD5M9wdfODbp/GQbZtCgIW6+v4+zOaTFBvFJydT2/7vittPM7Yd2l30GYKuGNbWAQfNakOdOdz4b/JMP Key fingerprint: ssh-rsa 4096 SHA256:5V0thHVun/anl7+cZ3hP+OtwE1PBEwml4E6LGbCfWtE Key passphrase: •••••••••••• Confirm passphrase: •••••••••• Actions •••••••••	zZnrl3m k5nK7X mVO18
Key Public key for pasting into OpenSSH authorized_keys file: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC9Pd1SLxLM7RIVkeLSEZFaXloLDIdEpHy86uhJAEn3xkFFUEUxRzB: nvWrNr4JEDVyu4uCSbcBclCNSsVRnoApLbDHVn2irbS4aDki6029deGTwq7hal/ZJkStN3DeD9/E0AVsW3SIFRhz 4zd080fKyLfk/YPbv4rsvllf/UViKnpjnnt4l3CG0gJzShDkWF7P6scEx5gY0af9l6R0jWhMiw/DaueLk93qUZg1VAnrdhr LbD5M9wdfODbp/GubZtCgIW6+v4+z0aTFBvFJydT2/7vittPM7Yd2l30GYKuGNbWAQfNakOd0dz4b/JMP Key fingerprint ssh-rsa 4096 SHA256:5V0thHVun/anl7+cZ3hP+OtwE1PBEwml4E6LGbCfWtE Key gomment: rsa-key-20250403 Key passphrase:	zZnrl3m ŀk5nK7X mVO18
Public key for pasting into OpenSSH authorized_keys file: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC9Pd1SLxLM7RIVkeLSEZFaXloLDIdEpHy86uhJAEn3xkFFUEUxRzB nvWrNr4JEDVyu4uCSbcBclCNSsVRnoApLbDHVn2irbS4aDki6029deGTwq7hal/ZJkSth3DeD9/E0AVsW3SIFRhz 4zd080fKyLfk/YPbv4rsvllf/UViKnpjnnt4l3CG0gJzShDkWF7P6scEx5gY0af9l6R0jWhMlw/DaueLk93qUZg1VAnrdhr LbD5M9wdfODbp/GQbZtCglW6+v4+z0aTFBvFJydT2/7vittPM7Yd2l30GYKuGNbWAQfNakOdOdz4b/JMP Key fingerprint ssh-rsa 4096 SHA256:5V0thHVun/anl7+cZ3hP+OtwE1PBEwml4E6LGbCfWtE Key gomment rsa-key-20250403 Key passphrase: ••••••••••• Actions ••••••••••	zZnrl3m k5nK7X mVO18
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC9Pd1SLxLM7RIVkeLSEZFaXloLDIdEpHy86uhJAEn3xkFFUEUxRzB nvWrNr4JEDVyu4uCSbcBcICNSsVRnoApLbDHVn2irbS4aDki6029deGTwq7hal/ZJkStN3DeD9/E0AVsW3SIFRhz 4zd080fKyLfk/YPbv4rsvllf/UViKnpjnnt4l3CG0gJzShDkWF7P6scEx5gY0af9l6R0jWhMlw/DaueLk93qUZg1VAnrdhr LbD5M9wdf0Dbp/GubZtCglW6+v4+z0aTFBvFJydT2/7vittPM7Yd2l30GYKuGNbWAQftNakOd0dz4b/JMP Key fingerprint ssh-rsa 4096 SHA256:5V0thHVun/anl7+cZ3hP+OtwE1PBEwml4E6LGbCfWtE Key comment rsa-key-20250403 Key passphrase:	zZnrl3m k5nK7X mVO18
Key fingerprint: ssh-rsa 4096 SHA256:5V0thHVun/anl7+cZ3hP+OtwE1PBEwml4E6LGbCfWtE Key comment: rsa-key-20250403 Key passphrase: ••••••••••••••••••••••••••••••••••••	
Key comment rsa-key-20250403 Key passphrase: ••••••••••••••••••••••••••••••••••••	
Key passphrase: •••••••••••••••••• Confirm passphrase: ••••••••••••• Actions	
Confirm passphrase:Actions	
Actions	
Generate a public/private key pair <u>G</u> enerat	e
Load an existing private key file	
Save the generated key Save public key Save private	e key
Parameters	
Type of key to generate:	
Number of <u>b</u> its in a generated key: 4096	SA)

Give the Key Passphrase of your own choice and Confirm Passphrase. After that save public key with name **id_rsa.pub** and private key with name **id_rsa** to your local computer.

DUTTY Koy Conorat	or			2 🗸	
	01			1 ^	
Eile Key Conversion Key Public key for pasting i Ssh-rsa AAAAB3NzaC1yc2EA nvWrNr4JEDVyu4uC9 4zd080fKyLfk/YPbv4r LbD5M9wdf0Dbp/G0	nto OpenSSH author AAADAQABAAACA bcBcICNSsVRnoAp svIlf/UViKnpjnnt4I3C0 bZtCgIW6+v4+zOaT	rized_keys file: QC9Pd1SLxLM7RIVke LbDHVn2irbS4aDki60 GOgJzShDkWF7P6scE FBvFJydT2/7vittPM7Y 56:5V0ttbHVup/apl7+c23	LSEZFaXIoLDIdEpHy86uhJ/ 29deGTwq7hal/ZJkStN3DeI x5gYOaf9l6R0jWhMlw/Daue d2l30GYKuGNbWAQfNakOc	AEn3xkFFUEUxRzBzZnrl3m D9/E0AVsW3SIFRhzk5nK7X eLk93qUZg1VAnrdhmV018 d0dz4b/JMP	
Key ingerprint. ssirisa 4050 St /2250.5V0III 1V0II/all/+C25IIF+OtwE FP DEWINHEDEGDCIWIE					
Key <u>c</u> omment rsa-key-20250403					
Key p <u>a</u> ssphrase:	•••••	•••••			
Confirm passphrase:	•••••	•••••			
Actions					
Generate a public/priv	ate key pair			Generate	
Load an existing privat	e key file			Load	
Save the generated ke	уy.		Save p <u>u</u> blic key	Save private key	
Parameters					
Type of key to generat	e: () <u>D</u> SA		⊖ EdD <u>S</u> A	⊖SSH-1(RSA)	
Number of <u>b</u> its in a ger	erated key:			4096	

Copy the Public key to paste it in the authorized_keys file in your vps server

<u>Step 5: Log-in to vps from root user and root password and paste the public key in</u> <u>authorized keys file</u>

🕵 PuTTY Configuration		?	\times
Category:			
	Basic options for your PuTTY ses	sion	
	Specify the destination you want to connect to		
Keyboard	Host <u>N</u> ame (or IP address)	Port	
Bell		22	
⊡-Window	Connection type:		
Appearance	OSH OSe <u>r</u> ial Other: Telnet		\sim
- Behaviour - Translation	Load, save or delete a stored session		
⊕ Selection	Saved Sessions		
Colours	Ionos-Mainnet		
Data	Default Settings	Load	
Proxy ⊕-SSH		Sava	5
Serial		Jave	=
- Telnet		Delete	•
SUPDUP			
	Close window on exit:		
	Always Never Only on cle	an exit	
About <u>H</u> elp	<u>O</u> pen	<u>C</u> ance	I

Give the ip address and name, save it

🔀 PuTTY Configuration			?	\times	
Category:					
Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Connection Pata Proxy SSH Serial Telnet Rogin SUPDUP	Data to Login details Auto-login username When username is not s Prompt Use s Terminal details Terminal-type string Terminal speeds Environment variables Variable Value	root pecified: system username (sake xterm 38400,38400	et) Adc Remc	1 >vve	>
About Help		Open	Cance	1	

Go to Connection->Data and give Auto-login username as root. After that click on session

🔀 PuTTY Configuration		?	×
Category:			
Session	Basic options for your PuTTY ses	sion	
Logging	Specify the destination you want to connect to		
Keyboard	Host Name (or IP address)	Port	
Bell		22	_
- Window	Connection type:		
 Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP 	OSSH ○Serial ○Other: Telne	t	\sim
	Load, save or delete a stored session Saved Sessions Ionos-Mainnet Default Settings Ionos-Mainnet	Load Save Delete	
	Close window on exit: Always Never Only on cle	an exit	
About Help	Open	Cancel	

🕵 PuTTY Configuration		? >	\times
Category:			
Session	Basic options for your PuTTY see	sion	
Logging	Specify the destination you want to connect to		
- Keyboard	Host <u>N</u> ame (or IP address)	Port	
Features	Connection type:	22	-
Appearance	Oserial Other: Telne	t ~	
···· Translation	Load, save or delete a stored session Saved Sessions Ionos-Mainnet]	
Data Proxy	Default Settings Ionos-Mainnet	Load	
		Sa <u>v</u> e	
Serial Telnet Rlogin SUPDUP		Delete	
	Close window on exit Always Never	ean exit	
<u>A</u> bout <u>H</u> elp	<u>Open</u>	<u>C</u> ancel	

Now Select Ionos-Mainnet and open it

Now click on save



Click on Accept



Give the root password which is in the Ionos My VPS section. Please refer Step 2 to get the password

😴 PuTTY Key Genera	ator				? ×
<u>F</u> ile <u>K</u> ey Con <u>v</u> ersio	ons <u>H</u> elp				
Key <u>Public key for pasting</u> ssh-rsa AAAAB3NzaC1yc2E nvWrNr4JEDVyu4u0 4zd080fKyLfk/YPbv4 LbD5M9wdfODbp/G	into OpenSSH authorized AAAADAQABAAACAQC9 SbcBclCNSsVRnoApLbD IrsvIlf/UViKnpjnnt4I3CGOg QbZtCgIW6+v4+zOaTFBv	I_keys file: IPd1SLxLM7RIVk DHVn2irbS4aDki6 JzShDkWF7P6sc FJyd12/7vittPM7	eLSEZFaXIoLDIdEpHy86uhJA 029deGTwq7hal/ZJkStN3DeD Ex5gYOaf9l6R0jWhMlw/Dauel /d2l30GYKuGhbWAQfNakOd(En3xkFFUEUxRzBz 9/E0AVsW3SIFRhzł k93qUZg1VAnrdhm dz4b/JMP	Znrl3m t5nK7x VO18
Key fingerprint	ssh-rsa 4096 SHA256:5	/0thHVun/anl7+c2	3hP+OtwE1PBEwml4E6LGbCf	WtE	
Key <u>c</u> omment:	rsa-key-20250403				
Key p <u>a</u> ssphrase:	•••••	••••			
Confirm passphrase:	•••••	••••			
Actions					
Generate a public/pr	vate key pair			<u>G</u> enerate	
Load an existing priv	ate key file			<u>L</u> oad	
Save the generated	(ey		Save p <u>u</u> blic key	<u>S</u> ave private	key
Parameters					
Type of key to gener	ate: <u>D</u> SA	⊖ <u>e</u> cdsa	⊖ EdD <u>S</u> A	⊖ SSH- <u>1</u> (RS	ŝA)
Number of <u>b</u> its in a g	enerated key:			4096	

Copy the public key from PuttyGen and paste it in the authorized_keys file on the VPS

How to access authorized keys file and paste the ssh public key

On putty, go to the directory .ssh

🚰 root@ubuntu: ~			-		×		
System load: 0.0 Usage of /: 0.3% of 463.92GE Memory usage: 1% Swap usage: 0%	Processes: B Users logged in: IPv4 address for	160 Document was last save ens6: 65.38.9	d: Just now 9 . 16				
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.							
https://ubuntu.com/engage/secure-kubernetes-at-the-edge							
Expanded Security Maintenance fo	or Applications is n	ot enabled.					
0 updates can be applied immedia	ately.						
Enable ESM Apps to receive additional future security updates. See https://ubuntu.com/esm or run: sudo pro status							
The list of available updates is more than a week old. To check for new updates run: sudo apt update							
Last login: Sat Apr 5 13:35:39 root@ubuntu:~# cd ~/.ssh	2025 from 49.207.22	3.150					
Command: cd ~/.ssh							

After that open the authorized_keys file



Command: nano authorized_keys and press <ENTER>

🚰 root@ubuntu: ~/.ssh	—		\times
GNU nano 7.2 authorized keys *			
Q== rsa-key-20250405			
G Help ^{^O} Write Out [^] W Where Is ^{^K} Cut ^{^T} Execute	$^{\rm C}$ L	ocation	
X Exit ^R Read File ^\ Replace ^U Paste ^J Justify	^/ Go	o To Li	ne

Now right click on the mouse to paste the public key which is already copied previously, so that it will be pasted in the authorized_keys file

Command to save and Exit from the Nano Editor:

鍲 root@ubuntu: ~/.ssh				_		×
GNU nano 7.2	a	uthorized_keys *				
<q== rsa-key-2025040<="" td=""><td>5</td><td></td><td></td><td></td><td></td><td></td></q==>	5					
File Name to Write:	authorized keys					
'G Help	M-D DOS Format	M-A Append	M-B Ba	ckup F	ile	
^C Cancel	M-M Mac Format	M-P Prepend	^T Bro	wse		

Command to Save: Ctrl+O

🚰 root@ubuntu: ~/.ssh	-		Х
GNU nano 7.2 authorized keys			
<pre><g== pre="" rsa-key-20250405<=""></g==></pre>			
[Wrote 1 line]			
AG Help AQ Write Out AW Where Is AK Cut AT Execute	^C LO	cation	
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify	^/ Go	To Lin	e

Press <ENTER>



Ctrl+X will bring back the screen to the terminal. Please close this session.

Step 6: Access the node from putty with ssh keys

🔀 PuTTY Configuration		? ×					
Category:							
Session	Basic options for your PuTTY session						
Logging	Specify the destination you want to connect to						
Keyboard Bell	Host Name (or IP address)	Port 22					
- Window	Connection type:						
- Appearance - Behaviour	SSH Serial Other: Telne	et ~					
···· Translation ···· Selection ···· Colours	Saved Sessions						
Data Proxy	Default Settings	Load					
	E	Save					
Telnet Rlogin SUPDUP		Delete					
	Close window on exit Always Never Only on cl	ean exit					
About Help	Open	Cancel					

Click on Ionos-Mainnet



Go to Connection->SSH->Auth->Credentials and Browse the ssh private key file(id_rsa) which is stored in your local computer

🔆 PuTTY Configuration		? ×	
Category:			
Session	Basic options for your PuTTY see	ssion	
	Specify the destination you want to connect to		
Keyboard	Host <u>N</u> ame (or IP address)	<u>P</u> ort	
Bell		22	
Features	Connection type:		
Appearance	OSH ○Se <u>r</u> ial ○Other: Telne	t ~	
Behaviour			
Translation	Load, save or delete a stored session		
	Sav <u>e</u> d Sessions		
Data	Default Settings	beol	
Proxy	Ionos-Mainnet		
SSH		Sa <u>v</u> e	
Kex			
Ciphor		Delete	
Credentials			
GSSAPI	Close window on e <u>x</u> it:		
TTY	○ Always ○ Never ○ Only on cle	ean exit	
X11			
<u>A</u> bout <u>H</u> elp	<u>O</u> pen	<u>C</u> ancel	

Click on Session and Save.

😵 PuTTY Configuration		?	×
Category:			
Session	Basic options for your PuTTY ses	sion	
E- Terminal	Specify the destination you want to connect to		
Keyboard Bell	Host Name (or IP address)	Port 22	
- Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Connection - Data	Connection type: SSH Serial Other: Telnet		~
	Load, save or delete a stored session Saved Sessions Default Settings	Load	
Proxy ⊕-SSH	lonos-Mainnet	Save	•
Senai Telnet Rlogin SUPDUP		Delet	e
	Close window on exit Always Never Only on cle	an exit	
About Help	Open	Cance	əl

Click on Ionos-Mainnet and click on Open



Give the passphrase and login

NOTE: No need of Step 7, if you are building a node first time as you don't have p12 file

New Site	Session	
	<u>F</u> ile protocol:	
	SFTP	~
	<u>H</u> ost name:	Po <u>r</u> t number:
		22
	User name:	Password:
	<u>S</u> ave ▼	A <u>d</u> vanced

Step	7:	Configuring	WinSCP	and	copying	the	p12	file to	VPS	

Open Winscp

<u>ss</u>			
🔁 Login			- 🗆 X
New Site	Session File protocol: SFTP Host name: User name: root Save	Password:	Po <u>r</u> t number: 22 - Advanced
Tools Manage	🔁 Login	Clos	se Help
Show Login dialog on startup and when	the last session is closed		

Give your VPS ip address in Host name and User name as root and click on Advanced drop down symbol

Advanced Site Settings		?	×
Environment Directories Recycle bin Encryption SFTP Shell Connection Proxy Tunnel SSH Key exchange Authentication Bugs Note	 Bypass authentication entirely Authentication options Attempt authentication using Pageant Attempt 'keyboard-interactive' authentication Respond with a password to the first prompt Authentication parameters Allow agent forwarding Private key file: C:\Users\saket\OneDrive\Desktop\Ionos-Mainnet\id_rsa.ppk Display Public Key Tools Certificate to use with the private key: 		
	GSSAPI Attempt GSSAPI authentication Allow GSSAPI credential delegation		
Color 🔻	OK Cancel	He	lp

Click on Authentication and browse the private key file(id_rsa) which is saved in your local computer and click on OK

🔁 Login		-
New Site	Session <u>F</u> ile protocol: SFTP <u>H</u> ost name: <u>U</u> ser name: root <u>Save</u>	Port number: 22 2 Password: Advanced ▼
<u>I</u> ools ▼ <u>M</u> anag	Ie and when the last session is closed	Login 🔽 Close Help

Click on Save

New Site	Session
	<u>File protocol:</u>
	SFTP ~
	Save session as site ? × Port number:
	Site name:
	root@
	Folder:
	lonos-Mainnet ~ A <u>d</u> vanced
	Save password (not recommended)
	Create desktop shortcut
	OK Cancel Help
Tools T	

Give folder name of your choice. I have given lonos-Mainnet

📫 New Site	Session	
lonos-Mainnet	Eile protocol:	
root@	SFTP	
n an	<u>H</u> ost name:	Po <u>r</u> t number:
	<u>U</u> ser name:	Password:
	root	
	Edit	Advanced
		Auvalicediii
	大きなのからのないないのないの	
		annand and and and and and and and and a

You can see in the left as above. Now click on Login

Warning

	Continue connecting to an unknown server and add its host key to a cache?
	The host key is not cached for this server: (port 22)
	You have no guarantee that the server is the computer you think it is.
	The ssh-ed25519 key fingerprint is: ssh-ed25519 255 OneHmZqWfITeNY+CNORRagc/ZhxqGqNMBXsnQzvNLHc
	If you trust this host, select Accept to add the key to WinSCP's cache and carry on connecting.
	select Connect Once. If you do not trust this host, select Cancel to abandon the connection.
	Copy key fingerprints to clipboard
	Accept Cancel Help
Click o	n Accept
Key pas	ssphrase – Ionos-Mainnet/root@
<u></u>	Searching for host Connecting to host Authenticating Using username "root". Authenticating with public key "rsa-key-20250405".

Passphrase for key 'rsa-key-20)250405': ●●		
	ОК	Cancel	<u>H</u> elp

Give Passphrase and click OK

? ×

🗟 Ionos-Mainnet – Ionos-	Mainnet/roo	t@65.38.99.16 – WinSC	р Р					-		×
Local Mark Files Comm	ands Tabs (Options Remote Help	0							
🕂 🚼 😰 Synchronize	5 🥐 [🔁 🔅 🚰 Queue	• • Transfer Settings Default		• <u> </u> •					
📮 Ionos-Mainnet/root@	×	🛛 🔛 New Tab 🔻								
📕 Desktop 🔹 Ґ	• 🝸 •	🔶 🔹 🔶 🔹 🚺	i 🏫 🕄 💺 📰 •	= root	• 📁 • 🝸	• •	🔸 📲 🔁 🏫 🕄	🔒 🚉 Find Files	1. III	-
Upload 👻 📝 Edit	· × 🖌	Properties 👻 🎽	New 🕶 🛨 🚽 💙	Dow	nload 👻 📝 Ed	it • 🗙 📈	🕞 Properties 👻 💕	New -		
C:\Users\saket\OneDrive\De	sktop\lonos-	Mainnet\		/root/						
Name	Size 3 KB 1 KB 2 KB	Type Parent directory PuTTY Private Key PUB File Personal Informati	Changed 05-04-2025 20:38:10 05-04-2025 19:35:09 05-04-2025 19:35:27 06-07-2023 20:08:20	Name		Size	Changed 05-04-2025 05:25:21	Rights rwxr-xr-x	Owner root	
) B of 4.58 KB in 0 of 3				0 B of 0 B	in 0 of 0				8	hidden
								SFTP-3	0:14	4:56

Left side pane shows folders of your local computer, right side shows the directories of your VPS. Drag and drop your p12 file if you are rebuilding your node with existing p12 file.

🗟 Ionos-Mainnet – Ionos-	Mainnet/root	t@65.38.99.16 - WinSC	P					-		\times
Local Mark Files Comma	ands Tabs (Options Remote Help	0							
🖶 🚼 🧽 Synchronize	🗩 🥜 🚺	🔁 🔅 🚰 Queue	• Transfer Settings De	fault	- 🥘 -					
💻 Ionos-Mainnet/root@	×	🗳 New Tab 🔻								
🔜 Desktop 🔹 📁	- 🕎 -	← • → • 🔁 🖪	🏫 Ġ 💺 💷 -		🖿 root 🔹 🕶 🚰 🕶 🍸	• • - •	-> - 🗀 🗖 🏠	G 🚉 Find Files	- 📜 🖸	-
🙀 Upload 👻 📝 Edit	• × 🖌 [👌 Properties 👻 📫	New - 🛨 🚽 💙		Download 👻 📝 Edi	it - 🗙 📈	Properties 👻 🎽	New -	V	
:\Users\saket\OneDrive\De	sktop\lonos-	Mainnet\			/root/					
Name	Size 3 KB 1 KB 2 KB	Type Parent directory PuTTY Private Key PUB File Personal Informati	Changed 05-04-2025 20:38:10 05-04-2025 19:35:09 05-04-2025 19:35:27 06-07-2023 20:08:20		Name	Size	Changed 05-04-2025 05:25:21 06-07-2023 20:08:20	Rights rwxr-xr-x rw-rr-	Owner root root	τ
B of 4.58 KB in 0 of 3					0 B of 1.00 KB in 0 of 1			SFTP-3	8 0:0	3 hidde)0:51

Copied p12 file from local computer to /root/ directory on VPS

Step 8: Install nodectl

You can get the latest release of nodectl from

https://github.com/StardustCollective/nodectl/releases



Copy the latest nodectl from the above link and run on putty

🚰 root@ubuntu: ~					_		\times
-release-asset- ithm=AWS4-HMAC-s st-1%2Fs3%2Faws hature=f5cab4df medHeaders=host x86_64_2404&res esolving object 99.110.133,185 Connecting to ob 199.110.133]:44 HTTP request set Length: 3006731 Saving to: `/us	2e65be/6113 SHA256&X-Am 4 request&X 15cb4b3950f t&response- sponse-cont ts.githubus .199.109.13 bjects.gith 3 connec nt, awaitir 2 (29M) [ag r/local/bir	43043/cc56ad z-Credential (-Amz-Date=2) 22242b2dade content-disp cent-type=ap sercontent.cc 3, 185.199. nubusercontent ted. ag response. pplication/od (nodect1'	a7d-6fe7-499 l=releaseass 250405T1426 a7a5a643012c bosition=atta blication%2F bm (objects.c 108.133, ht.com (objects.c 200 OK ctet-stream]	1-86fd-536c62b2445 stproduction%2F202 592&X-Amz-Expires= 6ff8970c83685fb534 achment%3B%20filen octet-stream githubusercontent.	2?X-A 50405 300&X 8f8c& ame%3 com). ent.c	mz-Alo %2Fus -Amz- X-Amz Dnode 18: om) 1	gor -ea Sig ctl 5.1 85.
nodectl	100%[=		=====>] 28	3.67M 52.6MB/s	in O	.5s	
2025-04-05 14:2° 312]	7:00 (52.6	MB/s) - '/u	sr/local/bin/	/nodectl' saved [3	00673	12/30	067
No installation Creating log of VERSION MA v2.16.0 2	on found or directory f AJOR	log path ne for nodectl MINOR 16	PATCH 0	CONFIG v2.1.1			

Nodectl installed

Step 9: Install tessellation

Command to install tessellation: sudo nodectl install



Select node type

Proot@ubuntu: ~	—		\times
the <enter></enter> key to accept said value.			
n stands for no yes			
IMPORTANT nodectl was designed to run on a terminal session with a black background setting. Default terminal emulators with a white background may experience some 'hard to see' contrasts. It is recommended to change the preferences on your terminal [of choice] to run with black background.	ıa		
QUICK INSTALL nodectl's installer provides a quick install option that utilizes all the recommended default settings. This allows for a streamlined process, requiring minimal input from the future No Operator.	de		
Alternatively, you can choose a customization mode, step- by-step installation, where nodectl will ask you questions and explanations for the necessary elements to customize the installation of your node.	provid	le	
Install using quick install option? [y]:			

Give y

🚰 root@ubuntu: ~
= CONSTELLATION NETWORK HYPERGRAPH = = INSTALLATION REQUEST = = TESSELLATION VALIDATOR NODE =
Code Name: Princess Warrior
NOTE
befault options will be enclosed in [] (brackets). If you want to use the value defined in the brackets, simply hit the <enters accept="" key="" said="" th="" to="" value.<=""></enters>
n stands for no years
IMPORTANT nodectl was designed to run on a terminal session with a black background setting. Default terminal emulators with a
QUICK INSTALL REQUESTED
Even though this is the recommended options, nodectl will use all recommended settings without prompting for confirmations, be sure this is acceptable before continuing with this setting.
This includes removal of existing Tessellation and moderni service, p12, and other configuration files if present.
A few mandatory entries may be necessary; hence, nodectl will now prompt a series of questions before proceeding with the installation. If these options were already entered through the command line interface (CLI), the corresponding questions will be skipped.
nodectl quick install will not offer detailed explanation for various prompt requests, please use the normal installation or read the documentation. https://docs.constellationnetwork.io/validate/ WARNING for about to turn this VFS or Server into a Constellation Network validator node Are you sure you want to continue this installation? [y]:



ð	root@ubuntu: ~
	= CONSTELLATION NETWORK HYPERGRAPH = = INSTALLATION REQUEST = = TESSELLATION VALIDATOR NODE =
	Code Name: Princess Warrior
	nodectl installing [preparing] Obtain Install Parameters preparing
	Please choose which Hypergraph or metagraph you would like to install on this server:
	HYPERGRAPH or METAGRAPH predefined choices
	 mainnet [HyperGraph] integrationnet [HyperGraph] testnet [HyperGraph] dor-metagraph-mainnet [metagraph]
	Q)uit
	KEY PRESS an option

Select your choice



If you are building your node for first time, it should be n, else y



If you are rebuilding your node with existing p12 file, It will show as above. Else this is not shown



Enter nodeadmin password of your choice with minimum 10 characters



If you are installing node for first time, please give a p12 passphrase of your choice.

If you are installing node with an already existing p12 file, give the same passphrase as previous one



After installation completes, you will find this screen. Copy the NODE ID and give it to your Team Lead if you have built node for the first time

Step 10: Accessing the server after installation of tessellation

After installation of tessellation, root access will be disabled. We can access the node only with **nodeadmin**

🕵 PuTTY Configuration					?		\times
Category:							
 Session Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Connection Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP 	Login o Auto-I When O Pro Termir Termi Termi Cenviro Varial Value	Da details ogin username is sompt O nal details inal details inal speeds inment variablible	e not speci Jse syste	d to the server nodeadmin fied: m username (s xterm 38400,38400	saket)	Add	/e
About H	elp			Open	C	ancel	

Got to putty and change the Auto-login username to nodeadmin, Click on session and save it. Login to the server.

🚰 65.38.99.16 - PuTTY							
J Using username "nodeadmin". Authenticating with public key "rsa-key-20250405" Passphrase for key "rsa-key-20250405": Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)							
<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/pro</pre>							
System information as of Mon Apr	7 05:31:09 UTC 2025						
System load: 0.14 Usage of /: 2.4% of 463.92GB Memory usage: 2% Swap usage: 0%	Processes: 186 Users logged in: 1 IPv4 address for ens6: 65.38.99.16						
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.							
https://ubuntu.com/engage/secure	https://ubuntu.com/engage/secure-kubernetes-at-the-edge						
Expanded Security Maintenance for A	pplications is not enabled.						
160 updates can be applied immediat 60 of these updates are standard se To see these additional updates run	ely. curity updates. : apt listupgradable						
Enable ESM Apps to receive additional future security updates. See https://ubuntu.com/esm or run: sudo pro status							
Last login: Mon Apr 7 05:31:10 202 Torrunna command as administrator See "man sudo_root" for details"	5 from 49.207.232.241 nser root // // // // // // // // // // // // //						
nodeadmin@ubuntu:~\$ sudo nodectl up	grade_vpsni						

After logging in to the server, do security updates with the nodectl command "sudo nodectl upgrade_vps -ni"



While the security updates are running, if this screen pops up, then press <Tab> key on your laptop, so that <Ok> will be highlighted on the screen, then press <ENTER>



When security updates complete, sometimes it will reboot the server if needed. You can see this screen. The session gets disconnected. Wait for 2-3 mins and login back using Putty.

Step 11: Run Starchiver script to download all the snapshots and do a restart to join the cluster

Login back to the server from putty

🚰 65.38.99.16 - PuTTY				
g ^a Using username "nodeadmin". g ^a Authenticating with public key "rsa-key-20250405" g ^a Passphrase for key "rsa-key-20250405": Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-57-generic x86_64)				
<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/pro</pre>				
System information as of Mon Apr 7 05:38:55 UTC 2025				
System load:0.38Processes:188Usage of /:2.4% of 463.92GBUsers logged in:0Memory usage:2%IPv4 address for ens6:65.38.99.16Swap usage:0%				
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.				
https://ubuntu.com/engage/secure-kubernetes-at-the-edge				
Expanded Security Maintenance for Applications is not enabled.				
0 updates can be applied immediately.				
Enable ESM Apps to receive additional future security updates. See https://ubuntu.com/esm or run: sudo pro status				
Last login: Mon Apr 7 05:38:56 2025 from 49.207.232.241 nodeadmin@ubuntu:~\$ sudo nodectl execute_starchiver -p dag-10restart				

Command: sudo nodectl execute_starchiver -p dag-I0 -restart

- The session should be connected until the execution of this script completes

- After execution of the above script, all the snapshots will be downloaded and the node gets restarted to join the cluster. L0 will initially go to DownloadInProgress state followed by Ready state on L0 and L1

- Check the status after few mins using the command **sudo nodectl status**, the node should show Ready/Ready state



If L1 is in ReadytoJoin state, issue the command **sudo nodectl join -p dag-l1** on the terminal

Congratulations!!!

You can always refer the constellation docs for granular level information on running a node created by our one and only great Netmet <u>https://docs.constellationnetwork.io/run-a-node</u>