Rocket.Chat + Nextcloud

Collaboration Suite by Code Creator | Customer Instructions | Version 6.3

APPLICATIONS	DEPLOYMENT
Rocket.Chat messaging + Nextcloud file collaboration	Ubuntu 26.04 LTS EC2 AMI • HTTPS using the instance public IPv4 address

> **V6.3: TRUSTED HTTPS - NO DOMAIN REQUIRED**
>
> This release obtains a trusted HTTPS certificate for the EC2 public IP. Use HTTPS for setup and sign-in; do not use the older HTTP application URLs. Allow TCP 443 for certificate issuance and renewal.

1. Before you begin

Launch an EC2 instance from the AWS Marketplace product, using an EC2 key pair you control. Choose an instance size and storage capacity appropriate for your workload. For browser access, use the instance public IPv4 address; private-only networking requires an appropriate private access path.

Configure the EC2 security group. Restrict SSH and application access to the smallest practical source ranges. TCP 443 must be reachable publicly for automated certificate validation and renewal.

TCP PORT	PURPOSE	RECOMMENDED INBOUND SOURCE
22	SSH administration	Administrator IP /32
443	Trusted HTTPS welcome page; certificate validation/renewal	0.0.0.0/0 (and ::/0 only if IPv6 configured)
3000	Rocket.Chat over HTTPS	Your users / office IP ranges
8080	Nextcloud over HTTPS	Your users / office IP ranges
80	Legacy HTTP welcome page (optional; unencrypted)	Closed, or restricted to administrator IP

Do not expose MongoDB (27017), MariaDB (3306), Redis (6379), or internal Docker services to the public internet. Do not treat HTTP port 80 as a secure sign-in address.

2. Connect to the new instance

1. In the EC2 console, confirm the instance is Running and its EC2 status checks have passed. The applications and the initial HTTPS certificate can need several additional minutes.
2. For SSH, sign in as ubuntu using your selected EC2 private key. Example:

```
ssh -i /path/to/your-key.pem ubuntu@YOUR_PUBLIC_IP
```

Windows PuTTY users can connect as ubuntu with the matching .ppk private key.

3. Review your instance-specific startup/access information:

```
sudo cat /root/FIRST_LOGIN.txt
```

This file is generated on first boot. Keep its contents private. Replace YOUR_PUBLIC_IP with the EC2 instance public IPv4 address.

SERVICE	SECURE BROWSER ADDRESS
Welcome page	https://YOUR_PUBLIC_IP/
Rocket.Chat	https://YOUR_PUBLIC_IP:3000/
Nextcloud	https://YOUR_PUBLIC_IP:8080/

3. Complete Rocket.Chat setup

1. Open https://YOUR_PUBLIC_IP:3000/ using the browser. Wait for the initial workspace wizard if startup is still in progress.
2. Create the organization administrator using a strong, unique password and monitored email address; store credentials in your password manager.
3. Enter organization details and complete Rocket.Chat Cloud workspace registration if prompted. Email verification or a registration token may be necessary.
4. Sign in, create a test channel, send a message, and refresh to confirm the message remains available.

Some Rocket.Chat cloud-connected features may require registration and external connectivity.

4. Complete Nextcloud setup

> **IMPORTANT: NEXTCLOUD MAY TAKE SEVERAL MINUTES TO START**
>
> After first launch or reboot, Nextcloud does not necessarily open immediately. A temporary loading page, connection error, or 502 Bad Gateway may appear while it initializes. Wait several minutes, then refresh. Do not reinstall or repeatedly reboot just because the login page is not ready.

1. Open https://YOUR_PUBLIC_IP:8080/ and allow startup to finish. On a brand-new AMI, the initial setup screen is expected.
2. Create the first Nextcloud administrator account with a unique password. Save it securely.
3. MariaDB and Redis are configured internally. If unexpected manual database configuration is requested, inspect service status rather than guessing credentials or changing the database type.
4. Finish setup, open Files, then upload and download a small, non-sensitive test file.

5. Security steps before production use

- Use the trusted HTTPS endpoints above for all passwords and data. Leave TCP 443 reachable so Caddy can issue and renew the public-IP certificate.
- Limit access to HTTPS ports 3000 and 8080 to intended users. Keep SSH restricted, close unused HTTP port 80, and never expose database ports.
- V6.3 enables MongoDB authentication; retain the built-in database/network isolation and do not publish its port.
- Review application accounts, password policies, updates and monitoring. Follow your organization's information security requirements.
- Back up Nextcloud files together with its MariaDB database; separately back up Rocket.Chat/MongoDB. Practice a restore before relying on the system for important data.

> **PUBLIC IP AND CERTIFICATE RENEWAL**
>
> Let's Encrypt public-IP certificates are short-lived (160 hours, about 6 days). This image configures automatic Caddy renewal; successful renewal depends on an accessible TCP 443 endpoint and functioning network. If the instance public IP changes, a new certificate must be issued and access may be briefly interrupted. A stable Elastic IP can reduce address changes.

6. Common server commands

Run these from the normal ubuntu SSH session. They inspect state without resetting data or revealing passwords.

TASK	COMMAND
All containers	sudo docker ps --format "table {{.Names}}\t{{.Status}}"
Rocket.Chat logs	sudo docker logs --tail 100 codecreator-collab-rocketchat-1
Nextcloud logs	sudo docker logs --tail 100 codecreator-collab-nextcloud-1
HTTPS state	sudo codecreator-collab-ip-tls status
First-boot state	sudo systemctl status codecreator-collab-firstboot --no-pager
First-boot logs	sudo journalctl -u codecreator-collab-firstboot -n 50 --no-pager

CAUTION: Do not run docker compose down --volumes or Docker volume cleanup commands. They can permanently delete chat databases, Nextcloud files, certificate state, and credentials.

7. Basic troubleshooting

SYMPTOM	WHAT TO CHECK
Welcome page unavailable	Use https://YOUR_PUBLIC_IP/; confirm instance state, TCP 443 security-group rule, and first-boot status.
Rocket.Chat unavailable	Allow startup to finish; check HTTPS port 3000, container health, and Rocket.Chat logs.
Nextcloud unavailable / 502	Wait several minutes after launch or reboot and refresh; then inspect HTTPS port 8080 and Nextcloud logs.
Certificate warning or TLS failure	Confirm current public IPv4, TCP 443 reachable for certificate issuance/renewal, and Caddy container status. Do not bypass browser certificate warnings.
No first-login file	Check cloud-init and first-boot service: sudo systemctl status codecreator-collab-firstboot --no-pager
Public IP changed	Use the new public IPv4 address; allow time for IP refresh/new certificate issuance; consider an Elastic IP.
Nextcloud untrusted-domain message	Verify you are using the current instance IP in the URL; review Nextcloud trust/proxy configuration. Do not disable host validation.

8. Important operational notes

- No domain name or DNS setup is required for the public-IPv4 HTTPS launch path. EC2 instance, security group, and current IP still determine reachability.
- Each fresh customer launch generates instance-specific credentials and initializes new data volumes. Do not share /root/FIRST_LOGIN.txt or any setup secrets.
- Docker Compose, Caddy, Nginx, MongoDB, MariaDB, Redis and NATS support the packaged applications. Keep internal services isolated.
- AWS infrastructure, storage, Elastic IP (if used), outbound traffic, and third-party software/service costs are governed by the customer's own arrangements.

Reference: Let's Encrypt public-IP certificates - letsencrypt.org/2026/01/15/6day-and-ip-general-availability/ | AWS Marketplace AMI guidance - docs.aws.amazon.com/marketplace/latest/userguide/best-practices-for-building-your-amis.html