Upgrading from Jama Connect traditional to KOTS

Jama Connect is a Linux-based application that runs on Docker containers and uses Replicated software to "orchestrate" deploying applications. The current version of Jama Connect uses Replicated KOTS, while older versions use traditional Replicated software. The process of upgrading Jama Connect from traditional to KOTS includes planning, preparing your environment, and installing the software.

Upgrade scenarios

Upgrade with new servers (recommended) — This recommended scenario uses new application and database servers to support your KOTS Replicated environment. It requires you to:

- Copy targeted data from the existing application server into the new environment.
- Restore a backup of your current database to the new database server.

While this scenario results in the temporary overhead of supporting two separate environments, it comes with less risk of unwanted downtime.

Upgrade with existing servers — This scenario reuses the current application and database servers from your traditional Replicated environment. This scenario:

- Requires you to uninstall elements of the traditional Replicated platform before you can install the KOTS Replicated platform.
- Can cause significant maintenance downtime. Make sure to inform your users of this maintenance window. Also have an emergency plan in place to revert back to the traditional Replicated environment if necessary.

Before you upgrade

- Contact your Customer Success Manager to request a KOTS internet or airgap license.
- Choose the upgrade scenario that works best for your organization. Whichever scenario you choose, expect production downtime while the new instance is configured. Best to upgrade during off hours.
- Follow the instructions in the planning [2] and preparing [8] sections to ensure a successful upgrade.

Components and what they do

Replicated KOTS — A container-based platform for easily deploying cloud native applications inside customers' environments, providing greater security and control. The KOTS Admin Console is the interface for installing, configuring, and administering the KOTS deployment of the Jama Connect application and required services. See https://www.replicated.com/ for details.

Docker containers — A standalone executable package of software that includes code, runtime, system tools, system libraries, and settings. See https://www.docker.com/resources/what-container/ for details.

Jama Connect KOTS license — Contact your Customer Success Manager to request a KOTS license. Save the license file to a location you can access easily; you will need it when installing Jama Connect.

For more information about KOTS, see https://www.replicated.com/blog/announcing-kots/

NOTE
Replicated KOTS is the only supported platform for Jama Connect 9.0 and later. To upgrade Jama Connect traditional to KOTS, see Upgrade from Jama Connect traditional to KOTS workflow [2].

Workflow for upgrading from traditional to KOTS

Whether your environment is internet-enabled or airgapped, the upgrade process consists of three stages: planning, preparation, and installation.

Review the system and server requirements for your environment, then follow the instructions for each stage.

1 Plan

- Request a KOTS license
- Run the KOTS preflight installation checks
- Preserve data assets and tenant.properties file
- Review system requirements
- Calculate resource sizing and requirements for application and database servers
- Record existing settings for traditional Admin Console

2 Prepare

- Back up all your data
- Prepare application and database servers
- Install and configure database
- Configure memory settings for Elasticsearch

3 Install

- Install KOTS software
- Provision your tenant in Jama Connect KOTS
- Create a Replicated Snapshot

For this component...	Follow these instructions
MySQL	Install and configure MySQL [13]
Microsoft SQL	Install and configure Microsoft SQL Server [14]
Internet	Install KOTS software (internet) [18]
Airgap	Install KOTS software (airgap) [19]
Local Elasticsearch	Included by default
Remote Elasticsearch	Configure dedicated Elasticsearch nodes [17]

Planning your upgrade to KOTS

Before you upgrade from traditional to KOTS, make sure you have everything you need according to your type of installation.

Important considerations

- We recommend that you use a new application server and database server. Once the KOTS Replicated environment is installed successfully, the traditional Replicated environment can be removed.
- If you plan to reuse the existing application server and database server when upgrading:
  - Make sure you pay careful attention to resource sizing. System requirements for the KOTS Replicated platform are different from the traditional Replicated platform.
  - This scenario requires that you uninstall the traditional Replicated platform, resulting in potential unwanted downtime.

What you need

All environments	• The KOTS license file (submit a request to your Customer Success Manager).
	• Run the KOTS preflight installation checks [3] to ensure servers and settings are configured correctly.
	• Record the size of existing data assets and database for application and database server requirements and resource sizing. To check the current assets size, run the following command from the application server command line:
	`sudo du -shc /data/contour/*`
	• Record the existing settings from your traditional Replicated Admin Console. You can find the settings in the support bundle (under /daemon/replicated/app-config.json). These settings are used to configure Jama Connect after the upgrade to Jama Connect KOTS.
	• An application server with the necessary preparation [6] and sizing requirements [6].
	• A database server with the necessary preparation [12].
	• Supported [4] 64-bit Linux distribution with a kernel of:
	  • 4.x or greater (recommended)
	  • 3.10 (minimum)

Airgap environment	• The KOTS airgap license file (submit a request to your Customer Success Manager). • PDF of this installation guide for the version of Jama Connect you are installing. **IMPORTANT** If you lose the URL and password, contact Support to generate new ones.
Optional	• TLS certificate and private key to secure the Admin Console and Jama Connect application.

Run the KOTS preflight installation checks

Whether your environment is internet-enabled or airgapped, run the KOTS preflight installation checks to ensure your system is ready for upgrade.

The preflight checks verify that all server requirements are met to help avoid installation and upgrade issues. When the results display green checkmarks for each test, you can begin the installation process.

To run preflight checks for internet-enabled environments:

1. Run the command on your application server:

   ```
   curl -s https://raw.githubusercontent.com/JamaSoftware/kots-preflights/
   main/non-airgap/application-server.sh | sudo bash
   ```
2. Run the command on your database server:

   ```
   curl -s https://raw.githubusercontent.com/JamaSoftware/kots-preflights/
   main/non-airgap/database-server.sh | sudo bash
   ```
3. Press **S** to save the file, then review the results.
4. Submit an Installation Service Request Form (guided for Self-Hosted) and include your preflight check results to help our technical services team support your installation needs. Include any questions or concerns about the results in the ticket.

To run preflight checks for airgapped environments:

1. **From an internet-enabled server**
   a. Download the preflight script files for the application server:

   ```
   curl https://raw.githubusercontent.com/JamaSoftware/kots-preflights/
   main/airgap/linux/airgap-host-preflight_linux.tar.gz --output airgap-
   host-preflight_linux.tar.gz

   curl https://raw.githubusercontent.com/JamaSoftware/kots-preflights/
   ```

```
main/airgap/linux/airgap-application-server_linux.sh --output airgap-
application-server_linux.sh
```

b. Download the preflight script files for the database server:

```
curl https://raw.githubusercontent.com/JamaSoftware/kots-preflights/
main/airgap/linux/airgap-database-preflight_linux.tar.gz --output
airgap-database-preflight_linux.tar.gz

curl https://raw.githubusercontent.com/JamaSoftware/kots-preflights/
main/airgap/linux/airgap-database-server_linux.sh --output airgap-
database-server_linux.sh
```

2. **From your application server**
   a. Save both application server script files to a directory on the airgapped application server that will host your KOTS installation, then configure the file permissions for the shell script:

```
chmod +x <path to the files>/airgap-application-server_linux.sh
```

   b. Run the preflight installation check:

```
sudo bash <path to the files>/airgap-application-server_linux.sh
```

   c. Press **S** to save the file, then review the results.
3. **From your database server**
   a. Save both database server script files to a directory on the airgapped Jama Connect database server, then configure the file permissions for the shell script:

```
chmod +x <path to the files>/airgap-database-server_linux.sh
```

   b. Run the preflight installation check:

```
sudo bash <path to the files>/airgap-database-server_linux.sh
```

   c. Press **S** to save the file, then review the results.
4. Submit an Installation Service Request Form (guided for Self-Hosted) and include your preflight check results to help our technical services team support your installation needs. Include any questions or concerns about the results in the ticket.

System requirements and supported software (KOTS)

Make sure that your environment conforms to all requirements and recommendations before installing Jama Connect software.

After reviewing the information on this page, see Things to do before installation.

IMPORTANT

To use Ubuntu 22.04, you must update the memory or Elasticsearch fails. From the KOTS Admin Console, adjust the memory settings so that Maximum Memory is 6G and Maximum Memory for Container is 8G.

Application server

Use the information in this table for the server that runs the Jama Connect application. For details on sizing your application server to your environment, see Resource sizing for application server.

Component	
Minimum • 8 CPU • 32 GB RAM • 200 GB storage per node • Every node has the same storage space	**Recommended** • 16 CPU • 64 GB RAM • 200 GB storage • Every node has the same storage space
Operating system • *Recommended* — Ubuntu 20.04 or Ubuntu 22.04 • Red Hat 8.6 or 8.8 — Supported only when the RHEL Container Tools are not installed.	
Software installed with Jama Connect • KOTS • Containerd	
Musts • Dedicated server — Is running only Jama Connect • Accessible by admin with permissions • Uses only supported software and environments	

Database server

Use the information in this table for the server that runs your database. For details on sizing your database server to your environment, see Resource sizing for database server.

Component	
Minimum • 4–8 CPU • 16–24 GB RAM	**Recommended** • 8 CPU • 24 GB RAM • Dedicated volumes for data
Database software • MySQL 8 (recommended) • Microsoft SQL Server 2019 & 2022	
Operating system • *Recommended* — Ubuntu 20.04 or Ubuntu 22.04 • Red Hat 8.6 or 8.8	
Musts • Database is hosted on a server separate from the Jama Connect application. • Database server can host other databases, but no other applications. • Accessible by admin with permissions. • Uses only supported software and environments. • Databases must be able to accept a minimum of 300 concurrent connections.	
Not supported • Azure database • MariaDB • Custom configurations of Jama Connect databases (for example, query optimization and additional indexes that aren't shipped with Jama Connect)	

Supported software

Make sure your environment uses only supported software.

Component	
Browsers • Edge Chromium • Firefox* • Google Chrome* • Safari* *Versions released over the past 12 months are supported.	**Important** Browser zoom is supported only at 100%. Use of browser extensions/add-ons or enabling Compatibility View is not supported while using Jama Connect. **Tip** To prevent session issues, use the application in a single browser window.
Word processor and spreadsheet programs • Office 365 for Mac • Office 365 for Windows	Office 365 is used for exports and reports.

Application server requirements (upgrading traditional to KOTS)

To install and run Jama Connect successfully, your application server must meet these requirements.

Requirement	Notes
A dedicated application server	Jama Connect is the only application running on the application server. External services can affect stability of the application, for example by consuming memory resources.
Sufficient storage, CPU, and memory for optimal performance	To estimate the size of and required resources for your application server, see Resource sizing for application server [6].
Accessible by an admin with permissions	An admin must have proper permissions to maintain the application, perform upgrades, and access the server for regular maintenance.
Uses compatible software and environments	Verify that you're using supported software and environments [6] compatible with the most recent self-hosted release.

Resource sizing for application server (upgrading traditional to KOTS)

For optimal performance, estimate your application server needs before you install Jama Connect.

Requirements

- Each node must have a minimum volume of 200 GB. Increase this size based on the size of the assets that you plan to save in Jama Connect. We recommend that every node has the same storage space.
- KOTS must be up and running before you configure the application settings in the KOTS Admin Console.

IMPORTANT
To avoid performance issues, use the recommended requirements for horizontal scaling, rather than minimum requirements.

Use the following tables to help determine resources for the primary node of your application server.

Minimum size (AWS instance sizing = m5.2xlarge)

CPU	RAM	CPU + memory settings	CPU + memory setting with horizontal scaling jamacores
8	32 GB	N/A	*jamacore application settings:* • Maximum CPU: 1000m • Maximum memory: 2 G • Maximum memory per container: 3 G • Number of ingress nodes 2

Recommended size (AWS instance size = m5.4xlarge)

CPU	RAM	CPU + memory settings	CPU + memory setting with horizontal scaling jama-cores
16	64 GB	*Supports:* • 1,250 users with a ramp-up time of 30 sec-onds	*Supports:* • 1,250 users with a ramp-up time of 10 seconds • 2,500 users with a ramp-up time of 30 seconds
		jamacore application settings: • Maximum CPU: 12000m • Maximum memory: 48 G • Maximum memory for container: 60 G	*jamacore application settings:* • Maximum CPU: 3000m • Maximum memory: 12 G • Maximum memory for container: 15 G • Number of ingress nodes: 2
		Elasticsearch settings: • Maximum CPU: 8000m • Maximum memory: 8 G • Maximum memory for container: 10 G	*Elasticsearch settings:* • Maximum CPU: 8000m • Maximum memory: 8 G • Maximum memory for container: 10 G
		Diff Service settings: • Maximum memory: 2 G	*Diff Service settings:* • Maximum memory: 2 G

Use the following table to help determine resources for the secondary node of your application server.

Secondary nodes dedicated to Elasticsearch: Recommended size (AWS instance size = m5.2xlarge)

CPU	RAM	CPU + memory settings
8	32 GB	*Supports:* • 2,500 users with a ramp-up time of 10 seconds *Elasticsearch settings:* • Maximum CPU: 8000m • Maximum memory: 8 G • Maximum memory for container: 10 G

TIP

Once you're up and running, you can monitor usage and adjust your settings as needed.

Database server requirements (upgrading traditional to KOTS)

The database must be hosted on a server separate from the Jama Connect application. This server can host other databases, but we don’t support running other applications on the same server as the database.

Supported databases

- MySQL 8 (recommended)
- Microsoft SQL Server 2019 & 2022

What is not supported

- Azure database
- MariaDB
- Custom configurations of Jama Connect databases. Customizations such as query optimization and additional indexes that aren't shipped with Jama Connect aren't supported.

Resource sizing for database server (upgrading traditional to KOTS)

For optimal performance, estimate your database server needs before you install Jama Connect.

Use the information in this table to determine resources needed for your database server.

Database server	Small	Medium	Large	Enterprise
Active items in system	$\leq 600,000$	≤ 2 million	2–4 million	4 million+
Active projects	≤ 100	≤ 500	$\leq 1,000$	1,000+
Concurrent users	≤ 50	≤ 500	$\leq 1,000$	1,000+
CPU	4	8	16	Contact Support
Total systems of RAM	16 GB	32 GB	64 GB	Contact Support

If your usage approaches the Enterprise threshold, contact Support for customized recommendations and advanced, multi-server setup.

TIP

Once you're up and running, you can monitor usage and adjust your settings as needed.

Important considerations

- Total system RAM for your database server can vary if you're using memory intensive workflows such as reuse, exporting, move items, integrations, and batch updates. Database sizing is based on your usage patterns and platform. You must have a minimum of 4–8 cores and 16–24 GB of memory. Consult with your database admin when determining database size.
- The memory allocation allows for minimum headroom. If you need to run additional software for monitoring and analysis, consider the system requirements for that software. Configure dynamic memory settings as needed in the Admin Console.

Things to do before upgrading from traditional to KOTS

Whether your environment is internet-enabled or airgap, make sure that your application server and database server are ready before upgrading Jama Connect from traditional to KOTS.

Important considerations and requirements

- If using the existing application server and database server, you must back up the Jama Connect database and all project assets before proceeding with the upgrade.

- Recommended — Back up or create a snapshot of all relevant application servers in case you need to revert to the traditional Replicated environment.
- Record existing Admin Console settings before you uninstall the traditional Replicated platform elements. These settings are used when configuring new settings for the KOTS environment.

Perform these tasks before you upgrade to KOTS

- Preserve data assets and tenant.properties file [9]
- Prepare your application server [9]
- Prepare your new or existing database server [12]
- Install and configure your database (MySQL [13] or SQL Server [14])
- Restore database backups from traditional Replicated to KOTS [16]
- Configure custom memory settings for Elasticsearch [17]

Preserve data assets and tenant.properties files

You must preserve project data assets and the tenant.properties files from the traditional Replicated environment before beginning the upgrade and before uninstalling the traditional Replicated Docker containers.

The tenant.properties file is located on the application server in /data/tenant.

NOTE
These assets and files are used when you provision your tenant [22].

To preserve data assets and tenant.properties files:

1. Create a backup of your tenant and OAuth databases. If you are installing KOTS in an environment with a new database server, you must restore the backups to the new server.
2. Save the backup file to a location you can access easily. You need access to this file when provisioning the tenant in the new KOTS Replicated environment.
3. Preserve the data assets and save them to an accessible location:

   ```
   cd /data/contour
   tar -zcvf assets.tar.gz avatars/ attachments/ diagrams/ reports/
   equations/ tempreports/
   ```
4. Copy the tenant.properties file to an accessible location.

Prepare your application server (upgrading traditional to KOTS)

Make sure your application server meets all requirements. See System requirements and supported software [4].

For users and admins to properly access Jama Connect, specific ports must be accessible to inbound traffic. Work with your network admin to make sure your network is configured properly.

Prepare an existing application server

IMPORTANT

These steps apply only if you are upgrading with an existing server.

You must remove Replicated services and all Docker packages before you upgrade to KOTS.

You must preserve the existing data assets and tenant.properties file [9] before you uninstall the traditional Replicated Docker containers.

1. Record the existing settings of your Admin Console.
2. Stop the Replicated services.

Ubuntu/Debian	`sudo service replicated stop`
	`sudo service replicated-ui stop`
	`sudo service replicated-operator stop`
	`sudo docker stop replicated-premkit`
	`sudo docker stop replicated-statsd`

RHEL/Fedora	`systemctl stop replicated replicated-ui replicated-operator`
	`service replicated stop`
	`service replicated-ui stop`
	`service replicated-operator stop`
	`docker stop replicated-premkit`
	`docker stop replicated-statsd`

3. Stop and remove remaining containerd containers:

```
docker stop $(docker ps -aq)
docker rm $(docker ps -aq)
```

4. Run the command for your operating system to remove traditional Replicated platform elements. Removing these items does not remove data or assets associated with provisioned tenants.

IMPORTANT

Jama Connect is offline during this process. Make sure to inform your users of this maintenance downtime.

Ubuntu/ Debian	`docker rm -f replicated replicated-ui replicated-operator replicated-premkit replicated-statsd retraced-api retraced-processor retraced-cron retraced-nsqd retraced-postgres`
	`docker images | grep "quay\.io/replicated" | awk '{print $3}' | xargs sudo docker rmi -f`
	`docker images | grep "registry\.replicated\.com/library/retraced" | awk '{print $3}' | xargs sudo docker rmi -f`
	`apt-get remove -y replicated replicated-ui replicated-operator`
	`apt-get purge -y replicated replicated-ui replicated-operator`
	`rm -rf /var/lib/replicated* /etc/replicated* /etc/init/replicated* /etc/init.d/replicated* /etc/default/replicated* /var/log/upstart/replicated* /etc/systemd/system/replicated*`

RHEL/ Fedora	`docker rm -f replicated replicated-ui replicated-operator replicated-premkit replicated-statsd retraced-api retraced-processor retraced-cron retraced-nsqd retraced-postgres`
	`docker images | grep "quay\.io/replicated" | awk '{print $3}' | xargs sudo docker rmi -f`
	`docker images | grep "registry\.replicated\.com/library/retraced" | awk '{print $3}' | xargs sudo docker rmi -f`
	`yum remove -y replicated replicated-ui replicated-operator`
	`rm -rf /var/lib/replicated* /etc/replicated* /etc/init/replicated* /etc/default/replicated* /etc/systemd/system/replicated* /etc/sysconfig/replicated* /etc/systemd/system/multi-user.target.wants/replicated* /run/replicated*`

5. Stop and remove any remaining Docker resources, including containers, images, and volumes. This affects all containers on the system, not only those associated with Jama Connect and Replicated.

```
docker kill $(docker ps -q)
docker rmi -f $(docker images| awk '{print $3}')
docker volume rm $(docker volume ls -qf dangling=true)
docker system prune -a -f
```

6. Remove remaining Docker packages to prepare for the KOTS installer.

Ubuntu/ Debian	`#dpkg, purge and remove`
	`dpkg -l | grep -i docker`
	`sudo apt-get purge -y docker-engine docker docker.io docker-ce docker-ce-cli docker-compose-plugin`
	`sudo apt-get autoremove -y --purge docker-engine docker docker.io docker-ce docker-compose-plugin`
	
	`#remove remaining docker files`
	`sudo rm -rf /var/lib/docker /etc/docker`
	`sudo rm /etc/apparmor.d/docker`
	`sudo groupdel docker`
	`sudo rm -rf /var/run/docker.sock`

RHEL/ Fedora	`sudo yum remove docker-ce docker-ce-cli docker-scan-plugin docker-ce-rootless-extras containerd.io`
	`sudo yum remove docker \`
	`docker-client \`
	`docker-client-latest \`
	`docker-common \`
	`docker-latest \`
	`docker-latest-logrotate \`
	`docker-logrotate \`
	`docker-engine`

7. After removing Docker from the server, you must reboot the server before proceeding with the upgrade.

Prepare all application servers (existing and new)

1. **Inbound rules and ports for nodes** — Make sure the ports in the following table are accessible to inbound traffic and the inbound rules are configured for each server in the KOTS cluster.

Protocol	Port range	Source*	Inbound rule applies to node...	Description
HTTPS	443	Anywhere	All	Jama Connect port for SSL/TLS communication (HTTPS), which is used to access Jama Connect. It can be disabled or the port number can be reconfigured.
HTTP	80	Anywhere	All	Jama Connect port for clear text communication (HTTP), which is used to access Jama Connect. It can be disabled or the port number can be reconfigured.

Protocol	Port range	Source*	Inbound rule applies to node...	Description
TCP	8800	Anywhere	All	Allows admins to access the KOTS Admin Console, which is used to configure, install, and upgrade Jama Connect.
SSH	22	Anywhere	All	Allows admins to make remote connections to the nodes using SSH.
TCP	6443	Anywhere Any node	Primary	Allows admins and KOTS nodes to access the Kubernetes API server.**
TCP	2379–2380	Any node	Primary	Allows the KOTS nodes to access the etcd server client API.**
TCP	10250	Any node	All	Allows the KOTS nodes to access the Kubelet API server.**
UDP	8472	Any node	All	Allows KOTS (Flannel) to create a virtual network that connects the services running inside the cluster.**

* *Anywhere* means anyone or anything that must consume the resources in the environment.

** Can be disabled in single node clusters.

2. **User IDs** — Verify that the following User IDs are available and unused on the application server.
   - **User ID 91** — Used by Tomcat to read and write to directories inside jamacore pods.
   - **User IDs 480–499** — Used by the various services.
3. **Time sync setting** — To ensure accurate time on the application server, set up a cron job to sync the time on a routine schedule (for example, every day or hour). Use this command to set up the cron job:

   ```
   ntpdate pool.ntp.org
   ```

Your application server is now ready for the upgrade to KOTS.

Preparing your new or existing database server (upgrading traditional to KOTS)

The following information is needed when connecting the application server to the database server.

Information	Requirements
Type/vendor	Database must be one of the following: • MySQL 8 (recommended) — Install and configure MySQL • Microsoft SQL Server 2019 & 2022 — Install and configure Microsoft SQL Server
Database hostname	Example: *jama.companydb.com*
Listening ports	The application server must be allowed to communicate remotely with the database server over the listening ports. Default ports are: • MySQL = 3306 • Microsoft SQL Server = 1433
Database schema name	The database owner must be able to create one: • A new database schema • Tables inside an existing database schema of the given name The database name must follow these rules: • Start with a letter (a–z) • Contain any number of characters: a–z, 0–9 or an underscore ("_") • Letters must be lowercase
Username	*jamauser*
Password	
Connections	The database must be able to accept a minimum of 300 concurrent connections.

Information	Requirements
SAML schema user-name	*samluser*
OAuth database user-name	*oauthuser*

The username and password for SAML and OAuth must match what's entered in the Microsoft SQL Server upgrade preparation script. See Install and configure Microsoft SQL Server [14] for more details.

Install and configure MySQL (upgrading traditional to KOTS)

MySQL is the recommended database server. Follow these steps to install and configure the server.

Important considerations

- You must have full database admin permissions to the server hosting the MySQL database.
- For the Jama Connect installation to succeed, you must first create two additional database schemas.

Recommended settings and sample

The following recommended settings require 8 GB of memory allocated to MySQL Server for a typical installation and 16 GB for an enterprise installation.

These settings can be added to your my.cnf file (Linux) or my.ini file (Windows).

Property	Typical installation	Enterprise installation
max_allowed_packet	1 GB	1 GB
tmp_table_size	2 GB	2 GB
max_heap_table_size	2 GB	2 GB
table_open_cache	512	512
innodb_buffer_pool_size	2 GB	12 GB
innodb_log_file_size	256 MB	256 GB
innodb_log_buffer_size	12 MB	12 MB
innodb_thread_concurrency	16	16
max_connections	151	351
wait_timeout	259200	259200

Here is a sample text config file at an enterprise level. You must add the following values for your environment:

```
bind-address=0.0.0.0
key_buffer_size=16M
max_allowed_packet=1G
thread_stack=192K
thread_cache_size=8
tmp_table_size=2G
max_heap_table_size=2G
table_open_cache=512
innodb_buffer_pool_size=12G
innodb_log_file_size=256M
innodb_log_buffer_size=12M
innodb_thread_concurrency=16
max_connections=351
wait_timeout=259200
```

IMPORTANT
The following steps apply only if you are creating a new database instance to support the KOTS upgrade.

To install and configure MySQL:

1. Make sure that the InnoDB engine is enabled.
2. Download and install a supported version of MySQL [4].
3. On the MySQL database server, create an empty Jama Connect schema / database that uses UTF8:

   ```
   CREATE DATABASE jama character set utf8mb4;
   ```
4. On the MySQL database server, create two additional database schemas and a user ("jamauser") with the ability to access, create, and update tables within the database:

   ```
   CREATE DATABASE saml;
   CREATE DATABASE oauth;
   CREATE USER 'jamauser'@'%' IDENTIFIED BY 'password';
   CREATE USER 'oauthuser'@'%' IDENTIFIED BY 'password';
   CREATE USER 'samluser'@'%' IDENTIFIED BY 'password';
   GRANT ALL PRIVILEGES ON jama.* TO 'jamauser'@'%';
   GRANT ALL PRIVILEGES ON oauth.* TO 'oauthuser'@'%';
   GRANT ALL PRIVILEGES ON saml.* TO 'samluser'@'%';
   ```
5. Create a database schema for Quartz to support horizontal scaling in KOTS:

   ```
   CREATE DATABASE quartz;
   CREATE USER 'quartzuser'@'%' IDENTIFIED BY 'password';
   GRANT ALL PRIVILEGES ON quartz.* TO 'quartzuser'@'%'
   ```
6. Restart the database server.

Follow the instructions to Restore backup data from traditional Replicated to KOTS [16].

Install and configure Microsoft SQL Server (upgrading traditional to KOTS)

If you are using Microsoft SQL Server for your database, follow these steps to install and configure it.

Important considerations

- You must have full database admin permissions to the server hosting the SQL Server database.

IMPORTANT
The following steps apply only if you are creating a new database instance to support the KOTS upgrade.

To install and configure SQL Server:

1. Connect to the SQL Server using a SQL management application (such as SQL Server Management Studio).
2. Replace the following values in the installation script: **<JAMA_LOGIN_Psswd>, <SAML_LOGIN_Psswd> & <OAUTH_LOGIN_Psswd>**.

3. Copy and store the passwords you create here. You will need them later to configure the Admin Console settings.
4. In a new query window, run this SQL query script:

```
-- Fresh Install Preparation SCRIPT
/*

INSTRUCTIONS:
This script must be run prior to Jama installation or installation might
fail to
complete.
Modify login passwords as needed.
Passwords must be enclosed in single quotes.
*/

USE master;
CREATE LOGIN jamauser with password = 'password';
CREATE LOGIN samluser with password = 'password';
CREATE LOGIN oauthuser with password = 'password';
GO

USE master;
CREATE DATABASE jama;
GO
ALTER DATABASE jama SET READ_COMMITTED_SNAPSHOT ON WITH ROLLBACK IMMEDIAT
E
GO

USE jama;
EXEC ('CREATE SCHEMA oauth');
EXEC ('CREATE SCHEMA saml');
GO

USE jama;
CREATE USER jamauser for LOGIN jamauser;
CREATE USER samluser for LOGIN samluser with DEFAULT_SCHEMA=saml;
CREATE USER oauthuser for LOGIN oauthuser with DEFAULT_SCHEMA=oauth;
GO

EXEC sp_addrolemember N'db_owner', jamauser;
EXEC sp_addrolemember N'db_owner', samluser;
EXEC sp_addrolemember N'db_owner', oauthuser;
GO
```

5. Create a database schema for Quartz to support horizontal scaling in KOTS:

```
USE master;
CREATE LOGIN quartzuser with password = 'password';
GO

USE jama;
EXEC ('CREATE SCHEMA quartz');
GO

USE jama;
CREATE USER quartzuser for LOGIN quartzuser with
DEFAULT_SCHEMA=quartz;
```

```
GO

EXEC sp_addrolemember N'db_owner', quartzuser;
GO
```

6. Confirm that these actions were successful:
   - **Script completed** — Check the Query Execution results for errors.
   - **Users created** — Run the following SQL script in a new query window.

     ```
     USE jama
     SELECT * from master.sys.sql_logins
     SELECT * from Jama.sys.sysusers
     ```

     The results include **jamauser**, **samluser**, and **oauthuser** in the "Name" column of the result panes.
   - **Users granted the DB_owner role** — Run the following SQL script in a new query window.

     ```
     USE jama
     SELECT DP1.name AS DatabaseRoleName,
     isnull (DP2.name, 'No members') AS DatabaseUserName
     FROM sys.database_role_members AS DRM
     RIGHT OUTER JOIN sys.database_principals AS DP1
     ON DRM.role_principal_id = DP1.principal_id
     LEFT OUTER JOIN sys.database_principals AS DP2
     ON DRM.member_principal_id = DP2.principal_id
     WHERE DP1.type = 'R'
     ORDER BY DP1.name;
     ```

     The results show that db_owner role is granted to **jamauser**, **samluser**, and **oauthuser**.
7. Keep the database from locking users' accounts while they are logging in or working in Jama Connect (you must have db_owner permissions):

   ```
   ALTER DATABASE jama SET READ_COMMITTED_SNAPSHOT ON WITH
   ROLLBACK IMMEDIATE;
   ```
8. Make sure the flag was successfully enabled:

   ```
   SELECT is_read_committed_snapshot_on FROM sys.databases WHERE
   name='jama';
   ```

   If the returned value is 1, the flag is on.

Follow the instructions to Restore backup data from traditional Replicated to KOTS [16].

Restore database backups from traditional Replicated to KOTS

After you install and configure your MySQL or Microsoft SQL database server, you must restore backups of the tenant and OAuth databases from the existing traditional Replicated database instance to the new KOTS database instance.

IMPORTANT

If you use SAML authentication in your traditional Replicated environment, it must be configured in the new KOTS environment, rather than restoring from a backup.

Restore the database, using instructions for MySQL or SQL Server:

1. Restore the tenant database from a native backup to the new environment.
2. Restore the OAuth database from a native backup to the new environment.

Configure custom memory settings for Elasticsearch (upgrading traditional to KOTS)

To prepare for installing Jama Connect, you must first update the system that hosts the application. The update consists of configuring memory settings for Elasticsearch.

Requirements

- The memory settings must be configured on each server in the KOTS cluster for Elasticsearch to run on these servers. If you use the remote Elasticsearch setting, the memory settings can be applied only to servers that are dedicated to Elasticsearch.
- You must have admin permissions to configure the memory settings for Elasticsearch.

To configure memory settings:

1. As an admin, open the /etc/sysctl.conf file, add the following line to the file, then save the file.

   ```
   vm.max_map_count=262144
   ```
2. Reload the sysctl.conf file:

   ```
   sudo sysctl -p
   ```
3. To confirm, type this command:

   ```
   sudo sysctl -a | grep max_map_count
   ```

   The system responds with:

   ```
   vm.max_map_count=262144
   ```

Upgrading the Replicated platform from traditional to KOTS

Whether your organization is internet-enabled or requires an airgap installation, follow these instructions to download, install, and configure the software you need for your Jama Connect instance.

IMPORTANT
KOTS and Jama Connect must be installed on a new cluster that is created during installation and dedicated to KOTS.

The software includes:

- KOTS Admin Console (Replicated)
- Jama Connect
- Jama Connect KOTS license file (contact your Customer Success Manager to request a KOTS internet or airgap license)

The upgrade process consists of these tasks:

- Install KOTS and Jama Connect (internet [18] or airgap [19])
- Provision your tenant in Jama Connect KOTS [22]
- Create a Replicated Snapshot [26]

Depending on your environment, the process can also include these tasks:

- Configure KOTS to save tenant assets in Amazon EFS
- Enable horizontal scaling
- Configure dedicated Elasticsearch nodes
- Configure Federated Authentication for KOTS Admin Console

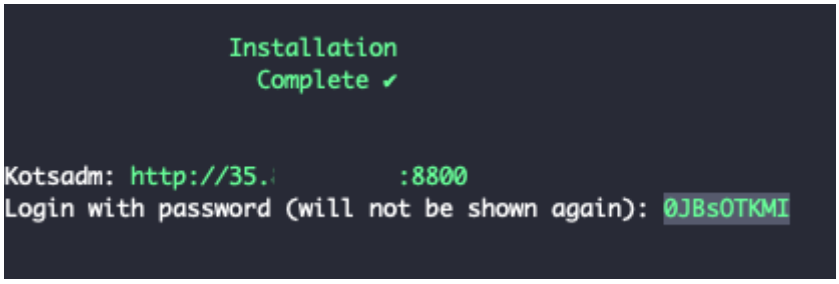
Install the Jama Connect Replicated KOTS platform (internet)

The installation script and the installation wizard guide you through the process of installing the KOTS-required software and Jama Connect, then configuring the KOTS Admin Console.

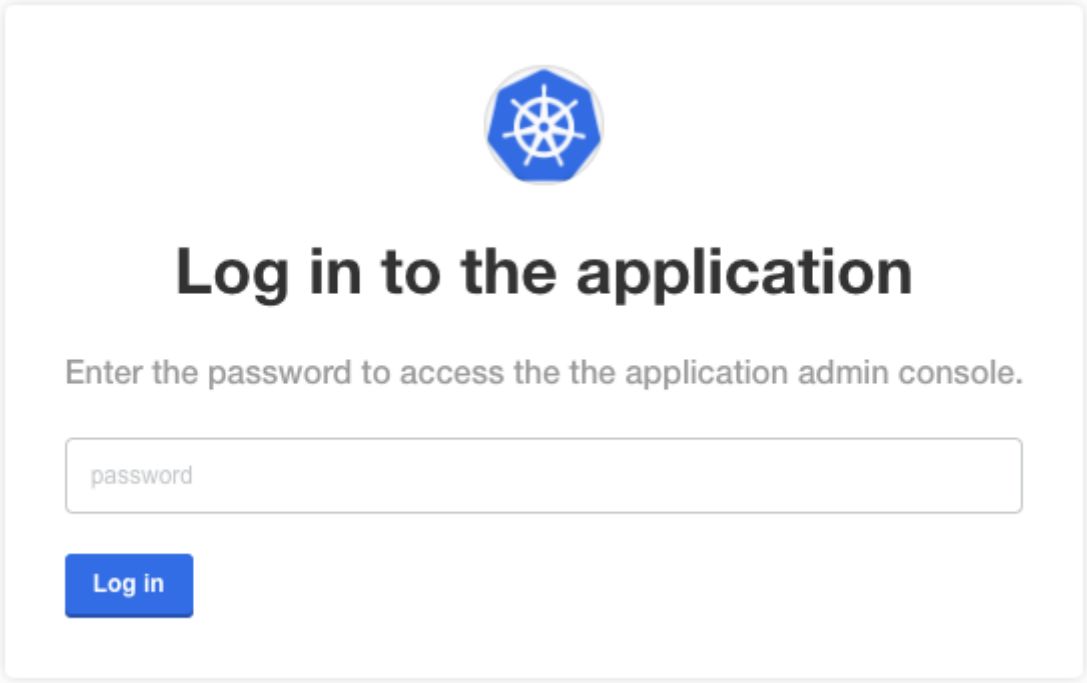
1. Contact your Customer Success Manager to request a KOTS internet license, then save the license file on your local system.
2. Run the command on the application server provisioned for Jama Connect:

   ```
   curl -sSL https://k8s.kurl.sh/jama-k8s-standardkots | sudo bash
   ```

   The installation process can take up to an hour to complete.
3. After the command runs, save the KOTS admin URL, password, and other configuration options for future reference. This is the only time these credentials appear, so make sure you save them.

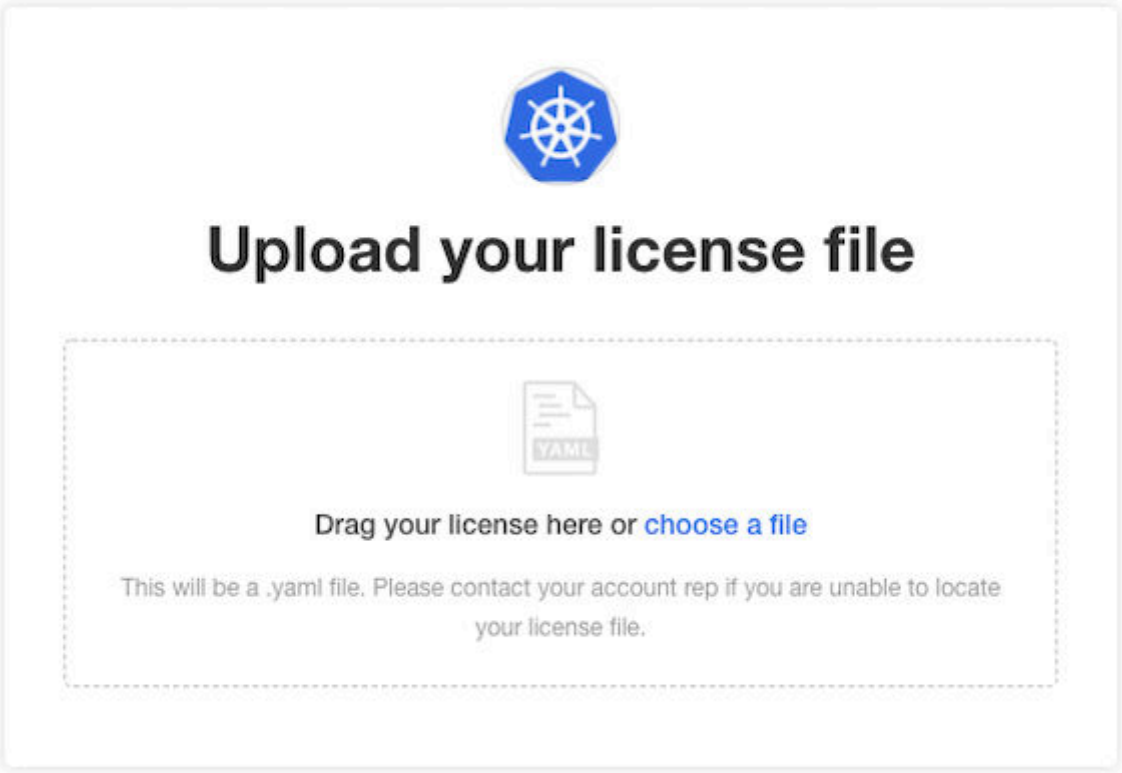
4. In a supported browser, enter the URL for **Kotsadm**, which was generated when you installed KOTS.
5. Log in to the KOTS Admin Console using the password you just saved.

6. Select the appropriate option:
   - **Have key/certificate** — Click **Choose file** under Private key and Certificate, navigate to the files and select them, then click **Upload & Continue**.
   - **No key/certificate** — Select **Self-Signed Cert**.

You can configure the SSL/TLS certificates in the KOTS Admin Console after the deployment as needed.

7. Upload the license file that you saved on your local system.

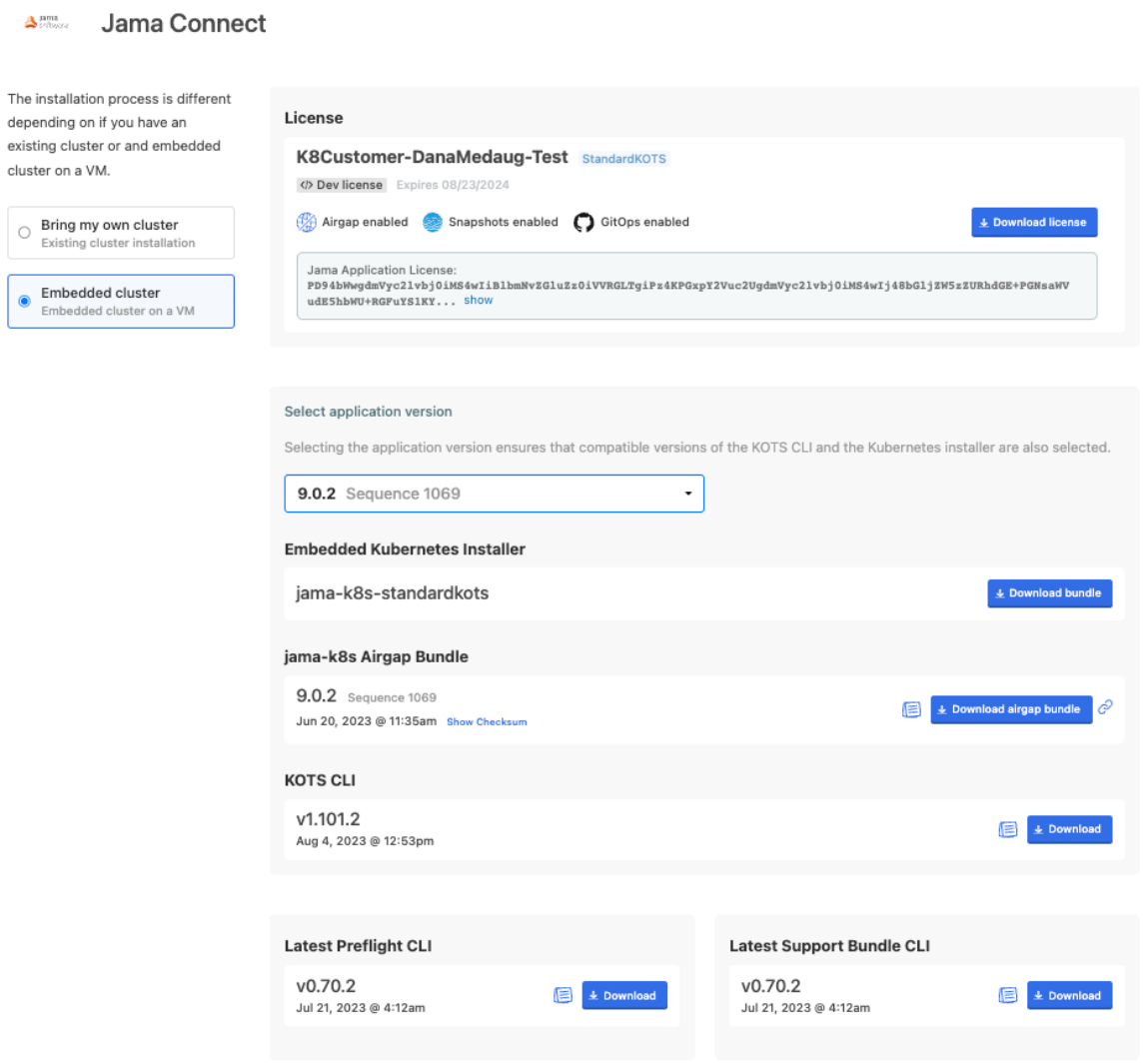


The Config tab in the KOTS Admin Console opens, where you can configure and provision Jama Connect [22].

Install the Jama Connect Replicated KOTS platform (airgap)

The installation script and the installation wizard guide you through the process of installing the KOTS-required software and Jama Connect, then configuring the KOTS Admin Console.

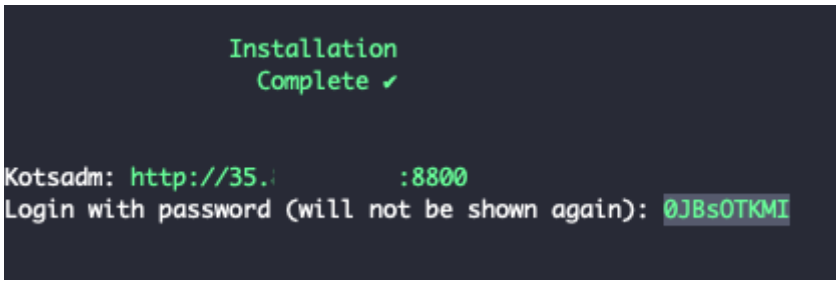
1. Contact your Customer Success Manager to request a KOTS airgap license, then save the license file on your local system.
2. Log in to the airgap portal, select **Embedded Cluster**, then download the **jama-k8s Airgap Bundle** and **Embedded Kubernetes Installer** files to your local system.



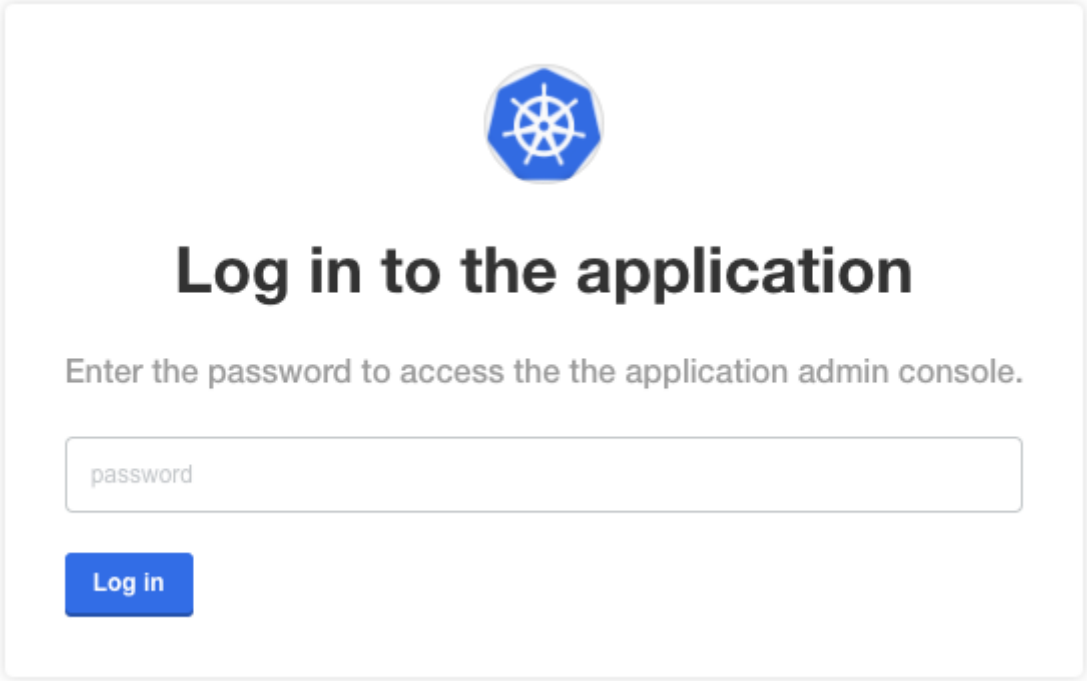
3. To download the Kubernetes Installer for your channel and install it, run the following command on the application server provisioned for Jama Connect.

   ```
   export REPLICATED_APP=jama-k8s
   export REPLICATED_CHANNEL=standardkots

   curl -LS https://k8s.kurl.sh/bundle/$REPLICATED_APP-
   $REPLICATED_CHANNEL.tar.gz -o $REPLICATED_APP-$REPLICATED_CHANNEL.tar.gz
   tar -zxvf $REPLICATED_APP-$REPLICATED_CHANNEL.tar.gz

   cat install.sh | sudo bash -s airgap
   ```

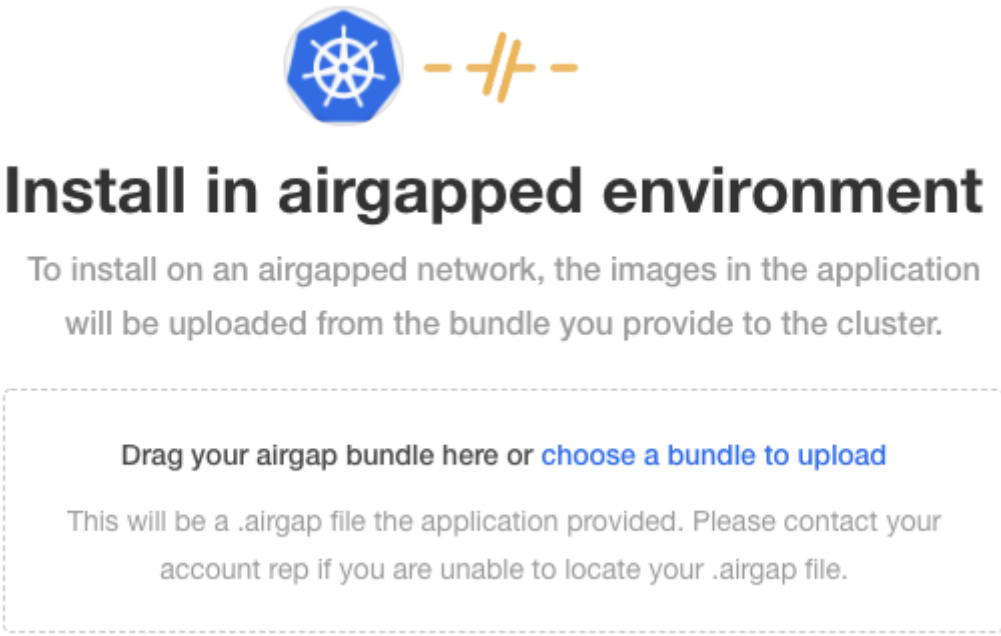
   If your application server doesn't have internet access, you can download the Kubernetes Installer from the airgap-safe portal and upload it to the application server.
4. After the command runs (which might take several minutes), save the KOTS admin URL, password, and other configuration options for future reference. This is the only time these credentials appear, so make sure you save them.
5. In a supported browser, enter the URL for **Kotsadm**, which was generated when you installed KOTS.



6. Log in to the KOTS Admin Console using the password you just saved.



7. Select the appropriate option:
   - **Have key/certificate** — Select **Choose file** under Private key and Certificate, navigate to the files and select them, then click **Upload & Continue**.
   - **No key/certificate** — Select **Use Self-Signed Cert**.
     You can configure the SSL/TLS certificates in the KOTS Admin Console after the deployment as needed.
8. Upload the license file saved on your local system.
9. Upload your jama-k8s airgap bundle, then click **Continue**.



The Config tab in the KOTS Admin Console opens, where you can configure and provision Jama Connect [22].

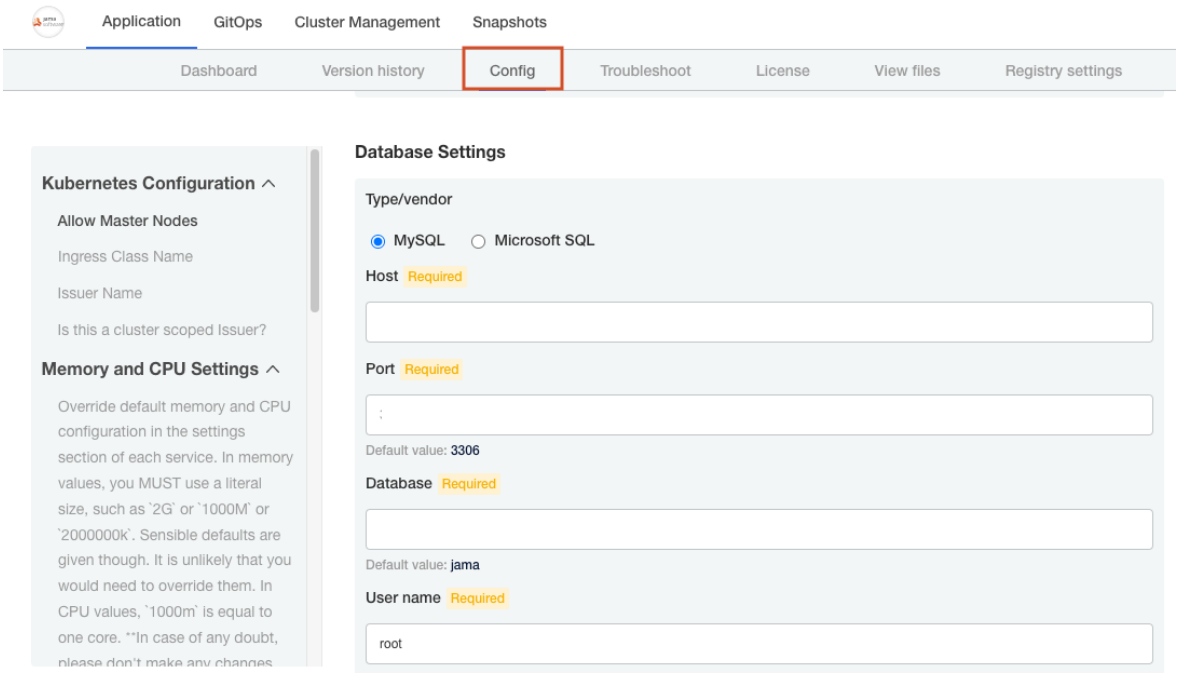
Provision your tenant in Jama Connect KOTS (upgrading traditional to KOTS)

After upgrading the KOTS Replicated environment, you must provision the existing tenant in the new environment.

IMPORTANT
The KOTS Admin Console doesn't support formulas. Instead, use literal values.

To provision your tenant in KOTS:

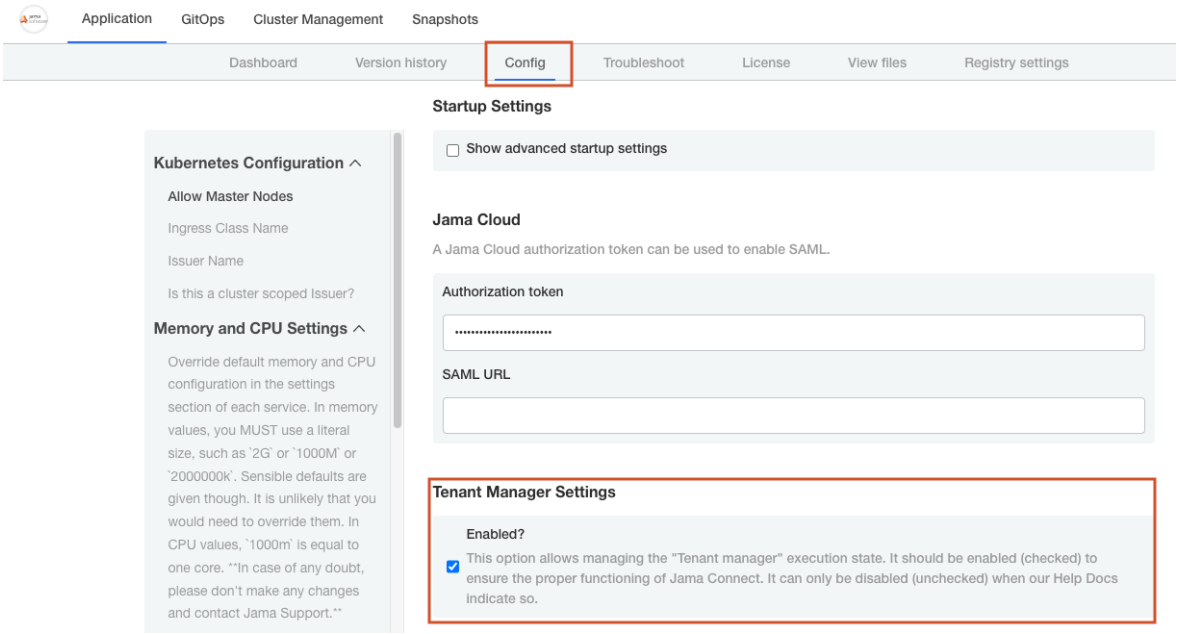
1. From the KOTS Admin Console, select the **Config** tab.



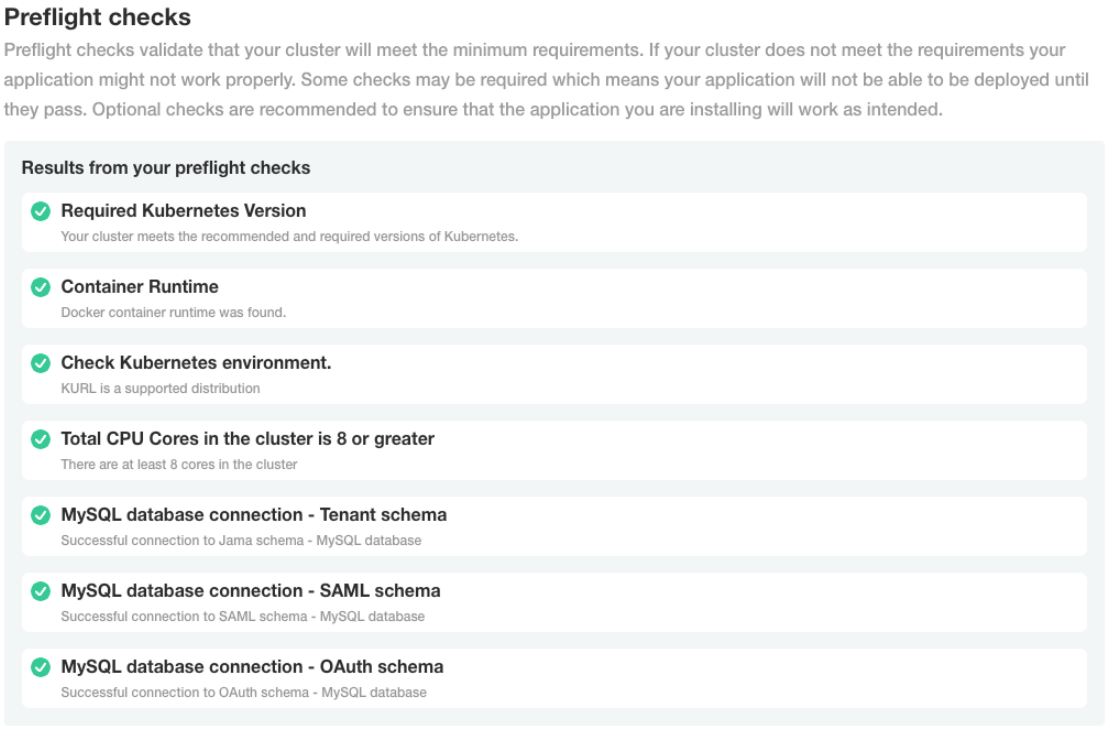
2. Configure the settings for each group, as needed. Scroll down to see each group of settings.

> **IMPORTANT**
> Make sure that the current Host name, Database name, Username, and Password are configured correctly in the KOTS Admin Console. If you installed KOTS in a new environment, you must point to the newly installed database host or the deployment fails.

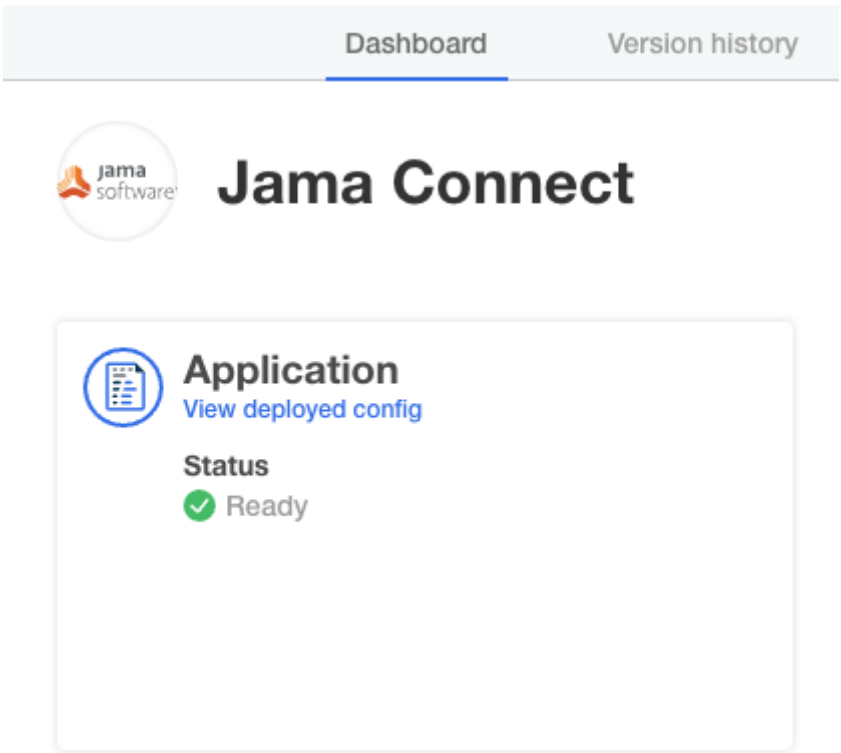
   - **Database Settings** — Select your database type (**MySQL** or **Microsoft SQL Server**), then use the information from Preparing your database server to complete the settings.
   - **Host Name** — Enter the name of the database server (for existing resources, enter current name; for new resources, enter the new name).
   - **TLS Key Pair Source** — (Optional) If you have a custom key and certificate for the host name, select **Custom TLS Configuration**. In the TLS Configuration section, upload the key and certificate.
   - **Assets Size** — Enter the estimated size of the assets based on the current data assets size of your environment and its projected growth.
   - **Elasticsearch Settings > Volume Size** — Enter the amount of disk space that each Elastic-search node is allowed to use.
3. (Optional) From the Config tab in the KOTS Admin Console, follow the steps to configure KOTS to save tenant assets in the Amazon EFS.
4. Scroll down to Tenant Manager Settings and deselect the checkbox to disable it.
   Disabling the Tenant Manager prevents Jama Connect from completing tenant provisioning, which allows you to copy data assets and tenant.properties from the traditional replicated environment to the KOTS environment.



5. Scroll to the bottom of the page and click **Save config**.
   The Preflight checks run.



6. From the Preflight checks screen, click **Continue** to deploy the Jama Connect application and services.
   When the system is available, the status in the KOTS Admin Console changes to **Ready**.
   The deployment process can take up to an hour.



When the preflight checks are complete, Jama Connect creates the Kubernetes pods, which contain the Jama Connect application and related services.

7. From the application server CLI, verify that the Kubernetes pods were successfully created:

   ```
   kubectl get pods
   ```

   Application server CLI example:

```
ubuntu@ip-10-59-0-42:~$ kubectl get pods
NAME                                READY   STATUS    RESTARTS   AGE
activemq-0                          1/1     Running   0          3d20h
core-0                              1/1     Running   0          3d18h
diff-0                              1/1     Running   0          3d20h
elasticsearch-0                     1/1     Running   0          3d20h
hazelcast-0                         1/1     Running   0          3d20h
kotsadm-7d889d7d4f-x7qxc            1/1     Running   0          4d
kotsadm-postgres-0                  1/1     Running   0          4d
kurl-proxy-kotsadm-5c6bb84446-lwdwg 1/1     Running   0          4d
nginx-0                             1/1     Running   0          3d20h
oauth-0                             1/1     Running   7          3d18h
saml-0                              1/1     Running   7          3d18h
search-0                            1/1     Running   0          3d20h
```

8. When the pods are ready and running, copy the data assets and tenant.properties file, which you preserved [9] in an earlier task, to an accessible location on the application server.
9. On the application server, set the tenant name for the environment (the tenant name, usually *jama*, and can be found in the tenant.properties file that you preserved earlier):

   ```
   export TENANT_NAME=<tenant_name>
   ```

10. On the application server:
    a. Copy and extract the previously preserved data assets into the running core pod and change the ownership permissions:

```
kubectl cp -c core /tmp/contour/assets.tar.gz default/core-0:/home/
contour/tenant/${TENANT_NAME}/
kubectl exec --tty -c core pods/core-0 -- tar -xvzf /home/
contour/tenant/${TENANT_NAME}/assets.tar.gz -C /home/contour/tenant/$
{TENANT_NAME}/
kubectl exec --tty -c core pods/core-0 -- chmod -R 755 /home/contour
kubectl exec --tty -c core pods/core-0 -- chown -R tomcat:tomcat /
home/contour
```

b. Copy the previously preserved tenant.properties file into the running core pod and change the ownership permissions:

```
kubectl cp -c core tenant.properties default/core-0:/home/contour/
tenant_properties/tenant.properties
kubectl exec --tty -c core pods/core-0 -- chmod -R 755 /home/contour
kubectl exec --tty -c core pods/core-0 -- chown -R tomcat:tomcat /
home/contour
kubectl exec --tty -c core pods/core-0 -- cat /home/contour/
tenant_properties/tenant.properties
```

c. Delete the core stateful set to recreate the core pod:

```
kubectl delete sts/core
```

11. From the KOTS Admin Console, select the **Config** tab, enable the Tenant Manager Settings, then click **Save config**.
12. Deploy the new version of Jama Connect.
    a. When the deployment is complete and all pods are running, log in to Jama Connect as root using the hostname configured for Jama Connect.
    b. If upgrading with new servers:
       - SAML authentication must be configured in the new KOTS Jama Connect environment.
       - Update the base URL before performing a full reindex.
    c. Perform a full reindex in Jama Connect to complete the deployment.

Create a Replicated Snapshot (KOTS)

Taking a full snapshot creates a backup of the KOTS Admin Console and application data. It can be used for full Disaster Recovery by restoring over the same instance or in a new cluster. Tenant assets are included in the snapshot. Elasticsearch data is included by default.

A Replicated Snapshot can be taken while Jama Connect is running without interruption.

Requirements

- Replicated Snapshots must be enabled for your Replicated customer license.
- KOTS Admin Console 1.79 and later.
- Replicated Snapshots don't include your database. You must use a proprietary backup/restore system for your type of database, MySQL or SQL Server.

Important considerations

- When restoring from a snapshot in a new cluster, you must reinstall KOTS.
- *Recommended* — Include Elasticsearch data in snapshots to avoid having to reindex your data after performing a restore. However, if your snapshot is not recent, we recommend reindexing your data.
- Replicated Snapshots don't support IAM authentication against EFS. Saving Replicated Snapshots in EFS requires that you use the default file system policy to allow all nodes in the cluster to mount the EFS.

To create a Replicated snapshot:

1. Capture the KOTS installer.
2. (Recommended) Include Elasticsearch data in snapshots: From the KOTS Admin Console under the Elasticsearch Settings section, select **Include Elasticsearch in Replicated Snapshots**.
3. *Airgap only* — Capture the IP address of the private registry, which is the IP address value in the Cluster-IP column:

   ```
   kubectl get service/registry -n kurl
   ```
4. Configure the storage destination:
   a. In the KOTS Admin Console, select **Snapshots > Settings & Schedule**.
   b. From the Destination drop-down menu, select a storage destination for your snapshots.
      - **For AWS S3** — The IAM role assigned to the underlaying servers or the user associated with the credentials (access and secret key) must have the Policy template attached. Use the following template to create a policy, replacing the **<arn-S3>** parameter with ARN of the S3 bucket. For example: arn:aws:s3:::jama-snapshots.

        ```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "s3:PutObject",
                        "s3:GetObject",
                        "s3:AbortMultipartUpload",
                        "s3:DeleteObject",
                        "s3:ListMultipartUploadParts"
                    ],
                    "Resource": "<arn-s3>/*"
                },
                {
                    "Effect": "Allow",
                    "Action": "s3:ListBucket",
                    "Resource": "<arn-s3>"
                }
            ]
        }
        ```
      - **For NFS** — If using EFS as an NFS server, the **Server** field = the **DNS name** of the EFS and the **Path** field = a directory inside the EFS, writable by the user:group 1001:1001.
   c. Click **Update storage settings** to save your preferences.
5. Schedule Full Snapshots:
   a. In the KOTS Admin Console, select **Snapshots > Settings & Schedule**.
   b. Select **Enable automatic scheduled snapshots**, then click **Update schedule**.
6. Create a Full Snapshot (follow the steps provided by Replicated).

After upgrading Jama Connect traditional to KOTS

Whether your environment is internet-enabled or airgap, after upgrading from Jama Connect traditional to KOTS you can continue to set up your Jama Connect environment.

Follow any post upgrade instructions that apply to your organization:

- Add Organization Admin account
- Modify organization details
- Configure email/collaboration settings
- Configure user authentication
- Create XML backups (optional)

- Update the license for KOTS environments (optional)

If you have further questions about Jama Connect installation and setup, visit the Jama Support Community or contact Support.