Overview

An overview of the architecture, services, and new features of CircleCI Server v3.4.1

docs@circleci.com

Version 3.4.1, 04/07/2022: FINAL
CircleCI Server v3.x FAQ

Does Server 3.0 have a data retention policy?

What control is granted over Nomad certificates?

Is it possible to change or disable the polling time which checks for health status?

What do the Application Status options in KOTS mean?
CircleCI Server v3.x Overview

Introduction

CircleCI server is an on-premises CI/CD platform for enterprise customers who have compliance or security needs that require them to operate within their firewall, in a private cloud, or in a data center.

Server provides the same features as CircleCI’s cloud offering, but operates within your Kubernetes cluster.

--

![CircleCI Server v3.x Architecture](image)

The CircleCI server application exposes four services, using load balancers. Three of these load balancers are VPC (Virtual Private Cloud)-internal for connecting to the Nomad cluster and virtual machines. If required, the front-end load balancer can be made private, separating it from the public internet. For further information see the Load Balancers doc.

<table>
<thead>
<tr>
<th>Load Balancer</th>
<th>Type</th>
<th>Ports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend GUI Proxy &amp; API</td>
<td>External</td>
<td>80 and 443</td>
<td>Exposes the web application.</td>
</tr>
<tr>
<td>Nomad Control Plane</td>
<td>Internal</td>
<td>4647</td>
<td>Exposes an RPC protocol for Nomad runners.</td>
</tr>
<tr>
<td>Output Processor</td>
<td>Internal</td>
<td>8585</td>
<td>Ingests output from Nomad runners.</td>
</tr>
<tr>
<td>VM Service</td>
<td>Internal</td>
<td>3000</td>
<td>Provisions virtual machines.</td>
</tr>
</tbody>
</table>

---
The application exposes a number of external ports. These ports are used for various functions as defined in the table below.

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Direction</th>
<th>Source / Destination</th>
<th>Use</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Inbound</td>
<td>End users</td>
<td>HTTP web app traffic</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Inbound</td>
<td>End users</td>
<td>HTTP web app traffic</td>
<td></td>
</tr>
<tr>
<td>8800</td>
<td>TCP</td>
<td>Inbound</td>
<td>Administrators</td>
<td>Admin console</td>
<td>Only required for the bastion host.</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>Inbound</td>
<td>Administrators</td>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>64535-65535</td>
<td>TCP</td>
<td>Inbound</td>
<td></td>
<td>SSH into builds</td>
<td>Only required for the Nomad clients.</td>
</tr>
</tbody>
</table>

CircleCI server schedules CI jobs using the Nomad scheduler. The Nomad control plane runs inside of Kubernetes, while the Nomad clients, which are responsible for running scheduled CircleCI jobs, are provisioned outside the cluster. CircleCI server can run Docker jobs on the Nomad clients themselves or in a dedicated virtual machine (VM).

Job artifacts and outputs are sent directly from jobs in Nomad to object storage (S3, GCS, or other supported options). Audit logs and other items from the application are also stored in object storage, so both the Kubernetes cluster and the Nomad clients need access to object storage.

## Services

CircleCI server 3.0 consists of the following services. Find their descriptions and failure implications below:

<table>
<thead>
<tr>
<th>Service</th>
<th>Component</th>
<th>Description</th>
<th>What happens if it fails?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>api-service</td>
<td>App Core</td>
<td>Provides a GraphQL API that provides data to render the web frontend.</td>
<td>Many parts of the UI (such as Contexts) will fail completely.</td>
<td></td>
</tr>
<tr>
<td>audit-log-service</td>
<td>App Core</td>
<td>Persists audit log events to blob storage for long-term storage.</td>
<td>Some events may not be recorded.</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Component</td>
<td>Description</td>
<td>What happens if it fails?</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>builds-service</td>
<td>App Core</td>
<td>Ingests from www-api and sends to plans-service, workflows-conductor, and to orbs-service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>circleci-mongodb</td>
<td>Execution</td>
<td>Primary datastore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>circleci-postgres</td>
<td>Data storage for microservices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>circleci-rabbitmq</td>
<td>Pipelines and Execution</td>
<td>Queuing for workflow messaging, test results, usage, crons, output, notifications, and scheduler.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>circleci-redis</td>
<td>Execution</td>
<td>Caches data that will not be stored permanently (such as build logs), for request caching, and for rate limit calculations.</td>
<td>A failed cache can result in rate limiting from the VCS if too many calls are made to it.</td>
<td></td>
</tr>
<tr>
<td>circleci-telegraf</td>
<td></td>
<td>Telegraf collects statsd metrics. All white-boxed metrics in our services publish statsd metrics that are sent to telegraf, but can also be configured to be exported to other places (such as Datadog or Prometheus).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>circleci-vault</td>
<td></td>
<td>HashiCorp Vault to run encryption and decryption as a service for secrets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>config</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Component</td>
<td>Description</td>
<td>What happens if it fails?</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>contexts-service</td>
<td>App Core</td>
<td>Stores and provides encrypted contexts.</td>
<td>All builds using Contexts will fail.</td>
<td></td>
</tr>
<tr>
<td>cron-service</td>
<td>Pipelines</td>
<td>Triggers scheduled workflows.</td>
<td>Scheduled workflows will not run.</td>
<td></td>
</tr>
<tr>
<td>dispatcher</td>
<td>Execution</td>
<td>Split jobs into tasks and send them to scheduler to run.</td>
<td>No jobs will be sent to Nomad. The run queue will increase in size, but there should be no meaningful loss of data.</td>
<td></td>
</tr>
<tr>
<td>domain-service</td>
<td>App Core</td>
<td>Stores and provides information about our domain model. Works with permissions and API.</td>
<td>Workflows will fail to start and some REST API calls may fail, causing 500 errors in the CircleCI UI. If LDAP authentication is in use, all logins will fail.</td>
<td></td>
</tr>
<tr>
<td>exim</td>
<td></td>
<td>Will be removed in GA, but users can provide mail submission credentials to an existing MTA.</td>
<td>No email notifications will be sent.</td>
<td></td>
</tr>
<tr>
<td>frontend</td>
<td>Frontend</td>
<td>CircleCI web app and www-api proxy.</td>
<td>The UI and REST API will be unavailable and no jobs will be triggered by GitHub/Enterprise. Running builds will be OK, but no updates will be seen.</td>
<td>Rate limit of 150 requests per second with a single user instantaneous limit of 300 requests.</td>
</tr>
<tr>
<td>Service</td>
<td>Component</td>
<td>Description</td>
<td>What happens if it fails?</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>inject-bottoken</td>
<td></td>
<td>A Kubernetes job that inserts a &quot;bot token&quot; into MongoDB. Bot tokens are authorization interservice communication.</td>
<td></td>
<td>Mainly for www-api</td>
</tr>
<tr>
<td>kotsadm-kots</td>
<td>Licensing</td>
<td>The main KOTS application. Runs the KOTS Admin Console, where upgrades and server configuration take place.</td>
<td>No upgrades or configuration possible for server. No admin console available.</td>
<td></td>
</tr>
<tr>
<td>kotsadm-migrations</td>
<td>Licensing</td>
<td>Performs database migrations to handle updates of Kotsadm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kotsadm-minio</td>
<td>Licensing</td>
<td>Object storage for KOTS licensing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kotsadm-postgres</td>
<td>Licensing</td>
<td>Database for KOTS licensing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>legacy-notifier</td>
<td>App Core</td>
<td>Handles notifications to external services (for example, Slack or email).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prometheus</td>
<td>Server</td>
<td>Used for metrics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>orb-service</td>
<td>Pipelines</td>
<td>Handles communication between orb registry and config.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Component</td>
<td>Description</td>
<td>What happens if it fails?</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>output-processor</td>
<td>Execution</td>
<td>Receives job output and status updates and writes them to MongoDB. Also provides an API to running jobs to access caches, workspaces, store caches, workspaces, artifacts, &amp; test results.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>permissions-service</td>
<td>App Core</td>
<td>Provides the CircleCI permissions interface.</td>
<td>Workflows will fail to start and some REST API calls may fail, causing 500 errors in the UI.</td>
<td></td>
</tr>
<tr>
<td>scheduler</td>
<td>Execution</td>
<td>Runs tasks sent to it. Works with Nomad server.</td>
<td>No jobs will be sent to Nomad. The run queue will increase in size, but there should be no meaningful loss of data.</td>
<td></td>
</tr>
<tr>
<td>slanger</td>
<td>server</td>
<td>Provides real-time events to the CircleCI app.</td>
<td>Live UI updates will stop, but hard refreshes will still work.</td>
<td></td>
</tr>
<tr>
<td>test-results</td>
<td>Execution</td>
<td>Parses test result files and stores data.</td>
<td>There will be no test failure or timing data for jobs, but this will be back-filled once the service is restarted.</td>
<td></td>
</tr>
<tr>
<td>vm-gc</td>
<td>Compute Management</td>
<td>Periodically checks for stale machine and remote Docker instances and requests that vm-service remove them.</td>
<td>Old vm-service instances might not be destroyed until this service is restarted.</td>
<td></td>
</tr>
</tbody>
</table>
## Platforms

CircleCI server is designed to deploy within a Kubernetes cluster. Virtual machine service (VM Service) is able to leverage unique EKS or GKE offerings to dynamically create VM images.

If installing outside of EKS or GKE, additional work is required to access some of the same machine build features. Setting up CircleCI runners gives you access to the same feature set as VM service across a much wider range of OSs and machine types (MacOS and much more).

We do our best to support a wide range of platforms for installation. We use environment-agnostic solutions wherever possible. However, we do not test all platforms and options. For that reason, we provide a list of tested environments, which we will continue to expand. We will be adding OpenShift to our list of regularly tested and supported platforms.

### Platforms Table

<table>
<thead>
<tr>
<th>Service</th>
<th>Component</th>
<th>Description</th>
<th>What happens if it fails?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-scaler</td>
<td>Machine</td>
<td>Periodically requests that vm-service provision more instances for running machine and remote Docker jobs.</td>
<td>VM instances for machine and Remote Docker might not be provisioned, causing you to run out of capacity to run jobs with these executors.</td>
<td>Different overlay for EKS versus GKE.</td>
</tr>
<tr>
<td>vm-service</td>
<td>Machine</td>
<td>Inventory of available vm-service instances, and provisioning of new instances.</td>
<td>Jobs that use machine or remote Docker will fail.</td>
<td></td>
</tr>
<tr>
<td>workflows-conductor-event-consumer</td>
<td>Pipelines</td>
<td>Takes in information from VCS to kick off pipelines.</td>
<td>New Pipelines will not be kicked off when there are changes in the VCS.</td>
<td></td>
</tr>
<tr>
<td>workflows-conductor-grpc-handler</td>
<td>Pipelines</td>
<td>Helps translate the information through gRPC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>web-ui-*</td>
<td>Frontend</td>
<td>Micro Front End (MFE) services used to render the frontend web application GUI.</td>
<td>The respective services page will fail to load. Example: A web-ui-server-admin failure means the server Admin page will fail to load.</td>
<td>The MFEs are used to render the web application located at app.&lt;my domain here&gt;</td>
</tr>
<tr>
<td>Environment</td>
<td>Status</td>
<td>Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>--------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EKS</td>
<td>Tested</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GKE</td>
<td>Tested</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure</td>
<td>Untested</td>
<td>Should work with Minio Azure gateway and Runner.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>Untested</td>
<td>Should work with Minio Digital Ocean gateway and Runner.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenShift</td>
<td>Untested</td>
<td>Known to not work.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rancher</td>
<td>Untested</td>
<td>Should work with Minio and Runner.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CircleCI Server v3.x What’s New

Server 3.x is now generally available. The newest version of server offers the ability to scale under heavy workloads, all within your own Kubernetes cluster and private network, while still enjoying the full CircleCI cloud experience.

Server 3.x includes the latest CircleCI features, such as orbs, scheduled workflows, matrix jobs, and more. For existing customers interested in migrating from 2.19 to 3.x, contact your customer success manager. Server 3.x will receive monthly patch releases and quarterly feature releases.

Release 3.4.1

Upgrade notes

Before upgrading to v3.4.x, delete the deployment named `circleci-server-kube-state-metrics`:

- Run `kubectl delete deployment/circleci-server-kube-state-metrics --cascade=orphan`
- Deploy the app from the KOTS Admin Console

Fixes

- Kong resource limits have been increased. The previous limits were affecting the stability of some server installations.
- Fixed a bug that was preventing distributor-external from running in certain environments.
- The KOTS config has been updated to allow private loadbalancers when ACM is in use.

Known issues

- The CircleCI Build Agent can now be pulled from a custom Docker registry if required. For more information contact customer support.
- You can now use Amazon Certificate Manager (ACM) to manage your TLS certificates. For more information see the Server v3.x Installation Guide.
- Kubernetes v1.16 - v1.23 are now supported.
- Workload Identities for installations on GCP are now supported. Workload Identities can be used as an alternative to static credentials. For more information see the Server v3.x Installation Guide.

Release 3.4.0

Upgrade notes

Before upgrading to v3.4.x, delete the deployment named `circleci-server-kube-state-metrics`:

- Run `kubectl delete deployment/circleci-server-kube-state-metrics --cascade=orphan`
- Deploy the app from the KOTS Admin Console
New Features

- Android images for the machine executor are now available. For more information, see the Using Android Images with the Machine Executor guide.
- The CircleCI Build Agent can now be pulled from a custom Docker registry if required. For more information contact customer support.
- You can now use Amazon Certificate Manager (ACM) to manage your TLS certificates. For more information see the Server v3.x Installation Guide.
- Kubernetes v1.16 - v1.23 are now supported.
- Workload Identities for installations on GCP are now supported. Workload Identities can be used as an alternative to static credentials. For more information see the Server v3.x Installation Guide.

Fixes

- Fixed a bug that was causing the jobs page and step output access to run very slow in the CircleCI web app.
- Fixed a bug that was causing the workflows conductor pod to crash and cause issues with StatsD metrics.

Known Issues

- Prometheus is broken in KOTS versions 1.65.0 - 1.67.0. If you rely on this feature, do not upgrade your KOTS version until this issue has been resolved.
- Retry with SSH for jobs using the machine executor advertises a private IP address. For this reason, retry with SSH for jobs using the machine executor works as standard for private installations, but for public installs you would need to ensure that you can access the private IP advertised. For example, by using a VPN into your VPC.
- CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.
- The KOTS admin console cannot be upgraded if your installation is set up to be behind a proxy. The proxy settings will be deleted and cause the KOTS admin console to break.

Release 3.3.1

Fixes

- CircleCI runner can now be used when server is installed behind a proxy.
- Fixed a bug that was causing some intermittent broken dependency caches.
- Removed outdated cert trust stores from some images. They were found to be causing access issues to some server installations.
- Self-signed certificates or private certificate authorities are now supported when using GitHub Enterprise.
- Fixed a bug that was affecting runner updates.
SSH reruns now work when server is installed behind a proxy.

Replaced deprecated GitHub API endpoint for teams.

**Known issues**

- Retry with SSH for jobs using the machine executor advertises a private IP address. For this reason, retry with SSH for jobs using the machine executor works as standard for private installations, but for public installs you would need to ensure that you can access the private IP advertised, for example, by using a VPN into your VPC.
- CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.
- The KOTS Admin Console cannot be upgraded if your installation is set up behind a proxy. The proxy settings will be deleted and cause the KOTS Admin Console to break.

**Release 3.3.0**

**New features**

- Nomad Autoscaler can now be used to scale Nomad clients. For more information see the [execution environments installation docs](#).
- Webhooks are now available.
- The Insights dashboard is now available.
- IRSA (AWS) can now be used as an alternative to keys for object storage authentication.
- The email address from which build notifications are sent is now configurable from the KOTS Admin Console.
- We have replaced Traefik with Kong as our reverse proxy. However, in order to minimize disruption when upgrading, we chose not to rename the service used by kong. Therefore, you will see a service named `circleci-server-traefik`, however, this service is actually for Kong.

**Fixes**

- Upgraded Python to v3 in Vault container.
- Docs improvements on using the shared VPC architecture in GCP.
- The JVM heap size has been updated so that output-processor can use up to 80% of the pod memory limit.

**Known issues**

- Updating GitHub Enterprise with a modified Let’s Encrypt certificate is unsupported.
- Let’s Encrypt’s new root certificate isrgrootx1 is not trusted.
- Retry with SSH for jobs using the machine executor advertises a private IP address. For this reason, retry with SSH for jobs using the machine executor works as standard for private installations, but for public installs you would need to ensure that you can access the private IP advertised, for example, by
using a VPN into your VPC.

- It is currently possible for multiple organizations under the same CircleCI server account to create contexts with identical names. This should be avoided, as it could cause errors and unexpected behavior.

- CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.

- The KOTS Admin Console cannot be upgraded if your installation is set up behind a proxy. The proxy settings will be deleted and cause the KOTS Admin Console to break.

- Runner cannot be used when server is installed behind a proxy.

Release 3.2.2

Upgrade notes

- The rerun workflow endpoint now returns workflow ID rather than the message accepted.

Fixes

- TLS is terminated outside of frontend so the SSL server has been completely removed from the frontend container.

- Moved the default certificate logic from KOTS to Helm.

- Fixed the build agent image version used in server v3.x. The image used previously was causing problems with runner.

Known issues

- Retry with SSH for jobs using the machine executor advertises a private IP address. For this reason, retry with SSH for jobs using the machine executor. Works as standard for private installations, but for public installs you would need to ensure that you can access the private IP advertised, for example, by using a VPN into your VPC.

- It is currently possible for multiple organizations under the same CircleCI server account to create contexts with identical names. This should be avoided, as it could cause errors and unexpected behavior.

- CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.

- The KOTS Admin Console cannot be upgraded if your installation is set up behind a proxy. The proxy settings will be deleted and cause the KOTS Admin Console to break.

- Runner cannot be used when server is installed behind a proxy.

- Let's Encrypt certificate generation does not work. You need to provide your own certificates or use the default certificates provided.
Release 3.2.1

Upgrade notes

From the KOTS Admin Console, select Version History from the menu bar and click Deploy for server v3.2.0.

See Upgrade notes before upgrading from v3.1.x to v3.2.x.

New features

• Private VMs are now supported for installations on GCP.

Fixes

• mTLS is now disabled by default.
• SSH timeout for VMs has been increased to 10 minutes.
• Private VMs now request private IPs.

Known issues

• Retry with SSH for jobs using the machine executor advertises a private IP address. For this reason, retry with SSH for jobs using the machine executor. Works as standard for private installations, but for public installs you would need to ensure that you can access the private IP advertised, for example, by using a VPN into your VPC.
• It is currently possible for multiple organizations under the same CircleCI server account to create contexts with identical names. This should be avoided, as it could cause errors and unexpected behavior.
• CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.
• The KOTS Admin Console cannot be upgraded if your installation is set up behind a proxy. The proxy settings will be deleted and cause the KOTS Admin Console to break.
• Runner cannot be used when server is installed behind a proxy.
• Let’s Encrypt certificate generation does not work. You need to provide your own certificates or use the default certificates provided.

Release 3.2.0

Upgrade notes

From the KOTS Admin Console, select Version History from the menu bar and click Deploy for server v3.2.0.

When upgrading from server 3.1.x to 3.2, there will be some downtime due to a change to the PostgreSQL pod. There are two issues you could run into with this update, which are covered in the following sections.
**PostgreSQL pod stuck in pending**

If you find that the PostgreSQL pod is stuck in a pending state after upgrading, scale down the pods to 0 and then scale up again by following the steps below.

To check if your PostgreSQL pod is stuck in pending, use the following command:

```bash
$ kubectl get pod -l app.kubernetes.io/name=postgresql
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>postgresql-0</td>
<td>1/1</td>
<td>Pending</td>
<td>0</td>
<td>3m</td>
</tr>
</tbody>
</table>

The following command will scale down pods to 0 and terminate the application pods without any data loss:

```bash
kubectl scale deployment -l layer=application --replicas 0
```

Once all the application-layer pods have finished terminating, do one of the following:

- **either** redeploy the update from the KOTS Admin Console
- **or** run the following two commands to redeploy the pods and return server to a functional state:

  ```bash
  kubectl scale deployment -l layer=application --replicas 1
  ```

  Then scale `output-processor` up with the following command:

  ```bash
  kubectl scale deployment output-processor --replicas 2
  ```

**Traefik pod fails to schedule**

If you find that there are two Traefik pods after upgrading, you need to locate the older pod and remove it to allow the new pod to schedule correctly.

To see the status of your Traefik pod, use the following command:

```bash
$ kubectl get pod -l app=traefik
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>circleci-server-traefik-9d6b86fd8-f7n2x</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>24d</td>
</tr>
<tr>
<td>circleci-server-traefik-cf7d4d7f6-6mb5g</td>
<td>1/1</td>
<td>Error</td>
<td>0</td>
<td>3m</td>
</tr>
</tbody>
</table>

Remove the older Traefik pod with the following command:
kubectl delete pod circleci-server-traefik-<older pod hash>

The new Traefik pod will then start to schedule correctly.

**New features**

- Customers who require a fully private installation can now access a setting in the KOTS Admin Console to ensure public IPs are not assigned to VMs. Note that with this non-public IP setting enabled, a workaround will be needed if SSH access to running jobs is required, for example, by using a VPN into your VPC.
- Customers who manage outbound traffic through a proxy can now configure proxy settings through the KOTS Admin Console. Please see our documentation for specifics on proxy support for server.
- We have expanded the machine execution environment options available to include additional resource classes, sizes, and executors. You now have access to Arm (medium, large), Linux (medium, large, X large, and XX large), and Windows (medium, large, XX large) resource classes.
- The insights API is now available to all server customers. Leverage build and other data to better understand the performance of teams and the health of your build and testing efforts.
- We have revamped the admin UI, and updated our installation instructions, making it easier to set up and manage server.
- You can now supply a custom Linux AMI for VM service.
- SSL termination can now be disabled. If you have put server login behind a firewall, this will enable SSL termination at the firewall.
- You can now control the size of persistent volumes. For larger customers, the initial persistent volume size was too small, by default. You can now set this at install time, providing an easier migration for those customers that require it. For further information see the Internal Database Volume Expansion doc.
- We have added an auto-scaling example to the nomad client terraform.
- You can now choose to serve 'unsafe' build artifacts. Previously this option was hidden, meaning potentially unsafe artifacts were rendered as plain text. For more information see the Build Artifacts doc.

**Fixes**

- The default windows executor was not as documented. We have increased the size to align with documentation and cloud.

**Known issues**

- KOTS admin configuration incorrectly selects the Nomad mTLS as enabled during setup. It should be set to mTLS disabled until after Nomad clients have been deployed.
- Retry with SSH for jobs using the machine executor advertises a private IP address. For this reason, retry with SSH for jobs using the machine executor. Works as standard for private installations. However, for public installs you would need to ensure that you can access the private IP advertised, for example, by using a VPN into your VPC.
• It is currently possible for multiple organizations under the same CircleCI server account to create contexts with identical names. This should be avoided, as it could cause errors and unexpected behavior.

• CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.

• The KOTS Admin Console cannot be upgraded if your installation is set up to be behind a proxy. The proxy settings will be deleted and cause the KOTS Admin Console to break.

• Runner cannot be used when server is installed behind a proxy.

• Let’s Encrypt certificate generation does not work. You need to provide your own certificates or use the default certificates provided.

**Release 3.1.0**

**Upgrade notes**

With this release, the frontend-external load balancer has been removed. The traefik load balancer now handles all incoming traffic. When updating from a previous server 3.x version, you need to update the DNS record that was pointing to the frontend-external load balancer and point it to the circleci-server-traefik load balancer instead. Remember, you can retrieve the external IP address or DNS name of your Traefik load balancer by typing kubectl get svc/circleci-server-traefik in a terminal that has access to the cluster.

To update your DNS record and upgrade your server installation, follow these steps:

1. Retrieve the external IP or DNS name for the Traefik load balancer as described, or by looking the DNS A record for app.<your domain name> - this should already point to your Traefik load balancer.

2. Locate the DNS A record that points to the domain name of your server installation (not the one pointing to the app. subdomain).

3. Edit the A record so that it points to the Traefik load balancer, the same as the app. subdomain record. Your changes might need a couple of minutes to take effect, depending on your DNS service.

Next, from the KOTS Admin Console, select Version History from the menu bar and click Deploy for server v3.1.0.

**New features**

• Telegraf plugins can now be added to server and customized to use third-party monitoring solutions, for example, Datadog. For more information, see the Metrics and Monitoring doc.

• The option to use only private load balancers has been introduced for customers who want a fully private installation. For more information, see the Load Balancers guide.

• Server 3.x hosts build artifacts, test results, and other state in object storage. We support any S3-compatible storage and Google Cloud Storage. For more information, see the Installation guide.

• Dynamic config via setup workflows is now available on server installations. For more information, see our blog post and the Dynamic Configuration docs page.
• Runner is now available on server. For further information, including installation steps, see the Runner docs. Runner allows the use of the macOS executor in server installations and VM service functionality for customers with server installed in a private data centre.

• The frontend load balancer from v3.0 has been removed and replaced with an Ingress resource and the Traefik Ingress controller. This is a breaking change requiring you to reconfigure your DNS. See the What's New in server docs for further information and guidance.

• The following services can now be externalized. For setup information, see the server v3.x installation guide:
  ◦ Postgres
  ◦ MongoDB
  ◦ Vault

• Backup and restore functionality is now available. For more information see the Backup and Restore guide.

• Prometheus is now deployed by default with server to monitor your cluster health and usage. Prometheus can be managed and configured from the KOTS Admin Console. For further information, see the Metrics and Monitoring doc.

• Server now supports the 2XL resource class. The Nomad cluster needs to be large enough to account for larger resource classes.

• The lifecycle of build artifacts and test results can now be configured from the KOTS Admin Console under Storage Object Expiry, including the option to disable the expiration and retain artifacts and test results indefinitely.

**Fixes**

• Resolved a collection of bugs that were leaking sensitive information into CircleCI support bundles:
  ◦ Instances of faulty and partial redactions of secrets were detected, in part due to 3rd party bugs.
  ◦ PostgreSQL leaking sensitive information to STDOUT.
  ◦ Several CircleCI services were logging secrets.

• Tightened network security in the Nomad Terraform module.

• Terraform v0.15.0 and up are now supported.

• Updated installation scripts to use functions supported by most recent versions of Terraform.

• Resolved a bug that was causing machine large builds to be run on the wrong machine type. Machine large builds now correctly use four vCPUs and 16GB of RAM.

• Resolved a bug that caused contexts-service to fail on expiration of Vault client tokens.

• Resolved a bug that was causing legacy-notifier to report readiness prematurely.

• The JVM heap size parameter has been removed for all services. The heap size is set to be half of the memory limit.

• Changes to networking config and certs are now picked up automatically by Traefik. Previously, a restart would have been required.

• Minimum requirements for CPU and memory have changed. For the new values, see the Installation Prerequisites doc.
Known issues

- It is currently possible for multiple organizations under the same CircleCI server account to create contexts with identical names. This should be avoided, as it could cause errors and unexpected behavior.

- CircleCI 1.0 builds are not supported. If an attempt is made to run a 1.0 build, no feedback will be available in the application to indicate the cause of the issue. If a build is run on your installation and does not show up in the CircleCI application, users should be directed to use the CircleCI CLI to validate the project configuration and get details of the possible cause of the issue.

Release 3.0.2

- Resolved a bug relating to artifacts disappearing after 30 days. The default settings for the artifact retention period have been updated to unlimited, and can be adjusted from the KOTS Admin Console.

- Resolved a bug that made Traefik "unaware" of TLS certificate updates without requiring a manual restart of the Traefik pod. The Traefik pod now restarts automatically after any TLS certificate updates go into effect after the initial post-KOTS deployment.

- Resolved a bug in builds-service that was causing pods to crash as a result of running out of memory.

Release 3.0.1

- build_agent version value updated, as the previous version was relying on a vulnerable version of PsExec.

- Due to an issue that was causing duplicated checks in GitHub, environment variables for output-processor were reconfigured.

- Adjusted deployment configuration for vm-service to handle out-of-order database migrations managed by Flyway.
CircleCI Server v3.x FAQ

Does Server 3.0 have a data retention policy?
We do not currently support a defined data retention policy. Data is stored indefinitely on server.

What control is granted over Nomad certificates?
Full control of the certificates, all the way down to mTLS for Nomad.

Is it possible to change or disable the polling time which checks for health status?
No, this is not customizable.

What do the Application Status options in KOTS mean?
Please see the KOTS documentation.