Edit This Page

Reference

This section of the Kubernetes documentation contains references.

- API Reference
- API Client Libraries
- CLI Reference
- Config Reference
- Design Docs

API Reference

- Kubernetes API Overview - Overview of the API for Kubernetes.
- Kubernetes API Versions
  - 1.12
  - 1.11
  - 1.10
  - 1.9
  - 1.8
  - 1.7

API Client Libraries

To call the Kubernetes API from a programming language, you can use client libraries. Officially supported client libraries:

- Kubernetes Go client library
- Kubernetes Python client library
- Kubernetes Java client library
- Kubernetes JavaScript client library

CLI Reference

- kubectl - Main CLI tool for running commands and managing Kubernetes clusters.
  - JSONPath - Syntax guide for using JSONPath expressions with kubectl.
- kubeadm - CLI tool to easily provision a secure Kubernetes cluster.
- kubefed - CLI tool to help you administrate your federated clusters.

Config Reference

- kubelet - The primary *node agent* that runs on each node. The kubelet takes a set of PodSpecs and ensures that the described containers are running and healthy.
- kube-apiserver - REST API that validates and configures data for API objects such as pods, services, replication controllers.
- kube-controller-manager - Daemon that embeds the core control loops shipped with Kubernetes.
- kube-proxy - Can do simple TCP/UDP stream forwarding or round-robin TCP/UDP forwarding across a set of back-ends.
- kube-scheduler - Scheduler that manages availability, performance, and capacity.
- federation-apiserver - API server for federated clusters.
- federation-controller-manager - Daemon that embeds the core control loops shipped with Kubernetes federation.

Design Docs

An archive of the design docs for Kubernetes functionality. Good starting points are Kubernetes Architecture and Kubernetes Design Overview.

Standardized Glossary

This glossary is intended to be a comprehensive, standardized list of Kubernetes terminology. It includes technical terms that are specific to K8s, as well as more general terms that provide useful context.

Filter terms according to their tags:

.

The inner components of Kubernetes.

Related to Kubernetes open-source development.

A resource type that Kubernetes supports by default.

Supported customizations of Kubernetes.

Relevant for a first-time user of Kubernetes.

How Kubernetes components talk to each other (and to programs outside the

cluster).

Starting and maintaining Kubernetes.

Keeping Kubernetes applications safe and secure.

How Kubernetes applications handle persistent data.

Software that makes Kubernetes easier or better to use.

Represents a common type of Kubernetes user.

Applications running on Kubernetes.

Architecture Community Core Object Extension Fundamental Networking Operation Security Storage Tool User Type Workload Select all Deselect all

Click on the [+] indicators below to get a longer explanation for any particular term.

- **Aggregation Layer**LINK

  The aggregation layer lets you install additional Kubernetes-style APIs in your cluster.

  [+]

  When you've configured the Kubernetes API ServerComponent on the master that exposes the Kubernetes API. It is the front-end for the Kubernetes control plane. to support additional APIs, you can add `APIService` objects to "claim" a URL path in the Kubernetes API.

- **Annotation**LINK

  A key-value pair that is used to attach arbitrary non-identifying metadata to objects.

  [+]

  The metadata in an annotation can be small or large, structured or unstructured, and can include characters not permitted by labels. Clients such as tools and libraries can retrieve this metadata.

- **Application Architect**LINK

  A person responsible for the high-level design of an application.

  [+]

  An architect ensures that an app's implementation allows it to interact with its surrounding components in a scalable, maintainable way. Surrounding components include databases, logging infrastructure, and other microservices.

3

- **Application Developer**LINK

  A person who writes an application that runs in a Kubernetes cluster.

  [+]

  An application developer focuses on one part of an application. The scale of their focus may vary significantly in size.

- **Approver**LINK

  A person who can review and approve Kubernetes code contributions.

  [+]

  While code review is focused on code quality and correctness, approval is focused on the holistic acceptance of a contribution. Holistic acceptance includes backwards/forwards compatibility, adhering to API and flag conventions, subtle performance and correctness issues, interactions with other parts of the system, and others. Approver status is scoped to a part of the codebase. Approvers were previously referred to as maintainers.

- **CLA (Contributor License Agreement)**LINK

  Terms under which a contributorSomeone who donates code, documentation, or their time to help the Kubernetes project or community. grants a license to an open source project for their contributions.

  [+]

  CLAs help resolve legal disputes involving contributed material and intellectual property (IP).

- **CNI (Container network interface)**LINK

  Container network interface (CNI) plugins are a type of Network plugin that adheres to the appc/CNI specification.

  [+]

  – For information on Kubernetes and CNI refer to this.
  – For information on Kubernetes and CNI, see "Network plugins".

  CertificateLINK

  A cryptographically secure file used to validate access to the Kubernetes cluster.

  [+]

  Certificates enable applications within a Kubernetes cluster to access the Kubernetes API securely. Certificates validate that clients are allowed to access the API.

- **Cloud Controller Manager**LINK

  Cloud Controller Manager is an alpha feature in 1.8. In upcoming releases it will be the preferred way to integrate Kubernetes with any cloud.

  [+]

  Kubernetes v1.6 contains a new binary called cloud-controller-manager. cloud-controller-manager is a daemon that embeds cloud-specific control loops. These cloud-specific control loops were originally in the kube-controller-manager. Since cloud providers develop and release at a different pace compared to the Kubernetes project, abstracting the provider-specific code to the cloud-controller-manager binary allows cloud vendors to evolve independently from the core Kubernetes code.

- **Cloud Provider**LINK

  Cloud provider is a company that offers cloud computing platform that can run Kubernetes clusters.

  [+]

  Cloud providers or sometime called Cloud Service Provider (CSPs) provides cloud computing platforms. They may offer services such as Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Cloud providers host the Kubernetes cluster and also provide services that interact with the cluster, such as Load Balancers, Storage Classes etc.

- **Cluster**LINK

  A set of machines, called nodes, that run containerized applications managed by Kubernetes.

  [+]

  A cluster has several worker nodes and at least one master node.

- **Cluster Architect**LINK

  A person who designs infrastructure that involves one or more Kubernetes clusters.

  [+]

  Cluster architects are concerned with best practices for distributed systems, for example: high availability and security.

- **Cluster Operator**LINK

  A person who configures, controls, and monitors clusters.

  [+]

Their primary responsibility is keeping a cluster up and running, which may involve periodic maintenance activities or upgrades.

> **Note:** Cluster operators are different from the Operator pattern that extends the Kubernetes API.

Code ContributorLINK

A person who develops and contributes code to the Kubernetes open source codebase.

[+]

They are also an active community memberA continuously active contributor in the K8s community. who participates in one or more Special Interest Groups (SIGs)Community members who collectively manage an ongoing piece or aspect of the larger Kubernetes open source project..

- **ConfigMap**LINK

  An API object used to store non-confidential data in key-value pairs. Can be consumed as environment variables, command-line arguments, or config files in a volumeA directory containing data, accessible to the containers in a pod..

  [+]

  Allows you to decouple environment-specific configuration from your container imagesThe lifecycle hooks expose events in the container management lifecycle and let the user run code when the events occur., so that your applications are easily portable. When storing confidential data use a Secret.

- **Container**LINK

  A lightweight and portable executable image that contains software and all of its dependencies.

  [+]

  Containers decouple applications from underlying host infrastructure to make deployment easier in different cloud or OS environments, and for easier scaling.

- **Container Environment Variables**LINK

  Container environment variables are name=value pairs that provide useful information into containers running in a Pod.

  [+]

  Container environment variables provide information that is required by the running containerized applications along with information about im-

portant resources to the ContainersThe lifecycle hooks expose events in the container management lifecycle and let the user run code when the events occur.. For example, file system details, information about the container itself, and other cluster resources such as service endpoints.

- **Container Lifecycle Hooks**LINK

  The lifecycle hooks expose events in the ContainerThe lifecycle hooks expose events in the container management lifecycle and let the user run code when the events occur.container management lifecycle and let the user run code when the events occur.

  [+]

  Two hooks are exposed to Containers: PostStart which executes immediately after a container is created and PreStop which is blocking and is called immediately before a container is terminated.

- **Container Storage Interface (CSI)**LINK

  The Container Storage Interface (CSI) defines a standard interface to expose storage systems to containers.

  [+]

  CSI allows vendors to create custom storage plugins for Kubernetes without adding them to the Kubernetes repository (out-of-tree plugins). To use a CSI driver from a storage provider, you must first deploy it to your cluster. You will then be able to create a Storage ClassA StorageClass provides a way for administrators to describe different available storage types. that uses that CSI driver.

  – CSI in the Kubernetes documentation
  – List of available CSI drivers

  ContributorLINK

  Someone who donates code, documentation, or their time to help the Kubernetes project or community.

  [+]

  Contributions include pull requests (PRs), issues, feedback, special interest groups (SIG)Community members who collectively manage an ongoing piece or aspect of the larger Kubernetes open source project. participation, or organizing community events.

- **Controller**LINK

  A control loop that watches the shared state of the cluster through the apiserverComponent on the master that exposes the Kubernetes API. It is the front-end for the Kubernetes control plane. and makes changes attempting to move the current state towards the desired state.

[+]

Examples of controllers that ship with Kubernetes today are the replication controller, endpoints controller, namespace controller, and serviceaccounts controller.

- **CronJob**LINK

Manages a Job that runs on a periodic schedule.

[+]

Similar to a line in a *crontab* file, a Cronjob object specifies a schedule using the Cron format.

- **CustomResourceDefinition**LINK

Custom code that defines a resource to add to your Kubernetes API server without building a complete custom server.

[+]

Custom Resource Definitions let you extend the Kubernetes API for your environment if the publicly supported API resources can't meet your needs.

- **DaemonSet**LINK

Ensures a copy of a PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. is running across a set of nodes in a clusterA set of machines, called nodes, that run containerized applications managed by Kubernetes..

[+]

Used to deploy system daemons such as log collectors and monitoring agents that typically must run on every NodeA node is a worker machine in Kubernetes..

- **Deployment**LINK

An API object that manages a replicated application.

[+]

Each replica is represented by a PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster., and the Pods are distributed among the nodes of a cluster.

- **Developer (disambiguation)**LINK

May refer to: Application DeveloperA person who writes an application that runs in a Kubernetes cluster., Code ContributorA person who develops and contributes code to the Kubernetes open source codebase., or

Platform DeveloperA person who customizes the Kubernetes platform to fit the needs of their project..

[+]

This overloaded term may have different meanings depending on the context

- **Downstream (disambiguation)**LINK

  May refer to: code in the Kubernetes ecosystem that depends upon the core Kubernetes codebase or a forked repo.

  [+]

  – In the **Kubernetes Community**: Conversations often use *downstream* to mean the ecosystem, code, or third-party tools that rely on the core Kubernetes codebase. For example, a new feature in Kubernetes may be adopted by applications *downstream* to improve their functionality.
  – In **GitHub** or **git**: The convention is to refer to a forked repo as *downstream*, whereas the source repo is considered *upstream*.

  Dynamic Volume ProvisioningLINK

  Allows users to request automatic creation of storage VolumesA directory containing data, accessible to the containers in a pod..

  [+]

  Dynamic provisioning eliminates the need for cluster administrators to pre-provision storage. Instead, it automatically provisions storage by user request. Dynamic volume provisioning is based on an API object, StorageClassA StorageClass provides a way for administrators to describe different available storage types., referring to a Volume PluginA Volume Plugin enables integration of storage within a Pod. that provisions a VolumeA directory containing data, accessible to the containers in a pod. and the set of parameters to pass to the Volume Plugin.

- **Flexvolume**LINK

  Flexvolume is an interface for creating out-of-tree volume plugins. The Container Storage InterfaceThe Container Storage Interface (CSI) defines a standard interface to expose storage systems to containers. is a newer interface which addresses several problems with Flexvolumes.

  [+]

  Flexvolumes enable users to write their own drivers and add support for their volumes in Kubernetes. FlexVolume driver binaries and dependencies must be installed on host machines. This requires root access. The Storage SIG suggests implementing a CSIThe Container Storage Interface

(CSI) defines a standard interface to expose storage systems to containers. driver if possible since it addresses the limitations with Flexvolumes.

- – Flexvolume in the Kubernetes documentation
- – More information on Flexvolumes
- – Volume Plugin FAQ for Storage Vendors

Helm ChartLINK

A package of pre-configured Kubernetes resources that can be managed with the Helm tool.

[+]

Charts provide a reproducible way of creating and sharing Kubernetes applications. A single chart can be used to deploy something simple, like a memcached Pod, or something complex, like a full web app stack with HTTP servers, databases, caches, and so on.

- **Horizontal Pod Autoscaler**LINK

  An API resource that automatically scales the number of pod replicas based on targeted CPU utilization or custom metric targets.

  [+]

  HPA is typically used with Replication ControllersKubernetes service that ensures a specific number of instances of a pod are always running., DeploymentsAn API object that manages a replicated application., or Replica Sets. It cannot be applied to objects that cannot be scaled, for example DaemonSetsEnsures a copy of a Pod is running across a set of nodes in a cluster..

- **Image**LINK

  Stored instance of a container that holds a set of software needed to run an application.

  [+]

  A way of packaging software that allows it to be stored in a container registry, pulled to a local system, and run as an application. Meta data is included in the image that can indicate what executable to run, who built it, and other information.

- **Ingress**LINK

  An API object that manages external access to the services in a cluster, typically HTTP.

  [+]

  Ingress can provide load balancing, SSL termination and name-based virtual hosting.

- **Init Container**LINK

  One or more initialization containers that must run to completion before any app containers run.

  [+]

  Initialization (init) containers are like regular app containers, with one difference: init containers must run to completion before any app containers can start. Init containers run in series: each init container must run to completion before the next init container begins.

- **Istio**LINK

  An open platform (not Kubernetes-specific) that provides a uniform way to integrate microservices, manage traffic flow, enforce policies, and aggregate telemetry data.

  [+]

  Adding Istio does not require changing application code. It is a layer of infrastructure between a service and the network, which when combined with service deployments, is commonly referred to as a service mesh. Istio's control plane abstracts away the underlying cluster management platform, which may be Kubernetes, Mesosphere, etc.

- **Job**LINK

  A finite or batch task that runs to completion.

  [+]

  Creates one or more PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. objects and ensures that a specified number of them successfully terminate. As Pods successfully complete, the Job tracks the successful completions.

- **Kops**LINK

  A CLI tool that helps you create, destroy, upgrade and maintain production-grade, highly available, Kubernetes clusters. *NOTE: Officially supports AWS only, with GCE and VMware vSphere in alpha.*

  [+]

  `kops` provisions your cluster with:

  - Fully automated installation
  - DNS-based cluster identification
  - Self-healing: everything runs in Auto-Scaling Groups
  - Limited OS support (Debian preferred, Ubuntu 16.04 supported, early support for CentOS & RHEL)
  - High availability (HA) support
  - The ability to directly provision, or generate terraform manifests

You can also build your own cluster using KubeadmA tool for quickly installing Kubernetes and setting up a secure cluster. as a building block. `kops` builds on the kubeadm work.

- **Kubeadm**LINK

  A tool for quickly installing Kubernetes and setting up a secure cluster.

  [+]

  You can use kubeadm to install both the control plane and the worker node components.

- **Kubectl**LINK

  A command line tool for communicating with a Kubernetes APIThe application that serves Kubernetes functionality through a RESTful interface and stores the state of the cluster. server.

  [+]

  You can use kubectl to create, inspect, update, and delete Kubernetes objects.

- **Kubelet**LINK

  An agent that runs on each node in the cluster. It makes sure that containers are running in a pod.

  [+]

  The kubelet takes a set of PodSpecs that are provided through various mechanisms and ensures that the containers described in those PodSpecs are running and healthy. The kubelet doesn't manage containers which were not created by Kubernetes.

- **Kubernetes API**LINK

  The application that serves Kubernetes functionality through a RESTful interface and stores the state of the cluster.

  [+]

  Kubernetes resources and "records of intent" are all stored as API objects, and modified via RESTful calls to the API. The API allows configuration to be managed in a declarative way. Users can interact with the Kubernetes API directly, or via tools like `kubectl`. The core Kubernetes API is flexible and can also be extended to support custom resources.

- **Label**LINK

  Tags objects with identifying attributes that are meaningful and relevant to users.

  [+]

Labels are key/value pairs that are attached to objects such as PodsThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster.. They are used to organize and to select subsets of objects.

- **Managed Service**LINK

  A software offering maintained by a third-party provider.

  [+]

  Some examples of Managed Services are AWS EC2, Azure SQL Database, and GCP Pub/Sub, but they can be any software offering that can be used by an application. Service Catalog provides a way to list, provision, and bind with Managed Services offered by Service BrokersAn endpoint for a set of Managed Services offered and maintained by a third-party..

- **Member**LINK

  A continuously active contributorSomeone who donates code, documentation, or their time to help the Kubernetes project or community. in the K8s community.

  [+]

  Members can have issues and PRs assigned to them and participate in special interest groups (SIGs)Community members who collectively manage an ongoing piece or aspect of the larger Kubernetes open source project. through GitHub teams. Pre-submit tests are automatically run for members' PRs. A member is expected to remain an active contributor to the community.

- **Minikube**LINK

  A tool for running Kubernetes locally.

  [+]

  Minikube runs a single-node cluster inside a VM on your computer.

- **Name**LINK

  A client-provided string that refers to an object in a resource URL, such as `/api/v1/pods/some-name`.

  [+]

  Only one object of a given kind can have a given name at a time. However, if you delete the object, you can make a new object with the same name.

- **Namespace**LINK

  An abstraction used by Kubernetes to support multiple virtual clusters on the same physical clusterA set of machines, called nodes, that run containerized applications managed by Kubernetes..

[+]

Namespaces are used to organize objects in a cluster and provide a way to divide cluster resources. Names of resources need to be unique within a namespace, but not across namespaces.

- **Network Policy**LINK

  A specification of how groups of Pods are allowed to communicate with each other and with other network endpoints.

  [+]

  Network Policies help you declaratively configure which Pods are allowed to connect to each other, which namespaces are allowed to communicate, and more specifically which port numbers to enforce each policy on. `NetworkPolicy` resources use labels to select Pods and define rules which specify what traffic is allowed to the selected Pods. Network Policies are implemented by a supported network plugin provided by a network provider. Be aware that creating a network resource without a controller to implement it will have no effect.

- **Node**LINK

  A node is a worker machine in Kubernetes.

  [+]

  A worker machine may be a VM or physical machine, depending on the cluster. It has the ServicesAn API object that describes how to access applications, such as a set of Pods, and can describe ports and load-balancers. necessary to run PodsThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. and is managed by the master components. The ServicesAn API object that describes how to access applications, such as a set of Pods, and can describe ports and load-balancers. on a node include Docker, kubelet and kube-proxy.

- **Persistent Volume**LINK

  An API object that represents a piece of storage in the cluster. Available as a general, pluggable resource that persists beyond the lifecycle of any individual PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster..

  [+]

  PersistentVolumes (PVs) provide an API that abstracts details of how storage is provided from how it is consumed. PVs are used directly in scenarios where storage can be created ahead of time (static provisioning). For scenarios that require on-demand storage (dynamic provisioning), PersistentVolumeClaims (PVCs) are used instead.

- **Persistent Volume Claim**LINK

  Claims storage resources defined in a PersistentVolume so that it can be mounted as a volume in a container.

  [+]

  Specifies the amount of storage, how the storage will be accessed (read-only, read-write and/or exclusive) and how it is reclaimed (retained, recycled or deleted). Details of the storage itself are in the PersistentVolume specification.

- **Platform Developer**LINK

  A person who customizes the Kubernetes platform to fit the needs of their project.

  [+]

  A platform developer may, for example, use Custom Resources or Extend the Kubernetes API with the aggregation layer to add functionality to their instance of Kubernetes, specifically for their application. Some Platform Developers are also contributorsSomeone who donates code, documentation, or their time to help the Kubernetes project or community. and develop extensions which are contributed to the Kubernetes community. Others develop closed-source commercial or site-specific extensions.

- **Pod**LINK

  The smallest and simplest Kubernetes object. A Pod represents a set of running containersThe lifecycle hooks expose events in the container management lifecycle and let the user run code when the events occur. on your cluster.

  [+]

  A Pod is typically set up to run a single primary container. It can also run optional sidecar containers that add supplementary features like logging. Pods are commonly managed by a DeploymentAn API object that manages a replicated application..

- **Pod Security Policy**LINK

  Enables fine-grained authorization of PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. creation and updates.

  [+]

  A cluster-level resource that controls security sensitive aspects of the Pod specification. The `PodSecurityPolicy` objects define a set of conditions that a Pod must run with in order to be accepted into the system, as well as

defaults for the related fields. Pod Security Policy control is implemented as an optional admission controller.

- **PodPreset**LINK

  An API object that injects information such as secrets, volume mounts, and environment variables into pods at creation time.

  [+]

  This object chooses the pods to inject information into using standard selectors. This allows the podspec definitions to be nonspecific, decoupling the podspec from environment specific configuration.

- **Quantity**LINK

  A whole-number representation of small or large numbers using SI suffixes.

  [+]

  Quantities are representations of small or large numbers using a compact, whole-number notation with SI suffixes. Fractional numbers are represented using milli units, while large numbers can be represented using kilo, mega, or giga units.

  For instance, the number `1.5` is represented as `1500m`, while the number `1000` can be represented as `1k`, and `1000000` as `1M`. You can also specify binary-notation suffixes; the number 2048 can be written as `2Ki`.

  The accepted decimal (power-of-10) units are `m` (milli), `k` (kilo, intentionally lowercase), `M` (mega), `G` (giga), `T` (terra), `P` (peta), `E` (exa).

  The accepted binary (power-of-2) units are `Ki` (kibi), `Mi` (mebi), `Gi` (gibi), `Ti` (tebi), `Pi` (pebi), `Ei` (exbi).

- **RBAC (Role-Based Access Control)**LINK

  Manages authorization decisions, allowing admins to dynamically configure access policies through the Kubernetes APIThe application that serves Kubernetes functionality through a RESTful interface and stores the state of the cluster..

  [+]

  RBAC utilizes *roles*, which contain permission rules, and *role bindings*, which grant the permissions defined in a role to a set of users.

- **ReplicaSet**LINK

  ReplicaSet is the next-generation Replication Controller.

  [+]

  ReplicaSet, like ReplicationController, ensures that a specified number of pods replicas are running at one time. ReplicaSet supports the new set-

based selector requirements as described in the labels user guide, whereas a Replication Controller only supports equality-based selector requirements.

- **Replication Controller**LINK

  Kubernetes service that ensures a specific number of instances of a pod are always running.

  [+]

  Will automatically add or remove running instances of a pod, based on a set value for that pod. Allows the pod to return to the defined number of instances if pods are deleted or if too many are started by mistake.

- **Resource Quotas**LINK

  Provides constraints that limit aggregate resource consumption per NamespaceAn abstraction used by Kubernetes to support multiple virtual clusters on the same physical cluster..

  [+]

  Limits the quantity of objects that can be created in a namespace by type, as well as the total amount of compute resources that may be consumed by resources in that project.

- **Reviewer**LINK

  A person who reviews code for quality and correctness on some part of the project.

  [+]

  Reviewers are knowledgeable about both the codebase and software engineering principles. Reviewer status is scoped to a part of the codebase.

- **SIG (special interest group)**LINK

  Community membersA continuously active contributor in the K8s community. who collectively manage an ongoing piece or aspect of the larger Kubernetes open source project.

  [+]

  Members within a SIG have a shared interest in advancing a specific area, such as architecture, API machinery, or documentation. SIGs must follow the SIG Governance guidelines but can have their own contribution policy and channels of communication.

  For more information, see the kubernetes/community repo and the current list of SIGs and Working Groups.

- **Secret**LINK

Stores sensitive information, such as passwords, OAuth tokens, and ssh keys.

[+]

Allows for more control over how sensitive information is used and reduces the risk of accidental exposure, including encryption at rest. A PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. references the secret as a file in a volume mount or by the kubelet pulling images for a pod. Secrets are great for confidential data and ConfigMaps for non-confidential data.

- **Security Context**LINK

  The securityContext field defines privilege and access control settings for a Pod or Container, including the runtime UID and GID.

  [+]

  The securityContext field in a PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. (applying to all containers) or container is used to set the user (runAsUser) and group (fsGroup), capabilities, privilege settings, and security policies (SELinux/AppArmor/Seccomp) that container processes use.

- **Selector**LINK

  Allows users to filter a list of resources based on labels.

  [+]

  Selectors are applied when querying lists of resources to filter them by LabelsTags objects with identifying attributes that are meaningful and relevant to users..

- **Service**LINK

  An API object that describes how to access applications, such as a set of PodsThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster., and can describe ports and load-balancers.

  [+]

  The access point can be internal or external to the cluster.

- **Service Account**LINK

  Provides an identity for processes that run in a PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster..

  [+]

When processes inside Pods access the cluster, they are authenticated by the API server as a particular service account, for example, `default`. When you create a Pod, if you do not specify a service account, it is automatically assigned the default service account in the same namespace NamespaceAn abstraction used by Kubernetes to support multiple virtual clusters on the same physical cluster..

- **Service Broker**LINK

  An endpoint for a set of Managed ServicesA software offering maintained by a third-party provider. offered and maintained by a third-party.

  [+]

  Service BrokersAn endpoint for a set of Managed Services offered and maintained by a third-party. implement the Open Service Broker API spec and provide a standard interface for applications to use their Managed Services. Service Catalog provides a way to list, provision, and bind with Managed Services offered by Service Brokers.

- **Service Catalog**LINK

  An extension API that enables applications running in Kubernetes clusters to easily use external managed software offerings, such as a datastore service offered by a cloud provider.

  [+]

  It provides a way to list, provision, and bind with external Managed ServicesA software offering maintained by a third-party provider. from Service BrokersAn endpoint for a set of Managed Services offered and maintained by a third-party. without needing detailed knowledge about how those services are created or managed.

- **StatefulSet**LINK

  Manages the deployment and scaling of a set of PodsThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster., *and provides guarantees about the ordering and uniqueness* of these Pods.

  [+]

  Like a DeploymentAn API object that manages a replicated application., a StatefulSet manages Pods that are based on an identical container spec. Unlike a Deployment, a StatefulSet maintains a sticky identity for each of their Pods. These pods are created from the same spec, but are not interchangeable: each has a persistent identifier that it maintains across any rescheduling.

  A StatefulSet operates under the same pattern as any other Controller. You define your desired state in a StatefulSet *object*, and the StatefulSet

controller makes any necessary updates to get there from the current state.

- **Storage Class**LINK

  A StorageClass provides a way for administrators to describe different available storage types.

  [+]

  StorageClasses can map to quality-of-service levels, backup policies, or to arbitrary policies determined by cluster administrators. Each Storage-Class contains the fields `provisioner`, `parameters`, and `reclaimPolicy`, which are used when a Persistent VolumeAn API object that represents a piece of storage in the cluster. Available as a general, pluggable resource that persists beyond the lifecycle of any individual Pod. belonging to the class needs to be dynamically provisioned. Users can request a particular class using the name of a StorageClass object.

- **UID**LINK

  A Kubernetes systems-generated string to uniquely identify objects.

  [+]

  Every object created over the whole lifetime of a Kubernetes cluster has a distinct UID. It is intended to distinguish between historical occurrences of similar entities.

- **Upstream (disambiguation)**LINK

  May refer to: core Kubernetes or the source repo from which a repo was forked.

  [+]

  - In the **Kubernetes Community**: Conversations often use *upstream* to mean the core Kubernetes codebase, which the general ecosystem, other code, or third-party tools relies upon. For example, community members may suggest that a feature is moved upstream so that it is in the core codebase instead of in a plugin or third-party tool.
  - In **GitHub** or **git**: The convention is to refer to a source repo as *upstream*, whereas the forked repo is considered *downstream.*

  VolumeLINK

  A directory containing data, accessible to the containers in a podThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster..

  [+]

  A Kubernetes volume lives as long as the podThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your

cluster. that encloses it. Consequently, a volume outlives any containersThe lifecycle hooks expose events in the container management lifecycle and let the user run code when the events occur. that run within the podThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster., and data is preserved across containerThe lifecycle hooks expose events in the container management lifecycle and let the user run code when the events occur. restarts.

- **Volume Plugin**LINK

  A Volume Plugin enables integration of storage within a PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster..

  [+]

  A Volume Plugin lets you attach and mount storage volumes for use by a PodThe smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster.. Volume plugins can be *in tree* or *out of tree*. *In tree* plugins are part of the Kubernetes code repository and follow its release cycle. *Out of tree* plugins are developed independently.

- **WG (working group)**LINK

  Facilitates the discussion and/or implementation of a short-lived, narrow, or decoupled project for a committee, SIGCommunity members who collectively manage an ongoing piece or aspect of the larger Kubernetes open source project., or cross-SIG effort.

  [+]

  Working groups are a way of organizing people to accomplish a discrete task, and are relatively easy to create and deprecate when inactive.

  For more information, see the kubernetes/community repo and the current list of SIGs and working groups.

- **docker**LINK

  Docker is a software technology providing operating-system-level virtualization also known as containers.

  [+]

  Docker uses the resource isolation features of the Linux kernel such as cgroups and kernel namespaces, and a union-capable file system such as OverlayFS and others to allow independent "containers" to run within a single Linux instance, avoiding the overhead of starting and maintaining virtual machines (VMs).

- **etcd**LINK

Consistent and highly-available key value store used as Kubernetes' backing store for all cluster data.

[+]

Always have a backup plan for etcd's data for your Kubernetes cluster. For in-depth information on etcd, see etcd documentation.

- **kube-apiserver**LINK

Component on the master that exposes the Kubernetes API. It is the front-end for the Kubernetes control plane.

[+]

It is designed to scale horizontally – that is, it scales by deploying more instances. See Building High-Availability Clusters.

- **kube-controller-manager**LINK

Component on the master that runs controllersA control loop that watches the shared state of the cluster through the apiserver and makes changes attempting to move the current state towards the desired state..

[+]

Logically, each controllerA control loop that watches the shared state of the cluster through the apiserver and makes changes attempting to move the current state towards the desired state. is a separate process, but to reduce complexity, they are all compiled into a single binary and run in a single process.

- **kube-proxy**LINK

`kube-proxy` is a network proxy that runs on each node in the cluster.

[+]

`kube-proxy` is responsible for request forwarding. `kube-proxy` allows TCP and UDP stream forwarding or round robin TCP and UDP forwarding across a set of backend functions.

- **kube-scheduler**LINK

Component on the master that watches newly created pods that have no node assigned, and selects a node for them to run on.

[+]

Factors taken into account for scheduling decisions include individual and collective resource requirements, hardware/software/policy constraints, affinity and anti-affinity specifications, data locality, inter-workload interference and deadlines.

Edit This Page

Kubernetes Issue Tracker

Work on Kubernetes code is tracked using GitHub Issues.

Edit This Page

Kubernetes Security and Disclosure Information

This page describes Kubernetes security and disclosure information.

- Security Announcements
- Report a Vulnerability
- Security Vulnerability Response
- Public Disclosure Timing

Security Announcements

Join the kubernetes-announce group for emails about security and major API announcements.

Report a Vulnerability

We're extremely grateful for security researchers and users that report vulnerabilities to the Kubernetes Open Source Community. All reports are thoroughly investigated by a set of community volunteers.

To make a report, please email the private security@kubernetes.io list with the security details and the details expected for all Kubernetes bug reports.

You may encrypt your email to this list using the GPG keys of the Product Security Team members. Encryption using GPG is NOT required to make a disclosure.

When Should I Report a Vulnerability?

- You think you discovered a potential security vulnerability in Kubernetes
- You are unsure how a vulnerability affects Kubernetes
- You think you discovered a vulnerability in another project that Kubernetes depends on (e.g. docker, rkt, etcd)

When Should I NOT Report a Vulnerability?

- You need help tuning Kubernetes components for security
- You need help applying security related updates
- Your issue is not security related

Security Vulnerability Response

Each report is acknowledged and analyzed by Product Security Team members within 3 working days. This will set off the Security Release Process.

Any vulnerability information shared with Product Security Team stays within Kubernetes project and will not be disseminated to other projects unless it is necessary to get the issue fixed.

As the security issue moves from triage, to identified fix, to release planning we will keep the reporter updated.

Public Disclosure Timing

A public disclosure date is negotiated by the Kubernetes product security team and the bug submitter. We prefer to fully disclose the bug as soon as possible once a user mitigation is available. It is reasonable to delay disclosure when the bug or the fix is not yet fully understood, the solution is not well-tested, or for vendor coordination. The timeframe for disclosure is from immediate (especially if it's already publicly known) to a few weeks. As a basic default, we expect report date to disclosure date to be on the order of 7 days. The Kubernetes product security team holds the final say when setting a disclosure date.

Edit This Page

Kubernetes Deprecation Policy

This document details the deprecation policy for various facets of the system.

- Deprecating parts of the API

- Deprecating a flag or CLI
- Deprecating a feature or behavior
- Exceptions

Kubernetes is a large system with many components and many contributors. As with any such software, the feature set naturally evolves over time, and sometimes a feature may need to be removed. This could include an API, a flag, or even an entire feature. To avoid breaking existing users, Kubernetes follows a deprecation policy for aspects of the system that are slated to be removed.

Deprecating parts of the API

Since Kubernetes is an API-driven system, the API has evolved over time to reflect the evolving understanding of the problem space. The Kubernetes API is actually a set of APIs, called "API groups", and each API group is independently versioned. API versions fall into 3 main tracks, each of which has different policies for deprecation:

Example	Track
v1	GA (generally available, stable)
v1beta1	Beta (pre-release)
v1alpha1	Alpha (experimental)

A given release of Kubernetes can support any number of API groups and any number of versions of each.

The following rules govern the deprecation of elements of the API. This includes:

- REST resources (aka API objects)
- Fields of REST resources
- Annotations on REST resources, including "beta" annotations but not including "alpha" annotations.
- Enumerated or constant values
- Component config structures

These rules are enforced between official releases, not between arbitrary commits to master or release branches.

Rule #1: API elements may only be removed by incrementing the version of the API group.

Once an API element has been added to an API group at a particular version, it can not be removed from that version or have its behavior significantly changed, regardless of track.

> **Note:** For historical reasons, there are 2 "monolithic" API groups - "core" (no group name) and "extensions". Resources will incre-

25

mentally be moved from these legacy API groups into more domain-specific API groups.

Rule #2: API objects must be able to round-trip between API versions in a given release without information loss, with the exception of whole REST resources that do not exist in some versions.

For example, an object can be written as v1 and then read back as v2 and converted to v1, and the resulting v1 resource will be identical to the original. The representation in v2 might be different from v1, but the system knows how to convert between them in both directions. Additionally, any new field added in v2 must be able to round-trip to v1 and back, which means v1 might have to add an equivalent field or represent it as an annotation.

Rule #3: An API version in a given track may not be deprecated until a new API version at least as stable is released.

GA API versions can replace GA API versions as well as beta and alpha API versions. Beta API versions *may not* replace GA API versions.

Rule #4a: Other than the most recent API versions in each track, older API versions must be supported after their announced deprecation for a duration of no less than:

- **GA: 12 months or 3 releases (whichever is longer)**
- **Beta: 9 months or 3 releases (whichever is longer)**
- **Alpha: 0 releases**

This covers the maximum supported version skew of 2 releases.

> **Note:** Until #52185 is resolved, no API versions that have been persisted to storage may be removed. Serving REST endpoints for those versions may be disabled (subject to the deprecation timelines in this document), but the API server must remain capable of decoding/converting previously persisted data from storage.

Rule #4b: The "preferred" API version and the "storage version" for a given group may not advance until after a release has been made that supports both the new version and the previous version

Users must be able to upgrade to a new release of Kubernetes and then roll back to a previous release, without converting anything to the new API version or suffering breakages (unless they explicitly used features only available in the newer version). This is particularly evident in the stored representation of objects.

All of this is best illustrated by examples. Imagine a Kubernetes release, version X, which introduces a new API group. A new Kubernetes release is made every approximately 3 months (4 per year). The following table describes which API versions are supported in a series of subsequent releases.

Release	API Versions	Preferred/Storage Version	Notes
X	v1alpha1	v1alpha1	
X+1	v1alpha2	v1alpha2	• v1alpha1 is removed, "action required" relnote
X+2	v1beta1	v1beta1	• v1alpha2 is removed, "action required" relnote
X+3	v1beta2, v1beta1 (deprecated)	v1beta1	• v1beta1 is deprecated, "action required" relnote
X+4	v1beta2, v1beta1 (deprecated)	v1beta2	
X+5	v1, v1beta1 (deprecated), v1beta2 (deprecated)	v1beta2	• v1beta2 is deprecated, "action required" relnote
X+6	v1, v1beta2 (deprecated)	v1	• v1beta1 is removed, "action required" relnote
X+7	v1, v1beta2 (deprecated)	v1	
X+8	v2alpha1, v1	v1	• v1beta2 is removed, "action required" relnote

Release	API Versions	Preferred/Storage Version	Notes
X+9	v2alpha2, v1	v1	• v2alpha1 is removed, "action required" relnote
X+10	v2beta1, v1	v1	• v2alpha2 is removed, "action required" relnote
X+11	v2beta2, v2beta1 (deprecated), v1	v1	• v2beta1 is deprecated, "action required" relnote
X+12	v2, v2beta2 (deprecated), v2beta1 (deprecated), v1 (deprecated)	v1	• v2beta2 is deprecated, "action required" relnote • v1 is deprecated, "action required" relnote
X+13	v2, v2beta1 (deprecated), v2beta2 (deprecated), v1 (deprecated)	v2	
X+14	v2, v2beta2 (deprecated), v1 (deprecated)	v2	• v2beta1 is removed, "action required" relnote

Release	API Versions	Preferred/Storage Version	Notes
X+15	v2, v1 (deprecated)	v2	• v2beta2 is removed, "action required" relnote
X+16	v2, v1 (deprecated)	v2	
X+17	v2	v2	• v1 is removed, "action required" relnote

REST resources (aka API objects)

Consider a hypothetical REST resource named Widget, which was present in API v1 in the above timeline, and which needs to be deprecated. We document and announce the deprecation in sync with release X+1. The Widget resource still exists in API version v1 (deprecated) but not in v2alpha1. The Widget resource continues to exist and function in releases up to and including X+8. Only in release X+9, when API v1 has aged out, does the Widget resource cease to exist, and the behavior get removed.

Fields of REST resources

As with whole REST resources, an individual field which was present in API v1 must exist and function until API v1 is removed. Unlike whole resources, the v2 APIs may choose a different representation for the field, as long as it can be round-tripped. For example a v1 field named "magnitude" which was deprecated might be named "deprecatedMagnitude" in API v2. When v1 is eventually removed, the deprecated field can be removed from v2.

Enumerated or constant values

As with whole REST resources and fields thereof, a constant value which was supported in API v1 must exist and function until API v1 is removed.

Component config structures

Component configs are versioned and managed just like REST resources.

Future work

Over time, Kubernetes will introduce more fine-grained API versions, at which point these rules will be adjusted as needed.

Deprecating a flag or CLI

The Kubernetes system is comprised of several different programs cooperating. Sometimes, a Kubernetes release might remove flags or CLI commands (collectively "CLI elements") in these programs. The individual programs naturally sort into two main groups - user-facing and admin-facing programs, which vary slightly in their deprecation policies. Unless a flag is explicitly prefixed or documented as "alpha" or "beta", it is considered GA.

CLI elements are effectively part of the API to the system, but since they are not versioned in the same way as the REST API, the rules for deprecation are as follows:

Rule #5a: CLI elements of user-facing components (e.g. kubectl) must function after their announced deprecation for no less than:

- **GA: 12 months or 2 releases (whichever is longer)**
- **Beta: 3 months or 1 release (whichever is longer)**
- **Alpha: 0 releases**

Rule #5b: CLI elements of admin-facing components (e.g. kubelet) must function after their announced deprecation for no less than:

- **GA: 6 months or 1 release (whichever is longer)**
- **Beta: 3 months or 1 release (whichever is longer)**
- **Alpha: 0 releases**

Rule #6: Deprecated CLI elements must emit warnings (optionally disable) when used.

Deprecating a feature or behavior

Occasionally a Kubernetes release needs to deprecate some feature or behavior of the system that is not controlled by the API or CLI. In this case, the rules for deprecation are as follows:

Rule #7: Deprecated behaviors must function for no less than 1 year after their announced deprecation.

This does not imply that all changes to the system are governed by this policy. This applies only to significant, user-visible behaviors which impact the correctness of applications running on Kubernetes or that impact the administration of Kubernetes clusters, and which are being removed entirely.

An exception to the above rule is *feature gates*. Feature gates are key=value pairs that allow for users to enable/disable experimental features.

Feature gates are intended to cover the development life cycle of a feature - they are not intended to be long-term APIs. As such, they are expected to be deprecated and removed after a feature becomes GA or is dropped.

As a feature moves through the stages, the associated feature gate evolves. The feature life cycle matched to its corresponding feature gate is:

- Alpha: the feature gate is disabled by default and can be enabled by the user.
- Beta: the feature gate is enabled by default and can be disabled by the user.
- GA: the feature gate is deprecated (see "Deprecation") and becomes non-operational.
- GA, deprecation window complete: the feature gate is removed and calls to it are no longer accepted.

Deprecation

Features can be removed at any point in the life cycle prior to GA. When features are removed prior to GA, their associated feature gates are also deprecated.

When an invocation tries to disable a non-operational feature gate, the call fails in order to avoid unsupported scenarios that might otherwise run silently.

In some cases, removing pre-GA features requires considerable time. Feature gates can remain operational until their associated feature is fully removed, at which point the feature gate itself can be deprecated.

When removing a feature gate for a GA feature also requires considerable time, calls to feature gates may remain operational if the feature gate has no effect on the feature, and if the feature gate causes no errors.

Features intended to be disabled by users should include a mechanism for disabling the feature in the associated feature gate.

Versioning for feature gates is different from the previously discussed components, therefore the rules for deprecation are as follows:

Rule #8: Feature gates must be deprecated when the corresponding feature they control transitions a lifecycle stage as follows. Feature gates must function for no less than:

- **Beta feature to GA: 6 months or 2 releases (whichever is longer)**
- **Beta feature to EOL: 3 months or 1 release (whichever is longer)**
- **Alpha feature to EOL: 0 releases**

Rule #9: Deprecated feature gates must respond with a warning when used. When a feature gate is deprecated it must be documented in both in the release notes and the corresponding CLI help. Both warnings and documentation must indicate whether a feature gate is non-operational.

Exceptions

No policy can cover every possible situation. This policy is a living document, and will evolve over time. In practice, there will be situations that do not fit neatly into this policy, or for which this policy becomes a serious impediment. Such situations should be discussed with SIGs and project leaders to find the best solutions for those specific cases, always bearing in mind that Kubernetes is committed to being a stable system that, as much as possible, never breaks users. Exceptions will always be announced in all relevant release notes.

Edit This Page

Kubernetes API Overview

This page provides an overview of the Kubernetes API.

- API versioning
- API groups
- Enabling API groups
- Enabling resources in the groups

The REST API is the fundamental fabric of Kubernetes. All operations and communications between components, and external user commands are REST API calls that the API Server handles. Consequently, everything in the Kubernetes platform is treated as an API object and has a corresponding entry in the API.

Most operations can be performed through the kubectl command-line interface or other command-line tools, such as kubeadm, which in turn use the API. However, you can also access the API directly using REST calls.

Consider using one of the client libraries if you are writing an application using the Kubernetes API.

API versioning

To eliminate fields or restructure resource representations, Kubernetes supports multiple API versions, each at a different API path. For example: `/api/v1` or `/apis/extensions/v1beta1`.

The version is set at the API level rather than at the resource or field level to:

- Ensure that the API presents a clear and consistent view of system resources and behavior.
- Enable control access to end-of-life and/or experimental APIs.

The JSON and Protobuf serialization schemas follow the same guidelines for schema changes. The following descriptions cover both formats.

> **Note:** The API versioning and software versioning are indirectly related. The API and release versioning proposal describes the relationship between API versioning and software versioning.

Different API versions indicate different levels of stability and support. You can find more information about the criteria for each level in the API Changes documentation.

Here's a summary of each level:

- Alpha:

  - The version names contain `alpha` (for example, `v1alpha1`).
  - The software may contain bugs. Enabling a feature may expose bugs. A feature may be disabled by default.
  - The support for a feature may be dropped at any time without notice.
  - The API may change in incompatible ways in a later software release without notice.
  - The software is recommended for use only in short-lived testing clusters, due to increased risk of bugs and lack of long-term support.

- Beta:

  - The version names contain `beta` (for example, `v2beta3`).
  - The software is well tested. Enabling a feature is considered safe. Features are enabled by default.
  - The support for a feature will not be dropped, though the details may change.
  - The schema and/or semantics of objects may change in incompatible ways in a subsequent beta or stable release. When this happens, migration instructions are provided. This may require deleting, editing, and re-creating API objects. The editing process may require some thought. This may require downtime for applications that rely on the feature.

– The software is recommended for only non-business-critical uses because of potential for incompatible changes in subsequent releases. If you have multiple clusters which can be upgraded independently, you may be able to relax this restriction.

Note: Try the beta features and provide feedback. After the features exit beta, it may not be practical to make more changes.

- Stable:
    – The version name is `vX` where `X` is an integer.
    – The stable versions of features appear in released software for many subsequent versions.

API groups

API groups make it easier to extend the Kubernetes API. The API group is specified in a REST path and in the `apiVersion` field of a serialized object.

Currently, there are several API groups in use:

- The *core* (also called *legacy*) group, which is at REST path `/api/v1` and is not specified as part of the `apiVersion` field, for example, `apiVersion: v1`.
- The named groups are at REST path `/apis/$GROUP_NAME/$VERSION`, and use `apiVersion: $GROUP_NAME/$VERSION` (for example, `apiVersion: batch/v1`). You can find the full list of supported API groups in Kubernetes API reference.

The two paths that support extending the API with custom resources are:

- CustomResourceDefinition for basic CRUD needs.
- aggregator for a full set of Kubernetes API semantics to implement their own apiserver.

Enabling API groups

Certain resources and API groups are enabled by default. You can enable or disable them by setting `--runtime-config` on the apiserver. `--runtime-config` accepts comma separated values. For example: - to disable batch/v1, set `--runtime-config=batch/v1=false` - to enable batch/v2alpha1, set `--runtime-config=batch/v2alpha1` The flag accepts comma separated set of key=value pairs describing runtime configuration of the apiserver.

Note: When you enable or disable groups or resources, you need to restart the apiserver and controller-manager to pick up the `--runtime-config` changes.

Enabling resources in the groups

DaemonSets, Deployments, HorizontalPodAutoscalers, Ingress, Jobs and ReplicaSets are enabled by default. You can enable other extensions resources by setting `--runtime-config` on apiserver. `--runtime-config` accepts comma separated values. For example, to disable deployments and jobs, set `--runtime-config=extensions/v1beta1/deployments=false,extensions/v1beta1/jobs=false`

Edit This Page

Kubernetes API Concepts

This page describes common concepts in the Kubernetes API.

- Standard API terminology
- Efficient detection of changes
- Retrieving large results sets in chunks
- Receiving resources as Tables
- Alternate representations of resources
- Dry run

The Kubernetes API is a resource-based (RESTful) programmatic interface provided via HTTP. It supports retrieving, creating, updating, and deleting primary resources via the standard HTTP verbs (POST, PUT, PATCH, DELETE, GET), includes additional subresources for many objects that allow fine grained authorization (such as binding a pod to a node), and can accept and serve those resources in different representations for convenience or efficiency. It also supports efficient change notifications on resources via "watches" and consistent lists to allow other components to effectively cache and synchronize the state of resources.

Standard API terminology

Most Kubernetes API resource types are "objects" - they represent a concrete instance of a concept on the cluster, like a pod or namespace. A smaller number of API resource types are "virtual" - they often represent operations rather than objects, such as a permission check (use a POST with a JSON-encoded body of `SubjectAccessReview` to the `subjectaccessreviews` resource). All objects will have a unique name to allow idempotent creation and retrieval, but virtual resource types may not have unique names if they are not retrievable or do not rely on idempotency.

Kubernetes generally leverages standard RESTful terminology to describe the API concepts:

- A **resource type** is the name used in the URL (`pods`, `namespaces`, `services`)
- All resource types have a concrete representation in JSON (their object schema) which is called a **kind**
- A list of instances of a resource type is known as a **collection**
- A single instance of the resource type is called a **resource**

All resource types are either scoped by the cluster (`/apis/GROUP/VERSION/*`) or to a namespace (`/apis/GROUP/VERSION/namespaces/NAMESPACE/*`). A namespace-scoped resource type will be deleted when its namespace is deleted and access to that resource type is controlled by authorization checks on the namespace scope. The following paths are used to retrieve collections and resources:

- Cluster-scoped resources:
    - `GET /apis/GROUP/VERSION/RESOURCETYPE` - return the collection of resources of the resource type
    - `GET /apis/GROUP/VERSION/RESOURCETYPE/NAME` - return the resource with NAME under the resource type
- Namespace-scoped resources:
    - `GET /apis/GROUP/VERSION/RESOURCETYPE` - return the collection of all instances of the resource type across all namespaces
    - `GET /apis/GROUP/VERSION/namespaces/NAMESPACE/RESOURCETYPE` - return collection of all instances of the resource type in NAMESPACE
    - `GET /apis/GROUP/VERSION/namespaces/NAMESPACE/RESOURCETYPE/NAME` - return the instance of the resource type with NAME in NAMESPACE

Since a namespace is a cluster-scoped resource type, you can retrieve the list of all namespaces with `GET /api/v1/namespaces` and details about a particular namespace with `GET /api/v1/namespaces/NAME`.

Almost all object resource types support the standard HTTP verbs - GET, POST, PUT, PATCH, and DELETE. Kubernetes uses the term **list** to describe returning a collection of resources to distinguish from retrieving a single resource which is usually called a **get**.

Some resource types will have one or more sub-resources, represented as sub paths below the resource:

- Cluster-scoped subresource: `GET /apis/GROUP/VERSION/RESOURCETYPE/NAME/SUBRESOURCE`
- Namespace-scoped subresource: `GET /apis/GROUP/VERSION/namespaces/NAMESPACE/RESOURCETYPE/NA`

The verbs supported for each subresource will differ depending on the object - see the API documentation more information. It is not possible to access sub-resources across multiple resources - generally a new virtual resource type would be used if that becomes necessary.

Efficient detection of changes

To enable clients to build a model of the current state of a cluster, all Kubernetes object resource types are required to support consistent lists and an incremental change notification feed called a **watch**. Every Kubernetes object has a `resourceVersion` field representing the version of that resource as stored in the underlying database. When retrieving a collection of resources (either namespace or cluster scoped), the response from the server will contain a `resourceVersion` value that can be used to initiate a watch against the server. The server will return all changes (creates, deletes, and updates) that occur after the supplied `resourceVersion`. This allows a client to fetch the current state and then watch for changes without missing any updates. If the client watch is disconnected they can restart a new watch from the last returned `resourceVersion`, or perform a new collection request and begin again.

For example:

1. List all of the pods in a given namespace.

   ```
   GET /api/v1/namespaces/test/pods
   ---
   200 OK
   Content-Type: application/json
   {
     "kind": "PodList",
     "apiVersion": "v1",
     "metadata": {"resourceVersion":"10245"},
     "items": [...]
   }
   ```

2. Starting from resource version 10245, receive notifications of any creates, deletes, or updates as individual JSON objects.

   ```
   GET /api/v1/namespaces/test/pods?watch=1&resourceVersion=10245
   ---
   200 OK
   Transfer-Encoding: chunked
   Content-Type: application/json
   {
     "type": "ADDED",
     "object": {"kind": "Pod", "apiVersion": "v1", "metadata": {"resourceVersion": "10596"
   }
   {
     "type": "MODIFIED",
     "object": {"kind": "Pod", "apiVersion": "v1", "metadata": {"resourceVersion": "11020"
   }
   ...
   ```

A given Kubernetes server will only preserve a historical list of changes for a limited time. Older clusters using etcd2 preserve a maximum of 1000 changes. Newer clusters using etcd3 preserve changes in the last 5 minutes by default. When the requested watch operations fail because the historical version of that resource is not available, clients must handle the case by recognizing the status code `410 Gone`, clearing their local cache, performing a list operation, and starting the watch from the `resourceVersion` returned by that new list operation. Most client libraries offer some form of standard tool for this logic. (In Go this is called a `Reflector` and is located in the `k8s.io/client-go/cache` package.)

Retrieving large results sets in chunks

On large clusters, retrieving the collection of some resource types may result in very large responses that can impact the server and client. For instance, a cluster may have tens of thousands of pods, each of which is 1-2kb of encoded JSON. Retrieving all pods across all namespaces may result in a very large response (10-20MB) and consume a large amount of server resources. Starting in Kubernetes 1.9 the server supports the ability to break a single large collection request into many smaller chunks while preserving the consistency of the total request. Each chunk can be returned sequentially which reduces both the total size of the request and allows user-oriented clients to display results incrementally to improve responsiveness.

To retrieve a single list in chunks, two new parameters `limit` and `continue` are supported on collection requests and a new field `continue` is returned from all list operations in the list `metadata` field. A client should specify the maximum results they wish to receive in each chunk with `limit` and the server will return up to `limit` resources in the result and include a `continue` value if there are more resources in the collection. The client can then pass this `continue` value to the server on the next request to instruct the server to return the next chunk of results. By continuing until the server returns an empty `continue` value the client can consume the full set of results.

Like a watch operation, a `continue` token will expire after a short amount of time (by default 5 minutes) and return a `410 Gone` if more results cannot be returned. In this case, the client will need to start from the beginning or omit the `limit` parameter.

For example, if there are 1,253 pods on the cluster and the client wants to receive chunks of 500 pods at a time, they would request those chunks as follows:

1. List all of the pods on a cluster, retrieving up to 500 pods each time.

   ```
   GET /api/v1/pods?limit=500
   ---
   200 OK
   Content-Type: application/json
   ```

```
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion":"10245",
    "continue": "ENCODED_CONTINUE_TOKEN",
    ...
  },
  "items": [...] // returns pods 1-500
}
```

2. Continue the previous call, retrieving the next set of 500 pods.

```
GET /api/v1/pods?limit=500&continue=ENCODED_CONTINUE_TOKEN
---
200 OK
Content-Type: application/json
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion":"10245",
    "continue": "ENCODED_CONTINUE_TOKEN_2",
    ...
  },
  "items": [...] // returns pods 501-1000
}
```

3. Continue the previous call, retrieving the last 253 pods.

```
GET /api/v1/pods?limit=500&continue=ENCODED_CONTINUE_TOKEN_2
---
200 OK
Content-Type: application/json
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {
    "resourceVersion":"10245",
    "continue": "", // continue token is empty because we have reached the end of the l
    ...
  },
  "items": [...] // returns pods 1001-1253
}
```

Note that the `resourceVersion` of the list remains constant across each request, indicating the server is showing us a consistent snapshot of the pods. Pods that are created, updated, or deleted after version 10245 would not be shown unless

the user makes a list request without the `continue` token. This allows clients to break large requests into smaller chunks and then perform a watch operation on the full set without missing any updates.

Receiving resources as Tables

`kubectl get` is a simple tabular representation of one or more instances of a particular resource type. In the past, clients were required to reproduce the tabular and describe output implemented in `kubectl` to perform simple lists of objects. A few limitations of that approach include non-trivial logic when dealing with certain objects. Additionally, types provided by API aggregation or third party resources are not known at compile time. This means that generic implementations had to be in place for types unrecognized by a client.

In order to avoid potential limitations as described above, clients may request the Table representation of objects, delegating specific details of printing to the server. The Kubernetes API implements standard HTTP content type negotiation: passing an `Accept` header containing a value of `application/json;as=Table;g=meta.k8s.io;v=v1beta1` with a `GET` call will request that the server return objects in the Table content type.

For example:

1. List all of the pods on a cluster in the Table format.

   ```
   GET /api/v1/pods
   Accept: application/json;as=Table;g=meta.k8s.io;v=v1beta1
   ---
   200 OK
   Content-Type: application/json
   {
       "kind": "Table",
       "apiVersion": "meta.k8s.io/v1beta1",
       ...
       "columnDefinitions": [
           ...
       ]
   }
   ```

For API resource types that do not have a custom Table definition on the server, a default Table response is returned by the server, consisting of the resource's `name` and `creationTimestamp` fields.

```
GET /apis/crd.example.com/v1alpha1/namespaces/default/resources
---
200 OK
Content-Type: application/json
...
```

```
{
    "kind": "Table",
    "apiVersion": "meta.k8s.io/v1beta1",
    ...
    "columnDefinitions": [
        {
            "name": "Name",
            "type": "string",
            ...
        },
        {
            "name": "Created At",
            "type": "date",
            ...
        }
    ]
}
```

Table responses are available beginning in version 1.10 of the kube-apiserver. As such, not all API resource types will support a Table response, specifically when using a client against older clusters. Clients that must work against all resource types, or can potentially deal with older clusters, should specify multiple content types in their `Accept` header to support fallback to non-Tabular JSON:

```
Accept: application/json;as=Table;g=meta.k8s.io;v=v1beta1, application/json
```

Alternate representations of resources

By default Kubernetes returns objects serialized to JSON with content type `application/json`. This is the default serialization format for the API. However, clients may request the more efficient Protobuf representation of these objects for better performance at scale. The Kubernetes API implements standard HTTP content type negotiation: passing an `Accept` header with a `GET` call will request that the server return objects in the provided content type, while sending an object in Protobuf to the server for a `PUT` or `POST` call takes the `Content-Type` header. The server will return a `Content-Type` header if the requested format is supported, or the `406 Not acceptable` error if an invalid content type is provided.

See the API documentation for a list of supported content types for each API.

For example:

1. List all of the pods on a cluster in Protobuf format.

   ```
   GET /api/v1/pods
   Accept: application/vnd.kubernetes.protobuf
   ---
   ```

```
200 OK
Content-Type: application/vnd.kubernetes.protobuf
... binary encoded PodList object
```

2. Create a pod by sending Protobuf encoded data to the server, but request a response in JSON.

```
POST /api/v1/namespaces/test/pods
Content-Type: application/vnd.kubernetes.protobuf
Accept: application/json
... binary encoded Pod object
---
200 OK
Content-Type: application/json
{
  "kind": "Pod",
  "apiVersion": "v1",
  ...
}
```

Not all API resource types will support Protobuf, specifically those defined via Custom Resource Definitions or those that are API extensions. Clients that must work against all resource types should specify multiple content types in their `Accept` header to support fallback to JSON:

```
Accept: application/vnd.kubernetes.protobuf, application/json
```

Protobuf encoding

Kubernetes uses an envelope wrapper to encode Protobuf responses. That wrapper starts with a 4 byte magic number to help identify content in disk or in etcd as Protobuf (as opposed to JSON), and then is followed by a Protobuf encoded wrapper message, which describes the encoding and type of the underlying object and then contains the object.

The wrapper format is:

```
A four byte magic number prefix:
  Bytes 0-3: "k8s\x00" [0x6b, 0x38, 0x73, 0x00]

An encoded Protobuf message with the following IDL:
  message Unknown {
    // typeMeta should have the string values for "kind" and "apiVersion" as set on the JSON
    optional TypeMeta typeMeta = 1;

    // raw will hold the complete serialized object in protobuf. See the protobuf definition
    optional bytes raw = 2;
```

```
  // contentEncoding is encoding used for the raw data. Unspecified means no encoding.
  optional string contentEncoding = 3;

  // contentType is the serialization method used to serialize 'raw'. Unspecified means ap
  // omitted.
  optional string contentType = 4;
}

message TypeMeta {
  // apiVersion is the group/version for this type
  optional string apiVersion = 1;
  // kind is the name of the object schema. A protobuf definition should exist for this ob
  optional string kind = 2;
}
```

Clients that receive a response in `application/vnd.kubernetes.protobuf`
that does not match the expected prefix should reject the response, as future
versions may need to alter the serialization format in an incompatible way and
will do so by changing the prefix.

Dry run

FEATURE STATE: `Kubernetes v1.12` alpha

This feature is currently in a *alpha* state, meaning:

- The version names contain alpha (e.g. v1alpha1).
- Might be buggy. Enabling the feature may expose bugs. Disabled by
  default.
- Support for feature may be dropped at any time without notice.
- The API may change in incompatible ways in a later software release
  without notice.
- Recommended for use only in short-lived testing clusters, due to increased
  risk of bugs and lack of long-term support.

In version 1.12, if the dry run alpha feature is enabled, the modifying verbs
(`POST`, `PUT`, `PATCH`, and `DELETE`) can accept requests in a dry run mode. Dry run
mode helps to evaluate a request through the typical request stages (admission
chain, validation, merge conflicts) up until persisting objects to storage. The
response body for the request is as close as possible to a non dry run response.
The system guarantees that dry run requests will not be persisted in storage or
have any other side effects.

Enable the dry run alpha feature

Dry run is an alpha feature, so it is disabled by default. To turn it on, you need to:

- Include "DryRun=true" in the `--feature-gates` flag when starting `kube-apiserver`. If you have multiple `kube-apiserver` replicas, all should have the same flag setting.

If this feature is not enabled, all requests with a modifying verb (`POST`, `PUT`, `PATCH`, and `DELETE`) which set the `dryRun` query parameter will be rejected with a 400 Bad Request error. Kubernetes 1.11 always rejects dry run requests like this, so it is safe for clients to make dry run requests even if the feature is not enabled on the server, as long as the server version is >= 1.11.

Make a dry run request

Dry run is triggered by setting the `dryRun` query parameter. This parameter is a string, working as an enum, and in 1.12 the only accepted values are:

- `All`: Every stage runs as normal, except for the final storage stage. Admission controllers are run to check that the request is valid, mutating controllers mutate the request, merge is performed on `PATCH`, fields are defaulted, and schema validation occurs. The changes are not persisted to the underlying storage, but the final object which would have been persisted is still returned to the user, along with the normal status code. If the request would trigger an admission controller which would have side effects, the request will be failed rather than risk an unwanted side effect. Admission webhooks can now declare (in their configuration object) that they do not have side effects to prevent this. All built in admission control plugins support dry run.
- Leave the value empty, which is also the default: Keep the default modifying behavior.

For example:

```
POST /api/v1/namespaces/test/pods?dryRun=All
Content-Type: application/json
Accept: application/json
```

The response would look the same as for non dry run request, but the values of some generated fields may differ.

Generated values

Some values of an object are typically generated before the object is persisted. It is important not to rely upon the values of these fields set by a dry run request,

since these values will likely be different in dry run mode from when the real
request is made. Some of these fields are:

- `name`: if `generateName` is set, `name` will have a unique random name
- `creationTimestamp`/`deletionTimestamp`: records the time of cre-
  ation/deletion
- `UID`: uniquely identifies the object and is randomly generated (non-
  deterministic)
- `resourceVersion`: tracks the persisted version of the object
- Any field set by a mutating admission controller
- For the `Service` resource: Ports or IPs that kube-apiserver assigns to
  v1.Service objects

Edit This Page

Client Libraries

This page contains an overview of the client libraries for using the Kubernetes
API from various programming languages.

- Officially-supported Kubernetes client libraries
- Community-maintained client libraries

To write applications using the Kubernetes REST API, you do not need to
implement the API calls and request/response types yourself. You can use a
client library for the programming language you are using.

Client libraries often handle common tasks such as authentication for you. Most
client libraries can discover and use the Kubernetes Service Account to authenti-
cate if the API client is running inside the Kubernetes cluster, or can understand
the kubeconfig file format to read the credentials and the API Server address.

Officially-supported Kubernetes client libraries

The following client libraries are officially maintained by Kubernetes SIG API
Machinery.

Language	Client Library	Sample Programs
Go	github.com/kubernetes/client-go/	browse
Python	github.com/kubernetes-client/python/	browse
Java	github.com/kubernetes-client/java	browse
dotnet	github.com/kubernetes-client/csharp	browse
JavaScript	github.com/kubernetes-client/javascript	browse

Community-maintained client libraries

The following Kubernetes API client libraries are provided and maintained by their authors, not the Kubernetes team.

Language	Client Library
Clojure	github.com/yanatan16/clj-kubernetes-api
Go	github.com/ericchiang/k8s
Java (OSGi)	bitbucket.org/amdatulabs/amdatu-kubernetes
Java (Fabric8, OSGi)	github.com/fabric8io/kubernetes-client
Lisp	github.com/brendandburns/cl-k8s
Lisp	github.com/xh4/cube
Node.js (TypeScript)	github.com/Goyoo/node-k8s-client
Node.js	github.com/tenxcloud/node-kubernetes-client
Node.js	github.com/godaddy/kubernetes-client
Perl	metacpan.org/pod/Net::Kubernetes
PHP	github.com/devstub/kubernetes-api-php-client
PHP	github.com/maclof/kubernetes-client
Python	github.com/eldarion-gondor/pykube
Python	github.com/mnubo/kubernetes-py
Ruby	github.com/Ch00k/kuber
Ruby	github.com/abonas/kubeclient
Ruby	github.com/kontena/k8s-client
Scala	github.com/doriordan/skuber
dotNet	github.com/tonnyeremin/kubernetes_gen
DotNet (RestSharp)	github.com/masroorhasan/Kubernetes.DotNet
Elixir	github.com/obmarg/kazan
Haskell	github.com/soundcloud/haskell-kubernetes

Edit This Page

Kubernetes Deprecation Policy

This document details the deprecation policy for various facets of the system.

- Deprecating parts of the API
- Deprecating a flag or CLI
- Deprecating a feature or behavior
- Exceptions

Kubernetes is a large system with many components and many contributors. As with any such software, the feature set naturally evolves over time, and sometimes a feature may need to be removed. This could include an API, a flag,

or even an entire feature. To avoid breaking existing users, Kubernetes follows a deprecation policy for aspects of the system that are slated to be removed.

Deprecating parts of the API

Since Kubernetes is an API-driven system, the API has evolved over time to reflect the evolving understanding of the problem space. The Kubernetes API is actually a set of APIs, called "API groups", and each API group is independently versioned. API versions fall into 3 main tracks, each of which has different policies for deprecation:

Example	Track
v1	GA (generally available, stable)
v1beta1	Beta (pre-release)
v1alpha1	Alpha (experimental)

A given release of Kubernetes can support any number of API groups and any number of versions of each.

The following rules govern the deprecation of elements of the API. This includes:

- REST resources (aka API objects)
- Fields of REST resources
- Annotations on REST resources, including "beta" annotations but not including "alpha" annotations.
- Enumerated or constant values
- Component config structures

These rules are enforced between official releases, not between arbitrary commits to master or release branches.

Rule #1: API elements may only be removed by incrementing the version of the API group.

Once an API element has been added to an API group at a particular version, it can not be removed from that version or have its behavior significantly changed, regardless of track.

> **Note:** For historical reasons, there are 2 "monolithic" API groups - "core" (no group name) and "extensions". Resources will incrementally be moved from these legacy API groups into more domain-specific API groups.

Rule #2: API objects must be able to round-trip between API versions in a given release without information loss, with the exception of whole REST resources that do not exist in some versions.

For example, an object can be written as v1 and then read back as v2 and converted to v1, and the resulting v1 resource will be identical to the original. The representation in v2 might be different from v1, but the system knows how to convert between them in both directions. Additionally, any new field added in v2 must be able to round-trip to v1 and back, which means v1 might have to add an equivalent field or represent it as an annotation.

Rule #3: An API version in a given track may not be deprecated until a new API version at least as stable is released.

GA API versions can replace GA API versions as well as beta and alpha API versions. Beta API versions *may not* replace GA API versions.

Rule #4a: Other than the most recent API versions in each track, older API versions must be supported after their announced deprecation for a duration of no less than:

- **GA: 12 months or 3 releases (whichever is longer)**
- **Beta: 9 months or 3 releases (whichever is longer)**
- **Alpha: 0 releases**

This covers the maximum supported version skew of 2 releases.

> **Note:** Until #52185 is resolved, no API versions that have been persisted to storage may be removed. Serving REST endpoints for those versions may be disabled (subject to the deprecation timelines in this document), but the API server must remain capable of decoding/converting previously persisted data from storage.

Rule #4b: The "preferred" API version and the "storage version" for a given group may not advance until after a release has been made that supports both the new version and the previous version

Users must be able to upgrade to a new release of Kubernetes and then roll back to a previous release, without converting anything to the new API version or suffering breakages (unless they explicitly used features only available in the newer version). This is particularly evident in the stored representation of objects.

All of this is best illustrated by examples. Imagine a Kubernetes release, version X, which introduces a new API group. A new Kubernetes release is made every approximately 3 months (4 per year). The following table describes which API versions are supported in a series of subsequent releases.

Release	API Versions	Preferred/Storage Version	Notes
X	v1alpha1	v1alpha1	

Release	API Versions	Preferred/Storage Version	Notes
X+1	v1alpha2	v1alpha2	• v1alpha1 is removed, "action required" relnote
X+2	v1beta1	v1beta1	• v1alpha2 is removed, "action required" relnote
X+3	v1beta2, v1beta1 (deprecated)	v1beta1	• v1beta1 is deprecated, "action required" relnote
X+4	v1beta2, v1beta1 (deprecated)	v1beta2	
X+5	v1, v1beta1 (deprecated), v1beta2 (deprecated)	v1beta2	• v1beta2 is deprecated, "action required" relnote
X+6	v1, v1beta2 (deprecated)	v1	• v1beta1 is removed, "action required" relnote
X+7	v1, v1beta2 (deprecated)	v1	
X+8	v2alpha1, v1	v1	• v1beta2 is removed, "action required" relnote

Release	API Versions	Preferred/Storage Version	Notes
X+9	v2alpha2, v1	v1	• v2alpha1 is removed, "action required" relnote
X+10	v2beta1, v1	v1	• v2alpha2 is removed, "action required" relnote
X+11	v2beta2, v2beta1 (deprecated), v1	v1	• v2beta1 is deprecated, "action required" relnote
X+12	v2, v2beta2 (deprecated), v2beta1 (deprecated), v1 (deprecated)	v1	• v2beta2 is deprecated, "action required" relnote • v1 is deprecated, "action required" relnote
X+13	v2, v2beta1 (deprecated), v2beta2 (deprecated), v1 (deprecated)	v2	
X+14	v2, v2beta2 (deprecated), v1 (deprecated)	v2	• v2beta1 is removed, "action required" relnote

Release	API Versions	Preferred/Storage Version	Notes
X+15	v2, v1 (deprecated)	v2	• v2beta2 is removed, "action required" relnote
X+16	v2, v1 (deprecated)	v2	
X+17	v2	v2	• v1 is removed, "action required" relnote

REST resources (aka API objects)

Consider a hypothetical REST resource named Widget, which was present in API v1 in the above timeline, and which needs to be deprecated. We document and announce the deprecation in sync with release X+1. The Widget resource still exists in API version v1 (deprecated) but not in v2alpha1. The Widget resource continues to exist and function in releases up to and including X+8. Only in release X+9, when API v1 has aged out, does the Widget resource cease to exist, and the behavior get removed.

Fields of REST resources

As with whole REST resources, an individual field which was present in API v1 must exist and function until API v1 is removed. Unlike whole resources, the v2 APIs may choose a different representation for the field, as long as it can be round-tripped. For example a v1 field named "magnitude" which was deprecated might be named "deprecatedMagnitude" in API v2. When v1 is eventually removed, the deprecated field can be removed from v2.

Enumerated or constant values

As with whole REST resources and fields thereof, a constant value which was supported in API v1 must exist and function until API v1 is removed.

Component config structures

Component configs are versioned and managed just like REST resources.

Future work

Over time, Kubernetes will introduce more fine-grained API versions, at which point these rules will be adjusted as needed.

Deprecating a flag or CLI

The Kubernetes system is comprised of several different programs cooperating. Sometimes, a Kubernetes release might remove flags or CLI commands (collectively "CLI elements") in these programs. The individual programs naturally sort into two main groups - user-facing and admin-facing programs, which vary slightly in their deprecation policies. Unless a flag is explicitly prefixed or documented as "alpha" or "beta", it is considered GA.

CLI elements are effectively part of the API to the system, but since they are not versioned in the same way as the REST API, the rules for deprecation are as follows:

Rule #5a: CLI elements of user-facing components (e.g. kubectl) must function after their announced deprecation for no less than:

- **GA: 12 months or 2 releases (whichever is longer)**
- **Beta: 3 months or 1 release (whichever is longer)**
- **Alpha: 0 releases**

Rule #5b: CLI elements of admin-facing components (e.g. kubelet) must function after their announced deprecation for no less than:

- **GA: 6 months or 1 release (whichever is longer)**
- **Beta: 3 months or 1 release (whichever is longer)**
- **Alpha: 0 releases**

Rule #6: Deprecated CLI elements must emit warnings (optionally disable) when used.

Deprecating a feature or behavior

Occasionally a Kubernetes release needs to deprecate some feature or behavior of the system that is not controlled by the API or CLI. In this case, the rules for deprecation are as follows:

Rule #7: Deprecated behaviors must function for no less than 1 year after their announced deprecation.

This does not imply that all changes to the system are governed by this policy. This applies only to significant, user-visible behaviors which impact the correctness of applications running on Kubernetes or that impact the administration of Kubernetes clusters, and which are being removed entirely.

An exception to the above rule is *feature gates*. Feature gates are key=value pairs that allow for users to enable/disable experimental features.

Feature gates are intended to cover the development life cycle of a feature - they are not intended to be long-term APIs. As such, they are expected to be deprecated and removed after a feature becomes GA or is dropped.

As a feature moves through the stages, the associated feature gate evolves. The feature life cycle matched to its corresponding feature gate is:

- Alpha: the feature gate is disabled by default and can be enabled by the user.
- Beta: the feature gate is enabled by default and can be disabled by the user.
- GA: the feature gate is deprecated (see "Deprecation") and becomes non-operational.
- GA, deprecation window complete: the feature gate is removed and calls to it are no longer accepted.

Deprecation

Features can be removed at any point in the life cycle prior to GA. When features are removed prior to GA, their associated feature gates are also deprecated.

When an invocation tries to disable a non-operational feature gate, the call fails in order to avoid unsupported scenarios that might otherwise run silently.

In some cases, removing pre-GA features requires considerable time. Feature gates can remain operational until their associated feature is fully removed, at which point the feature gate itself can be deprecated.

When removing a feature gate for a GA feature also requires considerable time, calls to feature gates may remain operational if the feature gate has no effect on the feature, and if the feature gate causes no errors.

Features intended to be disabled by users should include a mechanism for disabling the feature in the associated feature gate.

Versioning for feature gates is different from the previously discussed components, therefore the rules for deprecation are as follows:

Rule #8: Feature gates must be deprecated when the corresponding feature they control transitions a lifecycle stage as follows. Feature gates must function for no less than:

- **Beta feature to GA: 6 months or 2 releases (whichever is longer)**
- **Beta feature to EOL: 3 months or 1 release (whichever is longer)**
- **Alpha feature to EOL: 0 releases**

Rule #9: Deprecated feature gates must respond with a warning when used. When a feature gate is deprecated it must be documented in both in the release notes and the corresponding CLI help. Both warnings and documentation must indicate whether a feature gate is non-operational.

Exceptions

No policy can cover every possible situation. This policy is a living document, and will evolve over time. In practice, there will be situations that do not fit neatly into this policy, or for which this policy becomes a serious impediment. Such situations should be discussed with SIGs and project leaders to find the best solutions for those specific cases, always bearing in mind that Kubernetes is committed to being a stable system that, as much as possible, never breaks users. Exceptions will always be announced in all relevant release notes.

Edit This Page

Using RBAC Authorization

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.

- API Overview
- Default Roles and Role Bindings
- Privilege Escalation Prevention and Bootstrapping
- Command-line Utilities
- Service Account Permissions
- Upgrading from 1.5
- Permissive RBAC Permissions

`RBAC` uses the `rbac.authorization.k8s.io` API group to drive authorization decisions, allowing admins to dynamically configure policies through the Kubernetes API.

As of 1.8, RBAC mode is stable and backed by the rbac.authorization.k8s.io/v1 API.

To enable RBAC, start the apiserver with `--authorization-mode=RBAC`.

API Overview

The RBAC API declares four top-level types which will be covered in this section. Users can interact with these resources as they would with any other API resource (via `kubectl`, API calls, etc.). For instance, `kubectl create -f (resource).yml` can be used with any of these examples, though readers who wish to follow along should review the section on bootstrapping first.

Role and ClusterRole

In the RBAC API, a role contains rules that represent a set of permissions. Permissions are purely additive (there are no "deny" rules). A role can be defined within a namespace with a `Role`, or cluster-wide with a `ClusterRole`.

A `Role` can only be used to grant access to resources within a single namespace. Here's an example `Role` in the "default" namespace that can be used to grant read access to pods:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups: [""] # "" indicates the core API group
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```

A `ClusterRole` can be used to grant the same permissions as a `Role`, but because they are cluster-scoped, they can also be used to grant access to:

- cluster-scoped resources (like nodes)
- non-resource endpoints (like "/healthz")
- namespaced resources (like pods) across all namespaces (needed to run `kubectl get pods --all-namespaces`, for example)

The following `ClusterRole` can be used to grant read access to secrets in any particular namespace, or across all namespaces (depending on how it is bound):

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  # "namespace" omitted since ClusterRoles are not namespaced
  name: secret-reader
rules:
- apiGroups: [""]
  resources: ["secrets"]
  verbs: ["get", "watch", "list"]
```

RoleBinding and ClusterRoleBinding

A role binding grants the permissions defined in a role to a user or set of users.
It holds a list of subjects (users, groups, or service accounts), and a reference to
the role being granted. Permissions can be granted within a namespace with a
`RoleBinding`, or cluster-wide with a `ClusterRoleBinding`.

A `RoleBinding` may reference a `Role` in the same namespace. The following
`RoleBinding` grants the "pod-reader" role to the user "jane" within the "default"
namespace. This allows "jane" to read pods in the "default" namespace.

`roleRef` is how you will actually create the binding. The `kind` will be either
`Role` or `ClusterRole`, and the `name` will reference the name of the specific `Role`
or `ClusterRole` you want. In the example below, this RoleBinding is using
`roleRef` to bind the user "jane" to the `Role` created above named `pod-reader`.

```
# This role binding allows "jane" to read pods in the "default" namespace.
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-pods
  namespace: default
subjects:
- kind: User
  name: jane # Name is case sensitive
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role #this must be Role or ClusterRole
  name: pod-reader # this must match the name of the Role or ClusterRole you wish to bind to
  apiGroup: rbac.authorization.k8s.io
```

A `RoleBinding` may also reference a `ClusterRole` to grant the permissions to
namespaced resources defined in the `ClusterRole` within the `RoleBinding`'s
namespace. This allows administrators to define a set of common roles for the
entire cluster, then reuse them within multiple namespaces.

For instance, even though the following `RoleBinding` refers to a `ClusterRole`,
"dave" (the subject, case sensitive) will only be able to read secrets in the "de-
velopment" namespace (the namespace of the `RoleBinding`).

```
# This role binding allows "dave" to read secrets in the "development" namespace.
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-secrets
  namespace: development # This only grants permissions within the "development" namespace.
subjects:
- kind: User
```

```
  name: dave # Name is case sensitive
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: secret-reader
  apiGroup: rbac.authorization.k8s.io
```

Finally, a `ClusterRoleBinding` may be used to grant permission at the cluster
level and in all namespaces. The following `ClusterRoleBinding` allows any user
in the group "manager" to read secrets in any namespace.

```
# This cluster role binding allows anyone in the "manager" group to read secrets in any name
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-secrets-global
subjects:
- kind: Group
  name: manager # Name is case sensitive
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: secret-reader
  apiGroup: rbac.authorization.k8s.io
```

Referring to Resources

Most resources are represented by a string representation of their name, such as
"pods", just as it appears in the URL for the relevant API endpoint. However,
some Kubernetes APIs involve a "subresource", such as the logs for a pod. The
URL for the pods logs endpoint is:

```
GET /api/v1/namespaces/{namespace}/pods/{name}/log
```

In this case, "pods" is the namespaced resource, and "log" is a subresource of
pods. To represent this in an RBAC role, use a slash to delimit the resource
and subresource. To allow a subject to read both pods and pod logs, you would
write:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: pod-and-pod-logs-reader
rules:
- apiGroups: [""]
  resources: ["pods", "pods/log"]
```

```
    verbs: ["get", "list"]
```

Resources can also be referred to by name for certain requests through the
`resourceNames` list. When specified, requests using the "get", "delete", "up-
date", and "patch" verbs can be restricted to individual instances of a resource.
To restrict a subject to only "get" and "update" a single configmap, you would
write:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: configmap-updater
rules:
- apiGroups: [""]
  resources: ["configmaps"]
  resourceNames: ["my-configmap"]
  verbs: ["update", "get"]
```

Notably, if `resourceNames` are set, then the verb must not be list, watch, create,
or deletecollection. Because resource names are not present in the URL for
create, list, watch, and deletecollection API requests, those verbs would not be
allowed by a rule with `resourceNames` set, since the `resourceNames` portion of
the rule would not match the request.

Aggregated ClusterRoles

As of 1.9, ClusterRoles can be created by combining other ClusterRoles using an
`aggregationRule`. The permissions of aggregated ClusterRoles are controller-
managed, and filled in by unioning the rules of any ClusterRole that matches
the provided label selector. An example aggregated ClusterRole:

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: monitoring
aggregationRule:
  clusterRoleSelectors:
  - matchLabels:
      rbac.example.com/aggregate-to-monitoring: "true"
rules: [] # Rules are automatically filled in by the controller manager.
```

Creating a ClusterRole that matches the label selector will add rules to
the aggregated ClusterRole. In this case rules can be added to the "mon-
itoring" ClusterRole by creating another ClusterRole that has the label
`rbac.example.com/aggregate-to-monitoring: true`.

```
kind: ClusterRole
```

```
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: monitoring-endpoints
  labels:
    rbac.example.com/aggregate-to-monitoring: "true"
# These rules will be added to the "monitoring" role.
rules:
- apiGroups: [""]
  resources: ["services", "endpoints", "pods"]
  verbs: ["get", "list", "watch"]
```

The default user-facing roles (described below) use ClusterRole aggregation. This lets admins include rules for custom resources, such as those served by CustomResourceDefinitions or Aggregated API servers, on the default roles.

For example, the following ClusterRoles let the "admin" and "edit" default roles manage the custom resource "CronTabs" and the "view" role perform read-only actions on the resource.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: aggregate-cron-tabs-edit
  labels:
    # Add these permissions to the "admin" and "edit" default roles.
    rbac.authorization.k8s.io/aggregate-to-admin: "true"
    rbac.authorization.k8s.io/aggregate-to-edit: "true"
rules:
- apiGroups: ["stable.example.com"]
  resources: ["crontabs"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
---
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: aggregate-cron-tabs-view
  labels:
    # Add these permissions to the "view" default role.
    rbac.authorization.k8s.io/aggregate-to-view: "true"
rules:
- apiGroups: ["stable.example.com"]
  resources: ["crontabs"]
  verbs: ["get", "list", "watch"]
```

Role Examples

Only the `rules` section is shown in the following examples.

Allow reading the resource "pods" in the core API group:

```
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
```

Allow reading/writing "deployments" in both the "extensions" and "apps" API groups:

```
rules:
- apiGroups: ["extensions", "apps"]
  resources: ["deployments"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
```

Allow reading "pods" and reading/writing "jobs":

```
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["batch", "extensions"]
  resources: ["jobs"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
```

Allow reading a `ConfigMap` named "my-config" (must be bound with a `RoleBinding` to limit to a single `ConfigMap` in a single namespace):

```
rules:
- apiGroups: [""]
  resources: ["configmaps"]
  resourceNames: ["my-config"]
  verbs: ["get"]
```

Allow reading the resource "nodes" in the core group (because a `Node` is cluster-scoped, this must be in a `ClusterRole` bound with a `ClusterRoleBinding` to be effective):

```
rules:
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["get", "list", "watch"]
```

Allow "GET" and "POST" requests to the non-resource endpoint "/healthz" and all subpaths (must be in a `ClusterRole` bound with a `ClusterRoleBinding` to be effective):

```
rules:
- nonResourceURLs: ["/healthz", "/healthz/*"] # '*' in a nonResourceURL is a suffix glob mat
  verbs: ["get", "post"]
```

Referring to Subjects

A `RoleBinding` or `ClusterRoleBinding` binds a role to *subjects*. Subjects can be groups, users or service accounts.

Users are represented by strings. These can be plain usernames, like "alice", email-style names, like "bob@example.com", or numeric IDs represented as a string. It is up to the Kubernetes admin to configure the authentication modules to produce usernames in the desired format. The RBAC authorization system does not require any particular format. However, the prefix `system:` is reserved for Kubernetes system use, and so the admin should ensure usernames do not contain this prefix by accident.

Group information in Kubernetes is currently provided by the Authenticator modules. Groups, like users, are represented as strings, and that string has no format requirements, other than that the prefix `system:` is reserved.

Service Accounts have usernames with the `system:serviceaccount:` prefix and belong to groups with the `system:serviceaccounts:` prefix.

Role Binding Examples

Only the `subjects` section of a `RoleBinding` is shown in the following examples.

For a user named "alice@example.com":

```
subjects:
- kind: User
  name: "alice@example.com"
  apiGroup: rbac.authorization.k8s.io
```

For a group named "frontend-admins":

```
subjects:
- kind: Group
  name: "frontend-admins"
  apiGroup: rbac.authorization.k8s.io
```

For the default service account in the kube-system namespace:

```
subjects:
- kind: ServiceAccount
  name: default
  namespace: kube-system
```

For all service accounts in the "qa" namespace:

```
subjects:
- kind: Group
  name: system:serviceaccounts:qa
  apiGroup: rbac.authorization.k8s.io
```

For all service accounts everywhere:

```
subjects:
- kind: Group
  name: system:serviceaccounts
  apiGroup: rbac.authorization.k8s.io
```

For all authenticated users (version 1.5+):

```
subjects:
- kind: Group
  name: system:authenticated
  apiGroup: rbac.authorization.k8s.io
```

For all unauthenticated users (version 1.5+):

```
subjects:
- kind: Group
  name: system:unauthenticated
  apiGroup: rbac.authorization.k8s.io
```

For all users (version 1.5+):

```
subjects:
- kind: Group
  name: system:authenticated
  apiGroup: rbac.authorization.k8s.io
- kind: Group
  name: system:unauthenticated
  apiGroup: rbac.authorization.k8s.io
```

Default Roles and Role Bindings

API servers create a set of default `ClusterRole` and `ClusterRoleBinding` objects. Many of these are `system:` prefixed, which indicates that the resource is "owned" by the infrastructure. Modifications to these resources can result in non-functional clusters. One example is the `system:node` ClusterRole. This role defines permissions for kubelets. If the role is modified, it can prevent kubelets from working.

All of the default cluster roles and rolebindings are labeled with `kubernetes.io/bootstrapping=rbac-default`

Auto-reconciliation

At each start-up, the API server updates default cluster roles with any missing permissions, and updates default cluster role bindings with any missing subjects. This allows the cluster to repair accidental modifications, and to keep roles and rolebindings up-to-date as permissions and subjects change in new releases.

To opt out of this reconciliation, set the `rbac.authorization.kubernetes.io/autoupdate`
annotation on a default cluster role or rolebinding to `false`. Be aware that
missing default permissions and subjects can result in non-functional clusters.

Auto-reconciliation is enabled in Kubernetes version 1.6+ when the RBAC au-
thorizer is active.

Discovery Roles

Default role bindings authorize unauthenticated and authenticated users to read
API information that is deemed safe to be publicly accessible (including Cus-
tomResourceDefinitions). To disable anonymous unauthenticated access add
`--anonymous-auth=false` to the API server configuration.

To view the configuration of these roles via `kubectl` run:

```
kubectl get clusterroles system:discovery -o yaml
```

NOTE: editing the role is not recommended as changes will be overwritten on
API server restart via auto-reconciliation (see above).

Default ClusterRole	Default ClusterRoleBinding	Description
system:basic-user	**system:authenticated** and **system:unauthenticated** groups	Allows a user read-only access to basic information about themselve
system:discovery	**system:authenticated** and **system:unauthenticated** groups	Allows read-only access to API discovery endpoints needed to disco

User-facing Roles

Some of the default roles are not `system:` prefixed. These are intended to be
user-facing roles. They include super-user roles (`cluster-admin`), roles intended
to be granted cluster-wide using ClusterRoleBindings (`cluster-status`), and
roles intended to be granted within particular namespaces using RoleBindings
(`admin`, `edit`, `view`).

As of 1.9, user-facing roles use ClusterRole Aggregation to allow admins to
include rules for custom resources on these roles. To add rules to the "admin",
"edit", or "view" role, create a ClusterRole with one or more of the following
labels:

```
metadata:
```

```
labels:
  rbac.authorization.k8s.io/aggregate-to-admin: "true"
  rbac.authorization.k8s.io/aggregate-to-edit: "true"
  rbac.authorization.k8s.io/aggregate-to-view: "true"
```

Default ClusterRole	Default ClusterRoleBinding	Description
cluster-admin	**system:masters** group	Allows super-user access to perform any action on any resource. Wh
admin	None	Allows admin access, intended to be granted within a namespace us
edit	None	Allows read/write access to most objects in a namespace. It does no
view	None	Allows read-only access to see most objects in a namespace. It does

Core Component Roles

Default ClusterRole	Default ClusterRoleBinding	Description
system:kube-scheduler	**system:kube-scheduler** user	Allows access to the resources required by the kube-scheduler comp
system:volume-scheduler	**system:kube-scheduler** user	Allows access to the volume resources required by the kube-schedule
system:kube-controller-manager	**system:kube-controller-manager** user	Allows access to the resources required by the kube-controller-mana
system:node	None in 1.8+	Allows access to resources required by the kubelet component, **inclu**
system:node-proxier	**system:kube-proxy** user	Allows access to the resources required by the kube-proxy componer

Other Component Roles

Default ClusterRole	Default ClusterRoleBinding	Description
system:auth-delegator	None	Allows delegated authentication and authorization checks. This is c
system:heapster	None	Role for the Heapster component.
system:kube-aggregator	None	Role for the kube-aggregator component.

Default ClusterRole	Default ClusterRoleBinding	Description
system:kube-dns	**kube-dns** service account in the **kube-system** namespace	Role for the kube-dns component.
system:kubelet-api-admin	None	Allows full access to the kubelet API.
system:node-bootstrapper	None	Allows access to the resources required to perform Kubelet TLS boc
system:node-problem-detector	None	Role for the node-problem-detector component.
system:persistent-volume-provisioner	None	Allows access to the resources required by most dynamic volume pro

Controller Roles

The Kubernetes controller manager runs core control loops. When invoked with `--use-service-account-credentials`, each control loop is started using a separate service account. Corresponding roles exist for each control loop, prefixed with `system:controller:`. If the controller manager is not started with `--use-service-account-credentials`, it runs all control loops using its own credential, which must be granted all the relevant roles. These roles include:

- system:controller:attachdetach-controller
- system:controller:certificate-controller
- system:controller:cronjob-controller
- system:controller:daemon-set-controller
- system:controller:deployment-controller
- system:controller:disruption-controller
- system:controller:endpoint-controller
- system:controller:generic-garbage-collector
- system:controller:horizontal-pod-autoscaler
- system:controller:job-controller
- system:controller:namespace-controller
- system:controller:node-controller
- system:controller:persistent-volume-binder
- system:controller:pod-garbage-collector
- system:controller:pv-protection-controller
- system:controller:pvc-protection-controller
- system:controller:replicaset-controller
- system:controller:replication-controller
- system:controller:resourcequota-controller

- system:controller:route-controller
- system:controller:service-account-controller
- system:controller:service-controller
- system:controller:statefulset-controller
- system:controller:ttl-controller

Privilege Escalation Prevention and Bootstrapping

The RBAC API prevents users from escalating privileges by editing roles or role bindings. Because this is enforced at the API level, it applies even when the RBAC authorizer is not in use.

A user can only create/update a role if at least one of the following things is true:

1. they already have all the permissions contained in the role, at the same scope as the object being modified (cluster-wide for a `ClusterRole`, within the same namespace or cluster-wide for a `Role`)
2. they are given explicit permission to perform the `escalate` verb on the `roles` or `clusterroles` resource in the `rbac.authorization.k8s.io` API group (Kubernetes 1.12 and newer)

For example, if "user-1" does not have the ability to list secrets cluster-wide, they cannot create a `ClusterRole` containing that permission. To allow a user to create/update roles:

1. Grant them a role that allows them to create/update `Role` or `ClusterRole` objects, as desired.
2. Grant them permission to include specific permissions in the roles the create/update:
   - implicitly, by giving them those permissions (if they attempt to create or modify a `Role` or `ClusterRole` with permissions they themselves have not been granted, the API request will be forbidden)
   - or explicitly allow specifying any permission in a `Role` or `ClusterRole` by giving them permission to perform the `escalate` verb on `roles` or `clusterroles` resources in the `rbac.authorization.k8s.io` API group (Kubernetes 1.12 and newer)

A user can only create/update a role binding if they already have all the permissions contained in the referenced role (at the same scope as the role binding) *or* if they've been given explicit permission to perform the `bind` verb on the referenced role. For example, if "user-1" does not have the ability to list secrets cluster-wide, they cannot create a `ClusterRoleBinding` to a role that grants that permission. To allow a user to create/update role bindings:

1. Grant them a role that allows them to create/update `RoleBinding` or `ClusterRoleBinding` objects, as desired.
2. Grant them permissions needed to bind a particular role:

- implicitly, by giving them the permissions contained in the role.
- explicitly, by giving them permission to perform the `bind` verb on the particular role (or cluster role).

For example, this cluster role and role binding would allow "user-1" to grant other users the `admin`, `edit`, and `view` roles in the "user-1-namespace" namespace:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: role-grantor
rules:
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["rolebindings"]
  verbs: ["create"]
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["clusterroles"]
  verbs: ["bind"]
  resourceNames: ["admin","edit","view"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: role-grantor-binding
  namespace: user-1-namespace
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: role-grantor
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: user-1
```

When bootstrapping the first roles and role bindings, it is necessary for the initial user to grant permissions they do not yet have. To bootstrap initial roles and role bindings:

- Use a credential with the `system:masters` group, which is bound to the `cluster-admin` super-user role by the default bindings.
- If your API server runs with the insecure port enabled (`--insecure-port`), you can also make API calls via that port, which does not enforce authentication or authorization.

Command-line Utilities

Two `kubectl` commands exist to grant roles within a namespace or across the entire cluster.

`kubectl create rolebinding`

Grants a `Role` or `ClusterRole` within a specific namespace. Examples:

- Grant the `admin ClusterRole` to a user named "bob" in the namespace "acme":

  `kubectl create rolebinding bob-admin-binding --clusterrole=admin --user=bob --namespace`

- Grant the `view ClusterRole` to a service account named "myapp" in the namespace "acme":

  `kubectl create rolebinding myapp-view-binding --clusterrole=view --serviceaccount=acme:`

`kubectl create clusterrolebinding`

Grants a `ClusterRole` across the entire cluster, including all namespaces. Examples:

- Grant the `cluster-admin ClusterRole` to a user named "root" across the entire cluster:

  `kubectl create clusterrolebinding root-cluster-admin-binding --clusterrole=cluster-admi`

- Grant the `system:node ClusterRole` to a user named "kubelet" across the entire cluster:

  `kubectl create clusterrolebinding kubelet-node-binding --clusterrole=system:node --user`

- Grant the `view ClusterRole` to a service account named "myapp" in the namespace "acme" across the entire cluster:

  `kubectl create clusterrolebinding myapp-view-binding --clusterrole=view --serviceaccoun`

See the CLI help for detailed usage.

Service Account Permissions

Default RBAC policies grant scoped permissions to control-plane components, nodes, and controllers, but grant *no permissions* to service accounts outside the `kube-system` namespace (beyond discovery permissions given to all authenticated users).

This allows you to grant particular roles to particular service accounts as needed. Fine-grained role bindings provide greater security, but require more effort to administrate. Broader grants can give unnecessary (and potentially escalating) API access to service accounts, but are easier to administrate.

In order from most secure to least secure, the approaches are:

1. Grant a role to an application-specific service account (best practice)

   This requires the application to specify a `serviceAccountName` in its pod spec, and for the service account to be created (via the API, application manifest, `kubectl create serviceaccount`, etc.).

   For example, grant read-only permission within "my-namespace" to the "my-sa" service account:

   ```
   kubectl create rolebinding my-sa-view \
     --clusterrole=view \
     --serviceaccount=my-namespace:my-sa \
     --namespace=my-namespace
   ```

2. Grant a role to the "default" service account in a namespace

   If an application does not specify a `serviceAccountName`, it uses the "default" service account.

   > **Note:** Permissions given to the "default" service account are available to any pod in the namespace that does not specify a `serviceAccountName`.

   For example, grant read-only permission within "my-namespace" to the "default" service account:

   ```
   kubectl create rolebinding default-view \
     --clusterrole=view \
     --serviceaccount=my-namespace:default \
     --namespace=my-namespace
   ```

   Many add-ons currently run as the "default" service account in the `kube-system` namespace. To allow those add-ons to run with super-user access, grant cluster-admin permissions to the "default" service account in the `kube-system` namespace.

   > **Note:** Enabling this means the `kube-system` namespace contains secrets that grant super-user access to the API.

   ```
   kubectl create clusterrolebinding add-on-cluster-admin \
     --clusterrole=cluster-admin \
     --serviceaccount=kube-system:default
   ```

3. Grant a role to all service accounts in a namespace

If you want all applications in a namespace to have a role, no matter what service account they use, you can grant a role to the service account group for that namespace.

For example, grant read-only permission within "my-namespace" to all service accounts in that namespace:

```
kubectl create rolebinding serviceaccounts-view \
  --clusterrole=view \
  --group=system:serviceaccounts:my-namespace \
  --namespace=my-namespace
```

4. Grant a limited role to all service accounts cluster-wide (discouraged)

If you don't want to manage permissions per-namespace, you can grant a cluster-wide role to all service accounts.

For example, grant read-only permission across all namespaces to all service accounts in the cluster:

```
kubectl create clusterrolebinding serviceaccounts-view \
  --clusterrole=view \
 --group=system:serviceaccounts
```

5. Grant super-user access to all service accounts cluster-wide (strongly discouraged)

If you don't care about partitioning permissions at all, you can grant super-user access to all service accounts.

> **Warning:**
>
> ```
> This allows any user with read access
> to secrets or the ability to create a pod to access super-user
> credentials.
> ```

```
kubectl create clusterrolebinding serviceaccounts-cluster-admin \
  --clusterrole=cluster-admin \
  --group=system:serviceaccounts
```

Upgrading from 1.5

Prior to Kubernetes 1.6, many deployments used very permissive ABAC policies, including granting full API access to all service accounts.

Default RBAC policies grant scoped permissions to control-plane components, nodes, and controllers, but grant *no permissions* to service accounts outside the `kube-system` namespace (beyond discovery permissions given to all authenticated users).

While far more secure, this can be disruptive to existing workloads expecting to automatically receive API permissions. Here are two approaches for managing this transition:

Parallel Authorizers

Run both the RBAC and ABAC authorizers, and specify a policy file that contains the legacy ABAC policy:

```
--authorization-mode=RBAC,ABAC --authorization-policy-file=mypolicy.json
```

The RBAC authorizer will attempt to authorize requests first. If it denies an API request, the ABAC authorizer is then run. This means that any request allowed by *either* the RBAC or ABAC policies is allowed.

When the apiserver is run with a log level of 5 or higher for the RBAC component (`--vmodule=rbac*=5` or `--v=5`), you can see RBAC denials in the apiserver log (prefixed with `RBAC DENY:`). You can use that information to determine which roles need to be granted to which users, groups, or service accounts. Once you have granted roles to service accounts and workloads are running with no RBAC denial messages in the server logs, you can remove the ABAC authorizer.

Permissive RBAC Permissions

You can replicate a permissive policy using RBAC role bindings.

> **Warning:**
>
> The following policy allows **ALL** service accounts to act as cluster administrators. Any application running in a container receives service account credentials automatically, and could perform any action against the API, including viewing secrets and modifying permissions. This is not a recommended policy.
>
> ```
> kubectl create clusterrolebinding permissive-binding \
>   --clusterrole=cluster-admin \
>   --user=admin \
>   --user=kubelet \
>   --group=system:serviceaccounts
> ```

Edit This Page

Controlling Access to the Kubernetes API

This page provides an overview of controlling access to the Kubernetes API.

- Transport Security
- Authentication
- Authorization
- Admission Control
- API Server Ports and IPs

Users access the API using `kubectl`, client libraries, or by making REST requests. Both human users and Kubernetes service accounts can be authorized for API access. When a request reaches the API, it goes through several stages, illustrated in the following diagram:
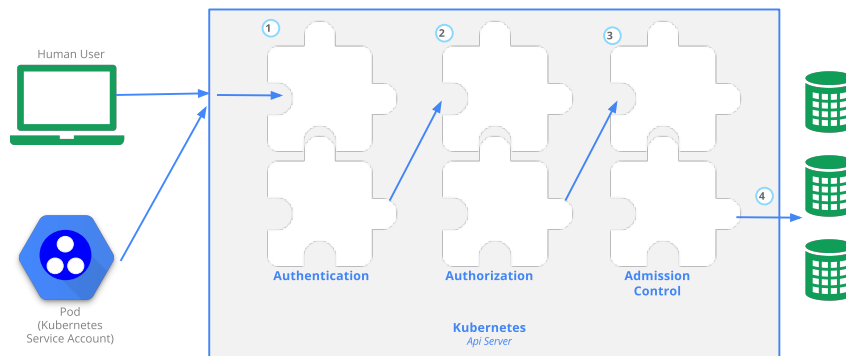
Transport Security

In a typical Kubernetes cluster, the API serves on port 443. The API server presents a certificate. This certificate is often self-signed, so `$USER/.kube/config` on the user's machine typically contains the root certificate for the API server's certificate, which when specified is used in place of the system default root certificate. This certificate is typically automatically written into your `$USER/.kube/config` when you create a cluster yourself using `kube-up.sh`. If the cluster has multiple users, then the creator needs to share the certificate with other users.

Authentication

Once TLS is established, the HTTP request moves to the Authentication step. This is shown as step **1** in the diagram. The cluster creation script or cluster

admin configures the API server to run one or more Authenticator Modules. Authenticators are described in more detail here.

The input to the authentication step is the entire HTTP request, however, it typically just examines the headers and/or client certificate.

Authentication modules include Client Certificates, Password, and Plain Tokens, Bootstrap Tokens, and JWT Tokens (used for service accounts).

Multiple authentication modules can be specified, in which case each one is tried in sequence, until one of them succeeds.

On GCE, Client Certificates, Password, Plain Tokens, and JWT Tokens are all enabled.

If the request cannot be authenticated, it is rejected with HTTP status code 401. Otherwise, the user is authenticated as a specific `username`, and the user name is available to subsequent steps to use in their decisions. Some authenticators also provide the group memberships of the user, while other authenticators do not.

While Kubernetes uses `usernames` for access control decisions and in request logging, it does not have a `user` object nor does it store usernames or other information about users in its object store.

Authorization

After the request is authenticated as coming from a specific user, the request must be authorized. This is shown as step **2** in the diagram.

A request must include the username of the requester, the requested action, and the object affected by the action. The request is authorized if an existing policy declares that the user has permissions to complete the requested action.

For example, if Bob has the policy below, then he can read pods only in the namespace `projectCaribou`:

```
{
    "apiVersion": "abac.authorization.kubernetes.io/v1beta1",
    "kind": "Policy",
    "spec": {
        "user": "bob",
        "namespace": "projectCaribou",
        "resource": "pods",
        "readonly": true
    }
}
```

If Bob makes the following request, the request is authorized because he is allowed to read objects in the `projectCaribou` namespace:

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "spec": {
    "resourceAttributes": {
      "namespace": "projectCaribou",
      "verb": "get",
      "group": "unicorn.example.org",
      "resource": "pods"
    }
  }
}
```

If Bob makes a request to write (`create` or `update`) to the objects in the `projectCaribou` namespace, his authorization is denied. If Bob makes a request to read (`get`) objects in a different namespace such as `projectFish`, then his authorization is denied.

Kubernetes authorization requires that you use common REST attributes to interact with existing organization-wide or cloud-provider-wide access control systems. It is important to use REST formatting because these control systems might interact with other APIs besides the Kubernetes API.

Kubernetes supports multiple authorization modules, such as ABAC mode, RBAC Mode, and Webhook mode. When an administrator creates a cluster, they configured the authorization modules that should be used in the API server. If more than one authorization modules are configured, Kubernetes checks each module, and if any module authorizes the request, then the request can proceed. If all of the modules deny the request, then the request is denied (HTTP status code 403).

To learn more about Kubernetes authorization, including details about creating policies using the supported authorization modules, see Authorization Overview.

Admission Control

Admission Control Modules are software modules that can modify or reject requests. In addition to the attributes available to Authorization Modules, Admission Control Modules can access the contents of the object that is being created or updated. They act on objects being created, deleted, updated or connected (proxy), but not reads.

Multiple admission controllers can be configured. Each is called in order.

This is shown as step **3** in the diagram.

Unlike Authentication and Authorization Modules, if any admission controller module rejects, then the request is immediately rejected.

In addition to rejecting objects, admission controllers can also set complex defaults for fields.

The available Admission Control Modules are described here.

Once a request passes all admission controllers, it is validated using the validation routines for the corresponding API object, and then written to the object store (shown as step **4**).

API Server Ports and IPs

The previous discussion applies to requests sent to the secure port of the API server (the typical case). The API server can actually serve on 2 ports:

By default the Kubernetes API server serves HTTP on 2 ports:

1. `Localhost Port:`

   - is intended for testing and bootstrap, and for other components of the master node (scheduler, controller-manager) to talk to the API
   - no TLS
   - default is port 8080, change with `--insecure-port` flag.
   - default IP is localhost, change with `--insecure-bind-address` flag.
   - request **bypasses** authentication and authorization modules.
   - request handled by admission control module(s).
   - protected by need to have host access

2. `Secure Port:`

   - use whenever possible
   - uses TLS. Set cert with `--tls-cert-file` and key with `--tls-private-key-file` flag.
   - default is port 6443, change with `--secure-port` flag.
   - default IP is first non-localhost network interface, change with `--bind-address` flag.
   - request handled by authentication and authorization modules.
   - request handled by admission control module(s).
   - authentication and authorization modules run.

When the cluster is created by `kube-up.sh`, on Google Compute Engine (GCE), and on several other cloud providers, the API server serves on port 443. On GCE, a firewall rule is configured on the project to allow external HTTPS access to the API. Other cluster setup methods vary.

Edit This Page

Authenticating

This page provides an overview of authenticating.

- Users in Kubernetes
- Authentication strategies
- Anonymous requests
- User impersonation
- client-go credential plugins

Users in Kubernetes

All Kubernetes clusters have two categories of users: service accounts managed by Kubernetes, and normal users.

Normal users are assumed to be managed by an outside, independent service. An admin distributing private keys, a user store like Keystone or Google Accounts, even a file with a list of usernames and passwords. In this regard, *Kubernetes does not have objects which represent normal user accounts.* Normal users cannot be added to a cluster through an API call.

In contrast, service accounts are users managed by the Kubernetes API. They are bound to specific namespaces, and created automatically by the API server or manually through API calls. Service accounts are tied to a set of credentials stored as `Secrets`, which are mounted into pods allowing in-cluster processes to talk to the Kubernetes API.

API requests are tied to either a normal user or a service account, or are treated as anonymous requests. This means every process inside or outside the cluster, from a human user typing `kubectl` on a workstation, to `kubelets` on nodes, to members of the control plane, must authenticate when making requests to the API server, or be treated as an anonymous user.

Authentication strategies

Kubernetes uses client certificates, bearer tokens, an authenticating proxy, or HTTP basic auth to authenticate API requests through authentication plugins. As HTTP requests are made to the API server, plugins attempt to associate the following attributes with the request:

- Username: a string which identifies the end user. Common values might be `kube-admin` or `jane@example.com`.
- UID: a string which identifies the end user and attempts to be more consistent and unique than username.
- Groups: a set of strings which associate users with a set of commonly grouped users.

- Extra fields: a map of strings to list of strings which holds additional information authorizers may find useful.

All values are opaque to the authentication system and only hold significance when interpreted by an authorizer.

You can enable multiple authentication methods at once. You should usually use at least two methods:

- service account tokens for service accounts
- at least one other method for user authentication.

When multiple authenticator modules are enabled, the first module to successfully authenticate the request short-circuits evaluation. The API server does not guarantee the order authenticators run in.

The `system:authenticated` group is included in the list of groups for all authenticated users.

Integrations with other authentication protocols (LDAP, SAML, Kerberos, alternate x509 schemes, etc) can be accomplished using an authenticating proxy or the authentication webhook.

X509 Client Certs

Client certificate authentication is enabled by passing the `--client-ca-file=SOMEFILE` option to API server. The referenced file must contain one or more certificates authorities to use to validate client certificates presented to the API server. If a client certificate is presented and verified, the common name of the subject is used as the user name for the request. As of Kubernetes 1.4, client certificates can also indicate a user's group memberships using the certificate's organization fields. To include multiple group memberships for a user, include multiple organization fields in the certificate.

For example, using the `openssl` command line tool to generate a certificate signing request:

```
openssl req -new -key jbeda.pem -out jbeda-csr.pem -subj "/CN=jbeda/O=app1/O=app2"
```

This would create a CSR for the username "jbeda", belonging to two groups, "app1" and "app2".

See Managing Certificates for how to generate a client cert.

Static Token File

The API server reads bearer tokens from a file when given the `--token-auth-file=SOMEFILE` option on the command line. Currently, tokens last indefinitely, and the token list cannot be changed without restarting API server.

The token file is a csv file with a minimum of 3 columns: token, user name, user uid, followed by optional group names.

> **Note:**
>
> If you have more than one group the column must be double quoted e.g.
>
> ```
> token,user,uid,"group1,group2,group3"
> ```

Putting a Bearer Token in a Request

When using bearer token authentication from an http client, the API server expects an `Authorization` header with a value of `Bearer THETOKEN`. The bearer token must be a character sequence that can be put in an HTTP header value using no more than the encoding and quoting facilities of HTTP. For example: if the bearer token is `31ada4fd-adec-460c-809a-9e56ceb75269` then it would appear in an HTTP header as shown below.

```
Authorization: Bearer 31ada4fd-adec-460c-809a-9e56ceb75269
```

Bootstrap Tokens

This feature is currently in **alpha**.

To allow for streamlined bootstrapping for new clusters, Kubernetes includes a dynamically-managed Bearer token type called a *Bootstrap Token*. These tokens are stored as Secrets in the `kube-system` namespace, where they can be dynamically managed and created. Controller Manager contains a TokenCleaner controller that deletes bootstrap tokens as they expire.

The tokens are of the form `[a-z0-9]{6}.[a-z0-9]{16}`. The first component is a Token ID and the second component is the Token Secret. You specify the token in an HTTP header as follows:

```
Authorization: Bearer 781292.db7bc3a58fc5f07e
```

You must enable the Bootstrap Token Authenticator with the `--enable-bootstrap-token-auth` flag on the API Server. You must enable the TokenCleaner controller via the `--controllers` flag on the Controller Manager. This is done with something like `--controllers=*,tokencleaner`. `kubeadm` will do this for you if you are using it to bootstrap a cluster.

The authenticator authenticates as `system:bootstrap:<Token ID>`. It is included in the `system:bootstrappers` group. The naming and groups are intentionally limited to discourage users from using these tokens past bootstrapping. The user names and group can be used (and are used by `kubeadm`) to craft the appropriate authorization policies to support bootstrapping a cluster.

Please see Bootstrap Tokens for in depth documentation on the Bootstrap Token authenticator and controllers along with how to manage these tokens with `kubeadm`.

Static Password File

Basic authentication is enabled by passing the `--basic-auth-file=SOMEFILE` option to API server. Currently, the basic auth credentials last indefinitely, and the password cannot be changed without restarting API server. Note that basic authentication is currently supported for convenience while we finish making the more secure modes described above easier to use.

The basic auth file is a csv file with a minimum of 3 columns: password, user name, user id. In Kubernetes version 1.6 and later, you can specify an optional fourth column containing comma-separated group names. If you have more than one group, you must enclose the fourth column value in double quotes ("). See the following example:

```
password,user,uid,"group1,group2,group3"
```

When using basic authentication from an http client, the API server expects an `Authorization` header with a value of `Basic BASE64ENCODED(USER:PASSWORD)`.

Service Account Tokens

A service account is an automatically enabled authenticator that uses signed bearer tokens to verify requests. The plugin takes two optional flags:

- `--service-account-key-file` A file containing a PEM encoded key for signing bearer tokens. If unspecified, the API server's TLS private key will be used.
- `--service-account-lookup` If enabled, tokens which are deleted from the API will be revoked.

Service accounts are usually created automatically by the API server and associated with pods running in the cluster through the `ServiceAccount` Admission Controller. Bearer tokens are mounted into pods at well-known locations, and allow in-cluster processes to talk to the API server. Accounts may be explicitly associated with pods using the `serviceAccountName` field of a `PodSpec`.

> **Note:** `serviceAccountName` is usually omitted because this is done automatically.

```
apiVersion: apps/v1 # this apiVersion is relevant as of Kubernetes 1.9
kind: Deployment
metadata:
  name: nginx-deployment
  namespace: default
```

```
spec:
  replicas: 3
  template:
    metadata:
    # ...
    spec:
      serviceAccountName: bob-the-bot
      containers:
      - name: nginx
        image: nginx:1.7.9
```

Service account bearer tokens are perfectly valid to use outside the cluster and can be used to create identities for long standing jobs that wish to talk to the Kubernetes API. To manually create a service account, simply use the `kubectl create serviceaccount (NAME)` command. This creates a service account in the current namespace and an associated secret.

```
$ kubectl create serviceaccount jenkins
serviceaccount "jenkins" created
$ kubectl get serviceaccounts jenkins -o yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  # ...
secrets:
- name: jenkins-token-1yvwg
```

The created secret holds the public CA of the API server and a signed JSON Web Token (JWT).

```
$ kubectl get secret jenkins-token-1yvwg -o yaml
apiVersion: v1
data:
  ca.crt: (APISERVER'S CA BASE64 ENCODED)
  namespace: ZGVmYXVsdA==
  token: (BEARER TOKEN BASE64 ENCODED)
kind: Secret
metadata:
  # ...
type: kubernetes.io/service-account-token
```

> **Note:** Values are base64 encoded because secrets are always base64 encoded.

The signed JWT can be used as a bearer token to authenticate as the given service account. See above for how the token is included in a request. Normally these secrets are mounted into pods for in-cluster access to the API server, but can be used from outside the cluster as well.

Service accounts authenticate with the username `system:serviceaccount:(NAMESPACE):(SERVICEACCOUNT)`, and are assigned to the groups `system:serviceaccounts` and `system:serviceaccounts:(NAMESPACE)`.

WARNING: Because service account tokens are stored in secrets, any user with read access to those secrets can authenticate as the service account. Be cautious when granting permissions to service accounts and read capabilities for secrets.

OpenID Connect Tokens

OpenID Connect is a flavor of OAuth2 supported by some OAuth2 providers, notably Azure Active Directory, Salesforce, and Google. The protocol's main extension of OAuth2 is an additional field returned with the access token called an ID Token. This token is a JSON Web Token (JWT) with well known fields, such as a user's email, signed by the server.

To identify the user, the authenticator uses the `id_token` (not the `access_token`) from the OAuth2 token response as a bearer token. See above for how the token is included in a request.
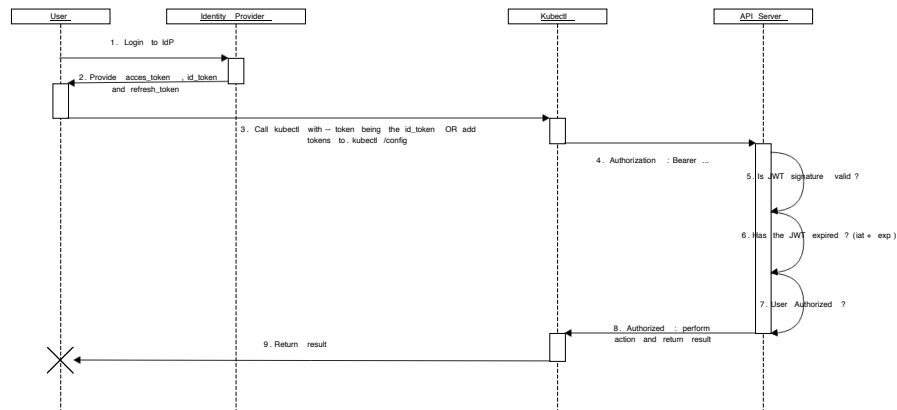
1. Login to your identity provider
2. Your identity provider will provide you with an `access_token`, `id_token` and a `refresh_token`
3. When using `kubectl`, use your `id_token` with the `--token` flag or add it directly to your `kubeconfig`
4. `kubectl` sends your `id_token` in a header called Authorization to the API server
5. The API server will make sure the JWT signature is valid by checking against the certificate named in the configuration
6. Check to make sure the `id_token` hasn't expired
7. Make sure the user is authorized
8. Once authorized the API server returns a response to `kubectl`
9. `kubectl` provides feedback to the user

Since all of the data needed to validate who you are is in the `id_token`, Kubernetes doesn't need to "phone home" to the identity provider. In a model where every request is stateless this provides a very scalable solution for authentication. It does offer a few challenges:

1. Kubernetes has no "web interface" to trigger the authentication process. There is no browser or interface to collect credentials which is why you need to authenticate to your identity provider first.
2. The `id_token` can't be revoked, it's like a certificate so it should be short-lived (only a few minutes) so it can be very annoying to have to get a new token every few minutes.
3. There's no easy way to authenticate to the Kubernetes dashboard without using the `kubectl proxy` command or a reverse proxy that injects the `id_token`.

Configuring the API Server

To enable the plugin, configure the following flags on the API server:

Parameter	Description
`--oidc-issuer-url`	URL of the provider which allows the API server to discover public signing keys.
`--oidc-client-id`	A client id that all tokens must be issued for.
`--oidc-username-claim`	JWT claim to use as the user name. By default `sub`, which is expected to be a u
`--oidc-username-prefix`	Prefix prepended to username claims to prevent clashes with existing names (suc
`--oidc-groups-claim`	JWT claim to use as the user's group. If the claim is present it must be an array
`--oidc-groups-prefix`	Prefix prepended to group claims to prevent clashes with existing names (such a
`--oidc-ca-file`	The path to the certificate for the CA that signed your identity provider's web c

Importantly, the API server is not an OAuth2 client, rather it can only be configured to trust a single issuer. This allows the use of public providers, such as Google, without trusting credentials issued to third parties. Admins who wish to utilize multiple OAuth clients should explore providers which support the `azp` (authorized party) claim, a mechanism for allowing one client to issue tokens on behalf of another.

Kubernetes does not provide an OpenID Connect Identity Provider. You can use an existing public OpenID Connect Identity Provider (such as Google, or others). Or, you can run your own Identity Provider, such as CoreOS dex, Keycloak, CloudFoundry UAA, or Tremolo Security's OpenUnison.

For an identity provider to work with Kubernetes it must:

1. Support OpenID connect discovery; not all do.
2. Run in TLS with non-obsolete ciphers
3. Have a CA signed certificate (even if the CA is not a commercial CA or is self signed)

A note about requirement #3 above, requiring a CA signed certificate. If you deploy your own identity provider (as opposed to one of the cloud providers like Google or Microsoft) you MUST have your identity provider's web server certificate signed by a certificate with the `CA` flag set to `TRUE`, even if it is self signed. This is due to GoLang's TLS client implementation being very strict to the standards around certificate validation. If you don't have a CA handy, you can use this script from the CoreOS team to create a simple CA and a signed certificate and key pair. Or you can use this similar script that generates SHA256 certs with a longer life and larger key size.

Setup instructions for specific systems:

- UAA
- Dex
- OpenUnison

Using kubectl

Option 1 - OIDC Authenticator

The first option is to use the kubectl `oidc` authenticator, which sets the `id_token` as a bearer token for all requests and refreshes the token once it expires. After you've logged into your provider, use kubectl to add your `id_token`, `refresh_token`, `client_id`, and `client_secret` to configure the plugin.

Providers that don't return an `id_token` as part of their refresh token response aren't supported by this plugin and should use "Option 2" below.

```
kubectl config set-credentials USER_NAME \
   --auth-provider=oidc \
   --auth-provider-arg=idp-issuer-url=( issuer url ) \
   --auth-provider-arg=client-id=( your client id ) \
   --auth-provider-arg=client-secret=( your client secret ) \
   --auth-provider-arg=refresh-token=( your refresh token ) \
   --auth-provider-arg=idp-certificate-authority=( path to your ca certificate ) \
   --auth-provider-arg=id-token=( your id_token )
```

As an example, running the below command after authenticating to your identity provider:

```
kubectl config set-credentials mmosley  \
        --auth-provider=oidc  \
        --auth-provider-arg=idp-issuer-url=https://oidcidp.tremolo.lan:8443/auth/idp/OidcIdP
        --auth-provider-arg=client-id=kubernetes  \
        --auth-provider-arg=client-secret=1db158f6-177d-4d9c-8a8b-d36869918ec5  \
        --auth-provider-arg=refresh-token=q1bKLFOyUiosTfawzA93TzZIDzH2TNa2SMm0zEiPKTUwME6BkE
        --auth-provider-arg=idp-certificate-authority=/root/ca.pem \
```

```
                --auth-provider-arg=id-token=eyJraWQiOiJDTj1vaWRjaWRwLnRyZW1vbG8ubGFuLCBPVT1EZW1vLCBP
```

Which would produce the below configuration:

```
users:
- name: mmosley
  user:
    auth-provider:
      config:
        client-id: kubernetes
        client-secret: 1db158f6-177d-4d9c-8a8b-d36869918ec5
        id-token: eyJraWQiOiJDTj1vaWRjaWRwLnRyZW1vbG8ubGFuLCBPVT1EZW1vLCBPPVRybWVVvbG8gU2VjdX
        idp-certificate-authority: /root/ca.pem
        idp-issuer-url: https://oidcidp.tremolo.lan:8443/auth/idp/OidcIdP
        refresh-token: q1bKLFOyUiosTfawzA93TzZIDzH2TNa2SMm0zEiPKTUwME6BkEo6Sql5yUWVBSWpKUGph
      name: oidc
```

Once your `id_token` expires, `kubectl` will attempt to refresh your `id_token`
using your `refresh_token` and `client_secret` storing the new values for the
`refresh_token` and `id_token` in your `.kube/config`.

Option 2 - Use the `--token` Option

The `kubectl` command lets you pass in a token using the `--token` option. Sim-
ply copy and paste the `id_token` into this option:

```
kubectl --token=eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwczovL21sYi50cmVtb2xvLmxhbjjo4MDQzL2F1dG
```


Webhook Token Authentication

Webhook authentication is a hook for verifying bearer tokens.

- `--authentication-token-webhook-config-file` a configuration file de-
  scribing how to access the remote webhook service.
- `--authentication-token-webhook-cache-ttl` how long to cache
  authentication decisions. Defaults to two minutes.

The configuration file uses the kubeconfig file format. Within the file, `clusters`
refers to the remote service and `users` refers to the API server webhook. An
example would be:

```
# Kubernetes API version
apiVersion: v1
# kind of the API object
kind: Config
# clusters refers to the remote service.
clusters:
  - name: name-of-remote-authn-service
```

```
      cluster:
        certificate-authority: /path/to/ca.pem        # CA for verifying the remote service.
        server: https://authn.example.com/authenticate # URL of remote service to query. Must

# users refers to the API server's webhook configuration.
users:
  - name: name-of-api-server
    user:
      client-certificate: /path/to/cert.pem # cert for the webhook plugin to use
      client-key: /path/to/key.pem          # key matching the cert

# kubeconfig files require a context. Provide one for the API server.
current-context: webhook
contexts:
- context:
    cluster: name-of-remote-authn-service
    user: name-of-api-sever
  name: webhook
```

When a client attempts to authenticate with the API server using a bearer token as discussed above, the authentication webhook POSTs a JSON-serialized `authentication.k8s.io/v1beta1 TokenReview` object containing the token to the remote service. Kubernetes will not challenge a request that lacks such a header.

Note that webhook API objects are subject to the same versioning compatibility rules as other Kubernetes API objects. Implementers should be aware of looser compatibility promises for beta objects and check the "apiVersion" field of the request to ensure correct deserialization. Additionally, the API server must enable the `authentication.k8s.io/v1beta1` API extensions group (`--runtime-config=authentication.k8s.io/v1beta1=true`).

The POST body will be of the following format:

```
{
  "apiVersion": "authentication.k8s.io/v1beta1",
  "kind": "TokenReview",
  "spec": {
    "token": "(BEARERTOKEN)"
  }
}
```

The remote service is expected to fill the `status` field of the request to indicate the success of the login. The response body's `spec` field is ignored and may be omitted. A successful validation of the bearer token would return:

```
{
  "apiVersion": "authentication.k8s.io/v1beta1",
  "kind": "TokenReview",
```

```
  "status": {
    "authenticated": true,
    "user": {
      "username": "janedoe@example.com",
      "uid": "42",
      "groups": [
        "developers",
        "qa"
      ],
      "extra": {
        "extrafield1": [
          "extravalue1",
          "extravalue2"
        ]
      }
    }
  }
}
```

An unsuccessful request would return:

```
{
  "apiVersion": "authentication.k8s.io/v1beta1",
  "kind": "TokenReview",
  "status": {
    "authenticated": false
  }
}
```

HTTP status codes can be used to supply additional error context.

Authenticating Proxy

The API server can be configured to identify users from request header values, such as `X-Remote-User`. It is designed for use in combination with an authenticating proxy, which sets the request header value.

- `--requestheader-username-headers` Required, case-insensitive. Header names to check, in order, for the user identity. The first header containing a value is used as the username.
- `--requestheader-group-headers` 1.6+. Optional, case-insensitive. "X-Remote-Group" is suggested. Header names to check, in order, for the user's groups. All values in all specified headers are used as group names.
- `--requestheader-extra-headers-prefix` 1.6+. Optional, case-insensitive. "X-Remote-Extra-" is suggested. Header prefixes to look for to determine extra information about the user (typically used by the configured authorization plugin). Any headers beginning with any of the

specified prefixes have the prefix removed. The remainder of the header name is lowercased and percent-decoded and becomes the extra key, and the header value is the extra value.

Note: Prior to 1.11.3 (and 1.10.7, 1.9.11), the extra key could only contain characters which were legal in HTTP header labels.

For example, with this configuration:

```
--requestheader-username-headers=X-Remote-User
--requestheader-group-headers=X-Remote-Group
--requestheader-extra-headers-prefix=X-Remote-Extra-
```

this request:

```
GET / HTTP/1.1
X-Remote-User: fido
X-Remote-Group: dogs
X-Remote-Group: dachshunds
X-Remote-Extra-Acme.com%2Fproject: some-project
X-Remote-Extra-Scopes: openid
X-Remote-Extra-Scopes: profile
```

would result in this user info:

```
name: fido
groups:
- dogs
- dachshunds
extra:
  acme.com/project:
  - some-project
  scopes:
  - openid
  - profile
```

In order to prevent header spoofing, the authenticating proxy is required to present a valid client certificate to the API server for validation against the specified CA before the request headers are checked. WARNING: do **not** reuse a CA that is used in a different context unless you understand the risks and the mechanisms to protect the CA's usage.

- `--requestheader-client-ca-file` Required. PEM-encoded certificate bundle. A valid client certificate must be presented and validated against the certificate authorities in the specified file before the request headers are checked for user names.
- `--requestheader-allowed-names` Optional. List of common names (cn). If set, a valid client certificate with a Common Name (cn) in the specified list must be presented before the request headers are checked for user names. If empty, any Common Name is allowed.

87

Anonymous requests

When enabled, requests that are not rejected by other configured authentication methods are treated as anonymous requests, and given a username of `system:anonymous` and a group of `system:unauthenticated`.

For example, on a server with token authentication configured, and anonymous access enabled, a request providing an invalid bearer token would receive a `401 Unauthorized` error. A request providing no bearer token would be treated as an anonymous request.

In 1.5.1-1.5.x, anonymous access is disabled by default, and can be enabled by passing the `--anonymous-auth=true` option to the API server.

In 1.6+, anonymous access is enabled by default if an authorization mode other than `AlwaysAllow` is used, and can be disabled by passing the `--anonymous-auth=false` option to the API server. Starting in 1.6, the ABAC and RBAC authorizers require explicit authorization of the `system:anonymous` user or the `system:unauthenticated` group, so legacy policy rules that grant access to the * user or * group do not include anonymous users.

User impersonation

A user can act as another user through impersonation headers. These let requests manually override the user info a request authenticates as. For example, an admin could use this feature to debug an authorization policy by temporarily impersonating another user and seeing if a request was denied.

Impersonation requests first authenticate as the requesting user, then switch to the impersonated user info.

- A user makes an API call with their credentials *and* impersonation headers.
- API server authenticates the user.
- API server ensures the authenticated users have impersonation privileges.
- Request user info is replaced with impersonation values.
- Request is evaluated, authorization acts on impersonated user info.

The following HTTP headers can be used to performing an impersonation request:

- `Impersonate-User`: The username to act as.
- `Impersonate-Group`: A group name to act as. Can be provided multiple times to set multiple groups. Optional. Requires "Impersonate-User"
- `Impersonate-Extra-( extra name )`: A dynamic header used to associate extra fields with the user. Optional. Requires "Impersonate-User". In order to be preserved consistently, (`extra name`) should be lower-

case, and any characters which aren't legal in HTTP header labels MUST be utf8 and percent-encoded.

Note: Prior to 1.11.3 (and 1.10.7, 1.9.11), (`extra name`) could only contain characters which were legal in HTTP header labels.

An example set of headers:

```
Impersonate-User: jane.doe@example.com
Impersonate-Group: developers
Impersonate-Group: admins
Impersonate-Extra-dn: cn=jane,ou=engineers,dc=example,dc=com
Impersonate-Extra-acme.com%2Fproject: some-project
Impersonate-Extra-scopes: view
Impersonate-Extra-scopes: development
```

When using `kubectl` set the `--as` flag to configure the `Impersonate-User` header, set the `--as-group` flag to configure the `Impersonate-Group` header.

```
$ kubectl drain mynode
Error from server (Forbidden): User "clark" cannot get nodes at the cluster scope. (get node

$ kubectl drain mynode --as=superman --as-group=system:masters
node/mynode cordoned
node/mynode drained
```

To impersonate a user, group, or set extra fields, the impersonating user must have the ability to perform the "impersonate" verb on the kind of attribute being impersonated ("user", "group", etc.). For clusters that enable the RBAC authorization plugin, the following ClusterRole encompasses the rules needed to set user and group impersonation headers:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: impersonator
rules:
- apiGroups: [""]
  resources: ["users", "groups", "serviceaccounts"]
  verbs: ["impersonate"]
```

Extra fields are evaluated as sub-resources of the resource "userextras". To allow a user to use impersonation headers for the extra field "scopes," a user should be granted the following role:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: scopes-impersonator
rules:
```

```
# Can set "Impersonate-Extra-scopes" header.
- apiGroups: ["authentication.k8s.io"]
  resources: ["userextras/scopes"]
  verbs: ["impersonate"]
```

The values of impersonation headers can also be restricted by limiting the set of `resourceNames` a resource can take.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: limited-impersonator
rules:
# Can impersonate the user "jane.doe@example.com"
- apiGroups: [""]
  resources: ["users"]
  verbs: ["impersonate"]
  resourceNames: ["jane.doe@example.com"]

# Can impersonate the groups "developers" and "admins"
- apiGroups: [""]
  resources: ["groups"]
  verbs: ["impersonate"]
  resourceNames: ["developers","admins"]

# Can impersonate the extras field "scopes" with the values "view" and "development"
- apiGroups: ["authentication.k8s.io"]
  resources: ["userextras/scopes"]
  verbs: ["impersonate"]
  resourceNames: ["view", "development"]
```

client-go credential plugins

FEATURE STATE: Kubernetes v1.11 beta

This feature is currently in a *beta* state, meaning:

- The version names contain beta (e.g. v2beta3).
- Code is well tested. Enabling the feature is considered safe. Enabled by default.
- Support for the overall feature will not be dropped, though details may change.
- The schema and/or semantics of objects may change in incompatible ways in a subsequent beta or stable release. When this happens, we will provide instructions for migrating to the next version. This may require deleting, editing, and re-creating API objects. The editing process may require

some thought. This may require downtime for applications that rely on the feature.

- Recommended for only non-business-critical uses because of potential for incompatible changes in subsequent releases. If you have multiple clusters that can be upgraded independently, you may be able to relax this restriction.
- **Please do try our beta features and give feedback on them! After they exit beta, it may not be practical for us to make more changes.**

`k8s.io/client-go` and tools using it such as `kubectl` and `kubelet` are able to execute an external command to receive user credentials.

This feature is intended for client side integrations with authentication protocols not natively supported by `k8s.io/client-go` (LDAP, Kerberos, OAuth2, SAML, etc.). The plugin implements the protocol specific logic, then returns opaque credentials to use. Almost all credential plugin use cases require a server side component with support for the webhook token authenticator to interpret the credential format produced by the client plugin.

Example use case

In a hypothetical use case, an organization would run an external service that exchanges LDAP credentials for user specific, signed tokens. The service would also be capable of responding to webhook token authenticator requests to validate the tokens. Users would be required to install a credential plugin on their workstation.

To authenticate against the API:

- The user issues a `kubectl` command.
- Credential plugin prompts the user for LDAP credentials, exchanges credentials with external service for a token.
- Credential plugin returns token to client-go, which uses it as a bearer token against the API server.
- API server uses the webhook token authenticator to submit a `TokenReview` to the external service.
- External service verifies the signature on the token and returns the user's username and groups.

Configuration

Credential plugins are configured through kubectl config files as part of the user fields.

```
apiVersion: v1
kind: Config
```

```
users:
- name: my-user
  user:
    exec:
      # Command to execute. Required.
      command: "example-client-go-exec-plugin"

      # API version to use when decoding the ExecCredentials resource. Required.
      #
      # The API version returned by the plugin MUST match the version listed here.
      #
      # To integrate with tools that support multiple versions (such as client.authenticatio
      # set an environment variable or pass an argument to the tool that indicates which ver
      apiVersion: "client.authentication.k8s.io/v1beta1"

      # Environment variables to set when executing the plugin. Optional.
      env:
      - name: "FOO"
        value: "bar"

      # Arguments to pass when executing the plugin. Optional.
      args:
      - "arg1"
      - "arg2"
clusters:
- name: my-cluster
  cluster:
    server: "https://172.17.4.100:6443"
    certificate-authority: "/etc/kubernetes/ca.pem"
contexts:
- name: my-cluster
  context:
    cluster: my-cluster
    user: my-user
current-context: my-cluster
```

Relative command paths are interpreted as relative to the directory of the config file. If KUBECONFIG is set to /home/jane/kubeconfig and the exec command is ./bin/example-client-go-exec-plugin, the binary /home/jane/bin/example-client-go-exec-plugin is executed.

```
- name: my-user
  user:
    exec:
      # Path relative to the directory of the kubeconfig
      command: "./bin/example-client-go-exec-plugin"
      apiVersion: "client.authentication.k8s.io/v1beta1"
```

Input and output formats

The executed command prints an `ExecCredential` object to `stdout`. `k8s.io/client-go` authenticates against the Kubernetes API using the returned credentials in the `status`.

When run from an interactive session, `stdin` is exposed directly to the plugin. Plugins should use a TTY check to determine if it's appropriate to prompt a user interactively.

To use bearer token credentials, the plugin returns a token in the status of the `ExecCredential`.

```
{
  "apiVersion": "client.authentication.k8s.io/v1beta1",
  "kind": "ExecCredential",
  "status": {
    "token": "my-bearer-token"
  }
}
```

Alternatively, a PEM-encoded client certificate and key can be returned to use TLS client auth. If the plugin returns a different certificate and key on a subsequent call, `k8s.io/client-go` will close existing connections with the server to force a new TLS handshake.

If specified, `clientKeyData` and `clientCertificateData` must both must be present.

`clientCertificateData` may contain additional intermediate certificates to send to the server.

```
{
  "apiVersion": "client.authentication.k8s.io/v1beta1",
  "kind": "ExecCredential",
  "status": {
    "clientCertificateData": "-----BEGIN CERTIFICATE-----\n...\n-----END CERTIFICATE-----",
    "clientKeyData": "-----BEGIN RSA PRIVATE KEY-----\n...\n-----END RSA PRIVATE KEY-----"
  }
}
```

Optionally, the response can include the expiry of the credential formatted as a RFC3339 timestamp. Presence or absence of an expiry has the following impact:

- If an expiry is included, the bearer token and TLS credentials are cached until the expiry time is reached, or if the server responds with a 401 HTTP status code, or when the process exits.
- If an expiry is omitted, the bearer token and TLS credentials are cached until the server responds with a 401 HTTP status code or until the process exits.

```
{
  "apiVersion": "client.authentication.k8s.io/v1beta1",
  "kind": "ExecCredential",
  "status": {
    "token": "my-bearer-token",
    "expirationTimestamp": "2018-03-05T17:30:20-08:00"
  }
}
```

Edit This Page

Authenticating with Bootstrap Tokens

Bootstrap tokens are a simple bearer token that is meant to be used when
creating new clusters or joining new nodes to an existing cluster. It was built
to support kubeadm, but can be used in other contexts for users that wish to
start clusters without `kubeadm`. It is also built to work, via RBAC policy, with
the Kubelet TLS Bootstrapping system.

- Bootstrap Tokens Overview
- Token Format
- Enabling Bootstrap Token Authentication
- Bootstrap Token Secret Format
- Token Management with kubeadm
- ConfigMap Signing

Bootstrap Tokens Overview

Bootstrap Tokens are defined with a specific type (`bootstrap.kubernetes.io/token`)
of secrets that lives in the `kube-system` namespace. These Secrets are then
read by the Bootstrap Authenticator in the API Server. Expired tokens are
removed with the TokenCleaner controller in the Controller Manager. The
tokens are also used to create a signature for a specific ConfigMap used in a
"discovery" process through a BootstrapSigner controller.

FEATURE STATE: `Kubernetes v1.12` beta

This feature is currently in a *beta* state, meaning:

- The version names contain beta (e.g. v2beta3).
- Code is well tested. Enabling the feature is considered safe. Enabled by
  default.
- Support for the overall feature will not be dropped, though details may
  change.
- The schema and/or semantics of objects may change in incompatible ways
  in a subsequent beta or stable release. When this happens, we will provide

94

instructions for migrating to the next version. This may require deleting, editing, and re-creating API objects. The editing process may require some thought. This may require downtime for applications that rely on the feature.

- Recommended for only non-business-critical uses because of potential for incompatible changes in subsequent releases. If you have multiple clusters that can be upgraded independently, you may be able to relax this restriction.
- **Please do try our beta features and give feedback on them! After they exit beta, it may not be practical for us to make more changes.**

Token Format

Bootstrap Tokens take the form of `abcdef.0123456789abcdef`. More formally, they must match the regular expression `[a-z0-9]{6}\.[a-z0-9]{16}`.

The first part of the token is the "Token ID" and is considered public information. It is used when referring to a token without leaking the secret part used for authentication. The second part is the "Token Secret" and should only be shared with trusted parties.

Enabling Bootstrap Token Authentication

The Bootstrap Token authenticator can be enabled using the following flag on the API server:

```
--enable-bootstrap-token-auth
```

When enabled, bootstrapping tokens can be used as bearer token credentials to authenticate requests against the API server.

```
Authorization: Bearer 07401b.f395accd246ae52d
```

Tokens authenticate as the username `system:bootstrap:<token id>` and are members of the group `system:bootstrappers`. Additional groups may be specified in the token's Secret.

Expired tokens can be deleted automatically by enabling the `tokencleaner` controller on the controller manager.

```
--controllers=*,tokencleaner
```

Bootstrap Token Secret Format

Each valid token is backed by a secret in the `kube-system` namespace. You can find the full design doc here.

Here is what the secret looks like.

```
apiVersion: v1
kind: Secret
metadata:
  # Name MUST be of form "bootstrap-token-<token id>"
  name: bootstrap-token-07401b
  namespace: kube-system

# Type MUST be 'bootstrap.kubernetes.io/token'
type: bootstrap.kubernetes.io/token
stringData:
  # Human readable description. Optional.
  description: "The default bootstrap token generated by 'kubeadm init'."

  # Token ID and secret. Required.
  token-id: 07401b
  token-secret: f395accd246ae52d

  # Expiration. Optional.
  expiration: 2017-03-10T03:22:11Z

  # Allowed usages.
  usage-bootstrap-authentication: "true"
  usage-bootstrap-signing: "true"

  # Extra groups to authenticate the token as. Must start with "system:bootstrappers:"
  auth-extra-groups: system:bootstrappers:worker,system:bootstrappers:ingress
```

The type of the secret must be `bootstrap.kubernetes.io/token` and the name must be `bootstrap-token-<token id>`. It must also exist in the `kube-system` namespace.

The `usage-bootstrap-*` members indicate what this secret is intended to be used for. A value must be set to `true` to be enabled.

- `usage-bootstrap-authentication` indicates that the token can be used to authenticate to the API server as a bearer token.
- `usage-bootstrap-signing` indicates that the token may be used to sign the `cluster-info` ConfigMap as described below.

The `expiration` field controls the expiry of the token. Expired tokens are rejected when used for authentication and ignored during ConfigMap signing. The expiry value is encoded as an absolute UTC time using RFC3339. Enable the `tokencleaner` controller to automatically delete expired tokens.

Token Management with kubeadm

You can use the `kubeadm` tool to manage tokens on a running cluster. See the kubeadm token docs for details.

ConfigMap Signing

In addition to authentication, the tokens can be used to sign a ConfigMap. This is used early in a cluster bootstrap process before the client trusts the API server. The signed ConfigMap can be authenticated by the shared token.

Enable ConfigMap signing by enabling the `bootstrapsigner` controller on the Controller Manager.

```
--controllers=*,bootstrapsigner
```

The ConfigMap that is signed is `cluster-info` in the `kube-public` namespace. The typical flow is that a client reads this ConfigMap while unauthenticated and ignoring TLS errors. It then validates the payload of the ConfigMap by looking at a signature embedded in the ConfigMap.

The ConfigMap may look like this:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-info
  namespace: kube-public
data:
  jws-kubeconfig-07401b: eyJhbGciOiJIUzI1NiIsImtpZCI6IjA3NDAxYiJ9..tYEfbo6zDNo40MQE07aZcQX2n
  kubeconfig: |
    apiVersion: v1
    clusters:
    - cluster:
        certificate-authority-data: <really long certificate data>
        server: https://10.138.0.2:6443
      name: ""
    contexts: []
    current-context: ""
    kind: Config
    preferences: {}
    users: []
```

The `kubeconfig` member of the ConfigMap is a config file with just the cluster information filled out. The key thing being communicated here is the `certificate-authority-data`. This may be expanded in the future.

The signature is a JWS signature using the "detached" mode. To validate the signature, the user should encode the `kubeconfig` payload according to JWS rules (base64 encoded while discarding any trailing `=`). That encoded payload is then used to form a whole JWS by inserting it between the 2 dots. You can verify the JWS using the `HS256` scheme (HMAC-SHA256) with the full token (e.g. `07401b.f395accd246ae52d`) as the shared secret. Users *must* verify that HS256 is used.

> **Warning:** Any party with a bootstrapping token can create a valid signature for that token. When using ConfigMap signing it's discouraged to share the same token with many clients, since a compromised client can potentially man-in-the middle another client relying on the signature to bootstrap TLS trust.

Consult the kubeadm security model section for more information.

Edit This Page

Using Admission Controllers

This page provides an overview of Admission Controllers.

- What are they?
- Why do I need them?
- How do I turn on an admission controller?
- How do I turn off an admission controller?
- Which plugins are enabled by default?
- What does each admission controller do?
- Is there a recommended set of admission controllers to use?

What are they?

An admission controller is a piece of code that intercepts requests to the Kubernetes API server prior to persistence of the object, but after the request is authenticated and authorized. The controllers consist of the list below, are compiled into the `kube-apiserver` binary, and may only be configured by the cluster administrator. In that list, there are two special controllers: MutatingAdmissionWebhook and ValidatingAdmissionWebhook. These execute the mutating and validating (respectively) admission control webhooks which are configured in the API.

Admission controllers may be "validating", "mutating", or both. Mutating controllers may modify the objects they admit; validating controllers may not.

The admission control process proceeds in two phases. In the first phase, mutating admission controllers are run. In the second phase, validating admission

controllers are run. Note again that some of the controllers are both.

If any of the controllers in either phase reject the request, the entire request is rejected immediately and an error is returned to the end-user.

Finally, in addition to sometimes mutating the object in question, admission controllers may sometimes have side effects, that is, mutate related resources as part of request processing. Incrementing quota usage is the canonical example of why this is necessary. Any such side-effect needs a corresponding reclamation or reconciliation process, as a given admission controller does not know for sure that a given request will pass all of the other admission controllers.

Why do I need them?

Many advanced features in Kubernetes require an admission controller to be enabled in order to properly support the feature. As a result, a Kubernetes API server that is not properly configured with the right set of admission controllers is an incomplete server and will not support all the features you expect.

How do I turn on an admission controller?

The Kubernetes API server flag `enable-admission-plugins` takes a comma-delimited list of admission control plugins to invoke prior to modifying objects in the cluster. For example, the following command line enables the `NamespaceLifecycle` and the `LimitRanger` admission control plugins:

```
kube-apiserver --enable-admission-plugins=NamespaceLifecycle,LimitRanger ...
```

> **Note:** Depending on the way your Kubernetes cluster is deployed and how the API server is started, you may need to apply the settings in different ways. For example, you may have to modify the systemd unit file if the API server is deployed as a systemd service, you may modify the manifest file for the API server if Kubernetes is deployed in a self-hosted way.

How do I turn off an admission controller?

The Kubernetes API server flag `disable-admission-plugins` takes a comma-delimited list of admission control plugins to be disabled, even if they are in the list of plugins enabled by default.

```
kube-apiserver --disable-admission-plugins=PodNodeSelector,AlwaysDeny ...
```

Which plugins are enabled by default?

To see which admission plugins are enabled:

`kube-apiserver -h | grep enable-admission-plugins`

In 1.11, they are:

`NamespaceLifecycle,LimitRanger,ServiceAccount,PersistentVolumeLabel,DefaultStorageClass,Defa`

What does each admission controller do?

AlwaysAdmit (DEPRECATED)

Use this admission controller by itself to pass-through all requests. AlwaysAdmit is DEPRECATED as no real meaning.

AlwaysPullImages

This admission controller modifies every new Pod to force the image pull policy to Always. This is useful in a multitenant cluster so that users can be assured that their private images can only be used by those who have the credentials to pull them. Without this admission controller, once an image has been pulled to a node, any pod from any user can use it simply by knowing the image's name (assuming the Pod is scheduled onto the right node), without any authorization check against the image. When this admission controller is enabled, images are always pulled prior to starting containers, which means valid credentials are required.

AlwaysDeny (DEPRECATED)

Rejects all requests. AlwaysDeny is DEPRECATED as no real meaning.

DefaultStorageClass

This admission controller observes creation of `PersistentVolumeClaim` objects that do not request any specific storage class and automatically adds a default storage class to them. This way, users that do not request any special storage class do not need to care about them at all and they will get the default one.

This admission controller does not do anything when no default storage class is configured. When more than one storage class is marked as default, it rejects any creation of `PersistentVolumeClaim` with an error and an administrator must revisit their `StorageClass` objects and mark only one as default. This

admission controller ignores any `PersistentVolumeClaim` updates; it acts only on creation.

See persistent volume documentation about persistent volume claims and storage classes and how to mark a storage class as default.

DefaultTolerationSeconds

This admission controller sets the default forgiveness toleration for pods to tolerate the taints `notready:NoExecute` and `unreachable:NoExecute` for 5 minutes, if the pods don't already have toleration for taints `node.kubernetes.io/not-ready:NoExecute` or `node.alpha.kubernetes.io/unreachable:NoExecute`.

DenyExecOnPrivileged (deprecated)

This admission controller will intercept all requests to exec a command in a pod if that pod has a privileged container.

If your cluster supports privileged containers, and you want to restrict the ability of end-users to exec commands in those containers, we strongly encourage enabling this admission controller.

This functionality has been merged into DenyEscalatingExec.

DenyEscalatingExec

This admission controller will deny exec and attach commands to pods that run with escalated privileges that allow host access. This includes pods that run as privileged, have access to the host IPC namespace, and have access to the host PID namespace.

If your cluster supports containers that run with escalated privileges, and you want to restrict the ability of end-users to exec commands in those containers, we strongly encourage enabling this admission controller.

EventRateLimit (alpha)

This admission controller mitigates the problem where the API server gets flooded by event requests. The cluster admin can specify event rate limits by:

- Ensuring that `eventratelimit.admission.k8s.io/v1alpha1=true` is included in the `--runtime-config` flag for the API server;
- Enabling the `EventRateLimit` admission controller;

- Referencing an `EventRateLimit` configuration file from the file provided to the API server's command line flag `--admission-control-config-file`:

```
kind: AdmissionConfiguration
apiVersion: apiserver.k8s.io/v1alpha1
plugins:
- name: EventRateLimit
  path: eventconfig.yaml
...
```

There are four types of limits that can be specified in the configuration:

- `Server`: All event requests received by the API server share a single bucket.
- `Namespace`: Each namespace has a dedicated bucket.
- `User`: Each user is allocated a bucket.
- `SourceAndObject`: A bucket is assigned by each combination of source and involved object of the event.

Below is a sample `eventconfig.yaml` for such a configuration:

```
kind: Configuration
apiVersion: eventratelimit.admission.k8s.io/v1alpha1
limits:
- type: Namespace
  qps: 50
  burst: 100
  cacheSize: 2000
- type: User
  qps: 10
  burst: 50
```

See the EventRateLimit proposal for more details.

ExtendedResourceToleration

This plug-in facilitates creation of dedicated nodes with extended resources. If operators want to create dedicated nodes with extended resources (like GPUs, FPGAs etc.), they are expected to taint the node with the extended resource name as the key. This admission controller, if enabled, automatically adds tolerations for such taints to pods requesting extended resources, so users don't have to manually add these tolerations.

ImagePolicyWebhook

The ImagePolicyWebhook admission controller allows a backend webhook to make admission decisions.

Configuration File Format

ImagePolicyWebhook uses a configuration file to set options for the behavior of the backend. This file may be json or yaml and has the following format:

```
imagePolicy:
  kubeConfigFile: /path/to/kubeconfig/for/backend
  # time in s to cache approval
  allowTTL: 50
  # time in s to cache denial
  denyTTL: 50
  # time in ms to wait between retries
  retryBackoff: 500
  # determines behavior if the webhook backend fails
  defaultAllow: true
```

Reference the ImagePolicyWebhook configuration file from the file provided to the API server's command line flag `--admission-control-config-file`:

```
kind: AdmissionConfiguration
apiVersion: apiserver.k8s.io/v1alpha1
plugins:
- name: ImagePolicyWebhook
  path: imagepolicyconfig.yaml
...
```

The ImagePolicyWebhook config file must reference a kubeconfig formatted file which sets up the connection to the backend. It is required that the backend communicate over TLS.

The kubeconfig file's cluster field must point to the remote service, and the user field must contain the returned authorizer.

```
# clusters refers to the remote service.
clusters:
- name: name-of-remote-imagepolicy-service
  cluster:
    certificate-authority: /path/to/ca.pem    # CA for verifying the remote service.
    server: https://images.example.com/policy # URL of remote service to query. Must use 'ht

# users refers to the API server's webhook configuration.
users:
- name: name-of-api-server
  user:
    client-certificate: /path/to/cert.pem # cert for the webhook admission controller to use
    client-key: /path/to/key.pem          # key matching the cert
```

For additional HTTP configuration, refer to the kubeconfig documentation.

Request Payloads

When faced with an admission decision, the API Server POSTs a JSON serialized `imagepolicy.k8s.io/v1alpha1 ImageReview` object describing the action. This object contains fields describing the containers being admitted, as well as any pod annotations that match `*.image-policy.k8s.io/*`.

Note that webhook API objects are subject to the same versioning compatibility rules as other Kubernetes API objects. Implementers should be aware of looser compatibility promises for alpha objects and check the "apiVersion" field of the request to ensure correct deserialization. Additionally, the API Server must enable the imagepolicy.k8s.io/v1alpha1 API extensions group (`--runtime-config=imagepolicy.k8s.io/v1alpha1=true`).

An example request body:

```
{
  "apiVersion":"imagepolicy.k8s.io/v1alpha1",
  "kind":"ImageReview",
  "spec":{
    "containers":[
      {
        "image":"myrepo/myimage:v1"
      },
      {
        "image":"myrepo/myimage@sha256:beb6bd6a68f114c1dc2ea4b28db81bdf91de202a9014972bec5e4
      }
    ],
    "annotations":[
      "mycluster.image-policy.k8s.io/ticket-1234": "break-glass"
    ],
    "namespace":"mynamespace"
  }
}
```

The remote service is expected to fill the ImageReviewStatus field of the request and respond to either allow or disallow access. The response body's "spec" field is ignored and may be omitted. A permissive response would return:

```
{
  "apiVersion": "imagepolicy.k8s.io/v1alpha1",
  "kind": "ImageReview",
  "status": {
    "allowed": true
  }
}
```

To disallow access, the service would return:

```
{
```

```
  "apiVersion": "imagepolicy.k8s.io/v1alpha1",
  "kind": "ImageReview",
  "status": {
    "allowed": false,
    "reason": "image currently blacklisted"
  }
}
```

For further documentation refer to the `imagepolicy.v1alpha1` API objects and `plugin/pkg/admission/imagepolicy/admission.go`.

Extending with Annotations

All annotations on a Pod that match `*.image-policy.k8s.io/*` are sent to the webhook. Sending annotations allows users who are aware of the image policy backend to send extra information to it, and for different backends implementations to accept different information.

Examples of information you might put here are:

- request to "break glass" to override a policy, in case of emergency.
- a ticket number from a ticket system that documents the break-glass request
- provide a hint to the policy server as to the imageID of the image being provided, to save it a lookup

In any case, the annotations are provided by the user and are not validated by Kubernetes in any way. In the future, if an annotation is determined to be widely useful, it may be promoted to a named field of ImageReviewSpec.

Initializers (alpha)

The admission controller determines the initializers of a resource based on the existing `InitializerConfiguration`s. It sets the pending initializers by modifying the metadata of the resource to be created. For more information, please check Dynamic Admission Control.

LimitPodHardAntiAffinityTopology

This admission controller denies any pod that defines `AntiAffinity` topology key other than `kubernetes.io/hostname` in `requiredDuringSchedulingRequiredDuringExecution`.

LimitRanger

This admission controller will observe the incoming request and ensure that it does not violate any of the constraints enumerated in the `LimitRange` object

in a `Namespace`. If you are using `LimitRange` objects in your Kubernetes deployment, you MUST use this admission controller to enforce those constraints. LimitRanger can also be used to apply default resource requests to Pods that don't specify any; currently, the default LimitRanger applies a 0.1 CPU requirement to all Pods in the `default` namespace.

See the limitRange design doc and the example of Limit Range for more details.

MutatingAdmissionWebhook (beta in 1.9)

This admission controller calls any mutating webhooks which match the request. Matching webhooks are called in serial; each one may modify the object if it desires.

This admission controller (as implied by the name) only runs in the mutating phase.

If a webhook called by this has side effects (for example, decrementing quota) it *must* have a reconciliation system, as it is not guaranteed that subsequent webhooks or validating admission controllers will permit the request to finish.

If you disable the MutatingAdmissionWebhook, you must also disable the `MutatingWebhookConfiguration` object in the `admissionregistration.k8s.io/v1beta1` group/version via the `--runtime-config` flag (both are on by default in versions >= 1.9).

Use caution when authoring and installing mutating webhooks

- Users may be confused when the objects they try to create are different from what they get back.
- Built in control loops may break when the objects they try to create are different when read back.
  - Setting originally unset fields is less likely to cause problems than overwriting fields set in the original request. Avoid doing the latter.
- This is a beta feature. Future versions of Kubernetes may restrict the types of mutations these webhooks can make.
- Future changes to control loops for built-in resources or third-party resources may break webhooks that work well today. Even when the webhook installation API is finalized, not all possible webhook behaviors will be guaranteed to be supported indefinitely.

NamespaceAutoProvision

This admission controller examines all incoming requests on namespaced resources and checks if the referenced namespace does exist. It creates a names-

pace if it cannot be found. This admission controller is useful in deployments that do not want to restrict creation of a namespace prior to its usage.

NamespaceExists

This admission controller checks all requests on namespaced resources other than `Namespace` itself. If the namespace referenced from a request doesn't exist, the request is rejected.

NamespaceLifecycle

This admission controller enforces that a `Namespace` that is undergoing termination cannot have new objects created in it, and ensures that requests in a non-existent `Namespace` are rejected. This admission controller also prevents deletion of three system reserved namespaces `default`, `kube-system`, `kube-public`.

A `Namespace` deletion kicks off a sequence of operations that remove all objects (pods, services, etc.) in that namespace. In order to enforce integrity of that process, we strongly recommend running this admission controller.

NodeRestriction

This admission controller limits the `Node` and `Pod` objects a kubelet can modify. In order to be limited by this admission controller, kubelets must use credentials in the `system:nodes` group, with a username in the form `system:node:<nodeName>`. Such kubelets will only be allowed to modify their own `Node` API object, and only modify `Pod` API objects that are bound to their node. In Kubernetes 1.11+, kubelets are not allowed to update or remove taints from their `Node` API object. Future versions may add additional restrictions to ensure kubelets have the minimal set of permissions required to operate correctly.

OwnerReferencesPermissionEnforcement

This admission controller protects the access to the `metadata.ownerReferences` of an object so that only users with "delete" permission to the object can change it. This admission controller also protects the access to `metadata.ownerReferences[x].blockOwnerDeletion` of an object, so that only users with "update" permission to the `finalizers` subresource of the referenced *owner* can change it.

PersistentVolumeLabel (DEPRECATED)

This admission controller automatically attaches region or zone labels to PersistentVolumes as defined by the cloud provider (for example, GCE or AWS). It helps ensure the Pods and the PersistentVolumes mounted are in the same region and/or zone. If the admission controller doesn't support automatic labelling your PersistentVolumes, you may need to add the labels manually to prevent pods from mounting volumes from a different zone. PersistentVolumeLabel is DEPRECATED and labeling persistent volumes has been taken over by cloud controller manager. Starting from 1.11, this admission controller is disabled by default.

PodNodeSelector

This admission controller defaults and limits what node selectors may be used within a namespace by reading a namespace annotation and a global configuration.

Configuration File Format

`PodNodeSelector` uses a configuration file to set options for the behavior of the backend. Note that the configuration file format will move to a versioned file in a future release. This file may be json or yaml and has the following format:

```
podNodeSelectorPluginConfig:
 clusterDefaultNodeSelector: <node-selectors-labels>
 namespace1: <node-selectors-labels>
 namespace2: <node-selectors-labels>
```

Reference the `PodNodeSelector` configuration file from the file provided to the API server's command line flag `--admission-control-config-file`:

```
kind: AdmissionConfiguration
apiVersion: apiserver.k8s.io/v1alpha1
plugins:
- name: PodNodeSelector
  path: podnodeselector.yaml
...
```

Configuration Annotation Format

`PodNodeSelector` uses the annotation key `scheduler.alpha.kubernetes.io/node-selector` to assign node selectors to namespaces.

```
apiVersion: v1
kind: Namespace
```

```
metadata:
  annotations:
    scheduler.alpha.kubernetes.io/node-selector: <node-selectors-labels>
  name: namespace3
```

Internal Behavior

This admission controller has the following behavior:

1. If the `Namespace` has an annotation with a key `scheduler.alpha.kubernetes.io/node-selector`, use its value as the node selector.
2. If the namespace lacks such an annotation, use the `clusterDefaultNodeSelector` defined in the `PodNodeSelector` plugin configuration file as the node selector.
3. Evaluate the pod's node selector against the namespace node selector for conflicts. Conflicts result in rejection.
4. Evaluate the pod's node selector against the namespace-specific whitelist defined the plugin configuration file. Conflicts result in rejection.

   Note: PodNodeSelector allows forcing pods to run on specifically labeled nodes. Also see the PodTolerationRestriction admission plugin, which allows preventing pods from running on specifically tainted nodes.

PersistentVolumeClaimResize

This admission controller implements additional validations for checking incoming `PersistentVolumeClaim` resize requests.

   Note: Support for volume resizing is available as an alpha feature. Admins must set the feature gate `ExpandPersistentVolumes` to `true` to enable resizing.

After enabling the `ExpandPersistentVolumes` feature gate, enabling the `PersistentVolumeClaimResize` admission controller is recommended, too. This admission controller prevents resizing of all claims by default unless a claim's `StorageClass` explicitly enables resizing by setting `allowVolumeExpansion` to `true`.

For example: all `PersistentVolumeClaims` created from the following `StorageClass` support volume expansion:

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: gluster-vol-default
provisioner: kubernetes.io/glusterfs
parameters:
```

```
  resturl: "http://192.168.10.100:8080"
  restuser: ""
  secretNamespace: ""
  secretName: ""
allowVolumeExpansion: true
```

For more information about persistent volume claims, see PersistentVolume-
Claims.

PodPreset

This admission controller injects a pod with the fields specified in a matching
PodPreset. See also PodPreset concept and Inject Information into Pods Using
a PodPreset for more information.

PodSecurityPolicy

This admission controller acts on creation and modification of the pod and
determines if it should be admitted based on the requested security context and
the available Pod Security Policies.

For Kubernetes < 1.6.0, the API Server must enable the extensions/v1beta1/podsecuritypolicy
API extensions group (`--runtime-config=extensions/v1beta1/podsecuritypolicy=true`).

See also Pod Security Policy documentation for more information.

PodTolerationRestriction

This admission controller first verifies any conflict between a pod's tolerations
and its namespace's tolerations, and rejects the pod request if there is a conflict.
It then merges the namespace's tolerations into the pod's tolerations. The
resulting tolerations are checked against the namespace's whitelist of tolerations.
If the check succeeds, the pod request is admitted otherwise rejected.

If the pod's namespace does not have any associated default or whitelist of
tolerations, then the cluster-level default or whitelist of tolerations are used
instead if specified.

Tolerations to a namespace are assigned via the `scheduler.alpha.kubernetes.io/defaultTolerations`
and `scheduler.alpha.kubernetes.io/tolerationsWhitelist` annotation
keys.

Priority

The priority admission controller uses the `priorityClassName` field and populates the integer value of the priority. If the priority class is not found, the Pod is rejected.

ResourceQuota

This admission controller will observe the incoming request and ensure that it does not violate any of the constraints enumerated in the `ResourceQuota` object in a `Namespace`. If you are using `ResourceQuota` objects in your Kubernetes deployment, you MUST use this admission controller to enforce quota constraints.

See the resourceQuota design doc and the example of Resource Quota for more details.

SecurityContextDeny

This admission controller will deny any pod that attempts to set certain escalating SecurityContext fields. This should be enabled if a cluster doesn't utilize pod security policies to restrict the set of values a security context can take.

ServiceAccount

This admission controller implements automation for serviceAccounts. We strongly recommend using this admission controller if you intend to make use of Kubernetes `ServiceAccount` objects.

Storage Object in Use Protection

The `StorageObjectInUseProtection` plugin adds the `kubernetes.io/pvc-protection` or `kubernetes.io/pv-protection` finalizers to newly created Persistent Volume Claims (PVCs) or Persistent Volumes (PV). In case a user deletes a PVC or PV the PVC or PV is not removed until the finalizer is removed from the PVC or PV by PVC or PV Protection Controller. Refer to the Storage Object in Use Protection for more detailed information.

ValidatingAdmissionWebhook (alpha in 1.8; beta in 1.9)

This admission controller calls any validating webhooks which match the request. Matching webhooks are called in parallel; if any of them rejects the request, the request fails. This admission controller only runs in the validation phase; the

webhooks it calls may not mutate the object, as opposed to the webhooks called by the `MutatingAdmissionWebhook` admission controller.

If a webhook called by this has side effects (for example, decrementing quota) it *must* have a reconciliation system, as it is not guaranteed that subsequent webhooks or other validating admission controllers will permit the request to finish.

If you disable the ValidatingAdmissionWebhook, you must also disable the `ValidatingWebhookConfiguration` object in the `admissionregistration.k8s.io/v1beta1` group/version via the `--runtime-config` flag (both are on by default in versions 1.9 and later).

Is there a recommended set of admission controllers to use?

Yes.

For Kubernetes version 1.10 and later, we recommend running the following set of admission controllers using the `--enable-admission-plugins` flag (**order doesn't matter**).

> **Note:** `--admission-control` was deprecated in 1.10 and replaced with `--enable-admission-plugins`.

`--enable-admission-plugins=NamespaceLifecycle,LimitRanger,ServiceAccount,DefaultStorageClass`

For Kubernetes 1.9 and earlier, we recommend running the following set of admission controllers using the `--admission-control` flag (**order matters**).

- v1.9

`--admission-control=NamespaceLifecycle,LimitRanger,ServiceAccount,DefaultStorageClass,Defa`

- It's worth reiterating that in 1.9, these happen in a mutating phase and a validating phase, and that e.g. `ResourceQuota` runs in the validating phase, and therefore is the last admission controller to run. `MutatingAdmissionWebhook` appears before it in this list, because it runs in the mutating phase.

  For earlier versions, there was no concept of validating vs mutating and the admission controllers ran in the exact order specified.

- v1.6 - v1.8

`--admission-control=NamespaceLifecycle,LimitRanger,ServiceAccount,PersistentVolumeLabel,De`

- v1.4 - v1.5

`--admission-control=NamespaceLifecycle,LimitRanger,ServiceAccount,DefaultStorageClass,Reso`

- v1.2 - v1.3

`--admission-control=NamespaceLifecycle,LimitRanger,ServiceAccount,ResourceQuota`

- v1.0 - v1.1

```
--admission-control=NamespaceLifecycle,LimitRanger,SecurityContextDeny,ServiceAccount,Pers
```

Edit This Page

Dynamic Admission Control

The admission controllers documentation introduces how to use standard, plugin-style admission controllers. However, plugin admission controllers are not flexible enough for all use cases, due to the following:

- They need to be compiled into kube-apiserver.
- They are only configurable when the apiserver starts up.

Two features, *Admission Webhooks* (beta in 1.9) and *Initializers* (alpha), address these limitations. They allow admission controllers to be developed out-of-tree and configured at runtime.

This page describes how to use Admission Webhooks and Initializers.

- Admission Webhooks
- Initializers

Admission Webhooks

What are admission webhooks?

Admission webhooks are HTTP callbacks that receive admission requests and do something with them. You can define two types of admission webhooks, validating admission Webhook and mutating admission webhook. With validating admission Webhooks, you may reject requests to enforce custom admission policies. With mutating admission Webhooks, you may change requests to enforce custom defaults.

Experimenting with admission webhooks

Admission webhooks are essentially part of the cluster control-plane. You should write and deploy them with great caution. Please read the user guides for instructions if you intend to write/deploy production-grade admission webhooks. In the following, we describe how to quickly experiment with admission webhooks.

Prerequisites

- Ensure that the Kubernetes cluster is at least as new as v1.9.

- Ensure that MutatingAdmissionWebhook and ValidatingAdmissionWebhook admission controllers are enabled. Here is a recommended set of admission controllers to enable in general.

- Ensure that the admissionregistration.k8s.io/v1beta1 API is enabled.

Write an admission webhook server

Please refer to the implementation of the admission webhook server that is validated in a Kubernetes e2e test. The webhook handles the `admissionReview` requests sent by the apiservers, and sends back its decision wrapped in `admissionResponse`.

The example admission webhook server leaves the `ClientAuth` field empty, which defaults to `NoClientCert`. This means that the webhook server does not authenticate the identity of the clients, supposedly apiservers. If you need mutual TLS or other ways to authenticate the clients, see how to authenticate apiservers.

Deploy the admission webhook service

The webhook server in the e2e test is deployed in the Kubernetes cluster, via the deployment API. The test also creates a service as the front-end of the webhook server. See code.

You may also deploy your webhooks outside of the cluster. You will need to update your webhook client configurations accordingly.

Configure admission webhooks on the fly

You can dynamically configure what resources are subject to what admission webhooks via ValidatingWebhookConfiguration or MutatingWebhookConfiguration.

The following is an example `validatingWebhookConfiguration`, a mutating webhook configuration is similar.

```
apiVersion: admissionregistration.k8s.io/v1beta1
kind: ValidatingWebhookConfiguration
metadata:
  name: <name of this configuration object>
webhooks:
```

114

```
- name: <webhook name, e.g., pod-policy.example.io>
  rules:
  - apiGroups:
    - ""
    apiVersions:
    - v1
    operations:
    - CREATE
    resources:
    - pods
  clientConfig:
    service:
      namespace: <namespace of the front-end service>
      name: <name of the front-end service>
    caBundle: <pem encoded ca cert that signs the server cert used by the webhook>
```

> **Note:** When using `clientConfig.service`, the server cert must be valid for `<svc_name>.<svc_namespace>.svc`.

When an apiserver receives a request that matches one of the `rules`, the apiserver sends an `admissionReview` request to webhook as specified in the `clientConfig`.

After you create the webhook configuration, the system will take a few seconds to honor the new configuration.

> **Note:** When the webhook plugin is deployed into the Kubernetes cluster as a service, it has to expose its service on the 443 port. The communication between the API server and the webhook service may fail if a different port is used.

Authenticate apiservers

If your admission webhooks require authentication, you can configure the apiservers to use basic auth, bearer token, or a cert to authenticate itself to the webhooks. There are three steps to complete the configuration.

- When starting the apiserver, specify the location of the admission control configuration file via the `--admission-control-config-file` flag.

- In the admission control configuration file, specify where the MutatingAdmissionWebhook controller and ValidatingAdmissionWebhook controller should read the credentials. The credentials are stored in kubeConfig files (yes, the same schema that's used by kubectl), so the field name is `kubeConfigFile`. Here is an example admission control configuration file:

```
apiVersion: apiserver.k8s.io/v1alpha1
kind: AdmissionConfiguration
```

```
plugins:
- name: ValidatingAdmissionWebhook
  configuration:
    apiVersion: apiserver.config.k8s.io/v1alpha1
    kind: WebhookAdmission
    kubeConfigFile: <path-to-kubeconfig-file>
- name: MutatingAdmissionWebhook
  configuration:
    apiVersion: apiserver.config.k8s.io/v1alpha1
    kind: WebhookAdmission
    kubeConfigFile: <path-to-kubeconfig-file>
```

The schema of `admissionConfiguration` is defined here.

- In the kubeConfig file, provide the credentials:

```
apiVersion: v1
kind: Config
users:
# DNS name of webhook service, i.e., <service name>.<namespace>.svc, or the URL
# of the webhook server.
- name: 'webhook1.ns1.svc'
  user:
    client-certificate-data: <pem encoded certificate>
    client-key-data: <pem encoded key>
# The `name` supports using * to wildmatch prefixing segments.
- name: '*.webhook-company.org'
  user:
    password: <password>
    username: <name>
# '*' is the default match.
- name: '*'
  user:
    token: <token>
```

Of course you need to set up the webhook server to handle these authentications.

Initializers

What are initializers?

Initializer has two meanings:

- A list of pending pre-initialization tasks, stored in every object's metadata (e.g., "AddMyCorporatePolicySidecar").

- A user customized controller, which actually performs those tasks. The name of the task corresponds to the controller which performs the task.

For clarity, we call them *initializer controllers* in this page.

Once the controller has performed its assigned task, it removes its name from the list. For example, it may send a PATCH that inserts a container in a pod and also removes its name from `metadata.initializers.pending`. Initializers may make mutations to objects.

Objects which have a non-empty initializer list are considered uninitialized, and are not visible in the API unless specifically requested by using the query parameter, `?includeUninitialized=true`.

When to use initializers?

Initializers are useful for admins to force policies (e.g., the AlwaysPullImages admission controller), or to inject defaults (e.g., the DefaultStorageClass admission controller), etc.

> **Note:** If your use case does not involve mutating objects, consider using external admission webhooks, as they have better performance.

How are initializers triggered?

When an object is POSTed, it is checked against all existing `initializerConfiguration` objects (explained below). For all that it matches, all `spec.initializers[].name`s are appended to the new object's `metadata.initializers.pending` field.

An initializer controller should list and watch for uninitialized objects, by using the query parameter `?includeUninitialized=true`. If using client-go, just set listOptions.includeUninitialized to true.

For the observed uninitialized objects, an initializer controller should first check if its name matches `metadata.initializers.pending[0]`. If so, it should then perform its assigned task and remove its name from the list.

Enable initializers alpha feature

Initializers is an alpha feature, so it is disabled by default. To turn it on, you need to:

- Include "Initializers" in the `--enable-admission-plugins` flag when starting `kube-apiserver`. If you have multiple `kube-apiserver` replicas, all should have the same flag setting.

- Enable the dynamic admission controller registration API by adding `admissionregistration.k8s.io/v1alpha1` to the `--runtime-config` flag passed to `kube-apiserver`, e.g. `--runtime-config=admissionregistration.k8s.io/v1alpha1`. Again, all replicas should have the same flag setting.

Deploy an initializer controller

You should deploy an initializer controller via the deployment API.

Configure initializers on the fly

You can configure what initializers are enabled and what resources are subject to the initializers by creating `initializerConfiguration` resources.

You should first deploy the initializer controller and make sure that it is working properly before creating the `initializerConfiguration`. Otherwise, any newly created resources will be stuck in an uninitialized state.

The following is an example `initializerConfiguration`:

```
apiVersion: admissionregistration.k8s.io/v1alpha1
kind: InitializerConfiguration
metadata:
  name: example-config
initializers:
  # the name needs to be fully qualified, i.e., containing at least two "."
  - name: podimage.example.com
    rules:
      # apiGroups, apiVersion, resources all support wildcard "*".
      # "*" cannot be mixed with non-wildcard.
      - apiGroups:
          - ""
        apiVersions:
          - v1
        resources:
          - pods
```

After you create the `initializerConfiguration`, the system will take a few seconds to honor the new configuration. Then, `"podimage.example.com"` will be appended to the `metadata.initializers.pending` field of newly created pods. You should already have a ready "podimage" initializer controller that handles pods whose `metadata.initializers.pending[0].name="podimage.example.com"`. Otherwise the pods will be stuck in an uninitialized state.

Make sure that all expansions of the `<apiGroup, apiVersions, resources>` tuple in a `rule` are valid. If they are not, separate them in different `rules`.

Edit This Page

Managing Service Accounts

This is a Cluster Administrator guide to service accounts. It assumes knowledge of the User Guide to Service Accounts.

Support for authorization and user accounts is planned but incomplete. Sometimes incomplete features are referred to in order to better describe service accounts.

- User accounts vs service accounts
- Service account automation

User accounts vs service accounts

Kubernetes distinguishes between the concept of a user account and a service account for a number of reasons:

- User accounts are for humans. Service accounts are for processes, which run in pods.
- User accounts are intended to be global. Names must be unique across all namespaces of a cluster, future user resource will not be namespaced. Service accounts are namespaced.
- Typically, a cluster's User accounts might be synced from a corporate database, where new user account creation requires special privileges and is tied to complex business processes. Service account creation is intended to be more lightweight, allowing cluster users to create service accounts for specific tasks (i.e. principle of least privilege).
- Auditing considerations for humans and service accounts may differ.
- A config bundle for a complex system may include definition of various service accounts for components of that system. Because service accounts can be created ad-hoc and have namespaced names, such config is portable.

Service account automation

Three separate components cooperate to implement the automation around service accounts:

- A Service account admission controller
- A Token controller
- A Service account controller

Service Account Admission Controller

The modification of pods is implemented via a plugin called an Admission Controller. It is part of the apiserver. It acts synchronously to modify pods as they

are created or updated. When this plugin is active (and it is by default on most distributions), then it does the following when a pod is created or modified:

1. If the pod does not have a `ServiceAccount` set, it sets the `ServiceAccount` to `default`.
2. It ensures that the `ServiceAccount` referenced by the pod exists, and otherwise rejects it.
3. If the pod does not contain any `ImagePullSecrets`, then `ImagePullSecrets` of the `ServiceAccount` are added to the pod.
4. It adds a `volume` to the pod which contains a token for API access.
5. It adds a `volumeSource` to each container of the pod mounted at `/var/run/secrets/kubernetes.io/serviceaccount`.

Token Controller

TokenController runs as part of controller-manager. It acts asynchronously. It:

- observes serviceAccount creation and creates a corresponding Secret to allow API access.
- observes serviceAccount deletion and deletes all corresponding ServiceAccountToken Secrets.
- observes secret addition, and ensures the referenced ServiceAccount exists, and adds a token to the secret if needed.
- observes secret deletion and removes a reference from the corresponding ServiceAccount if needed.

You must pass a service account private key file to the token controller in the controller-manager by using the `--service-account-private-key-file` option. The private key will be used to sign generated service account tokens. Similarly, you must pass the corresponding public key to the kube-apiserver using the `--service-account-key-file` option. The public key will be used to verify the tokens during authentication.

To create additional API tokens

A controller loop ensures a secret with an API token exists for each service account. To create additional API tokens for a service account, create a secret of type `ServiceAccountToken` with an annotation referencing the service account, and the controller will update it with a generated token:

secret.json:

```
{
    "kind": "Secret",
    "apiVersion": "v1",
    "metadata": {
        "name": "mysecretname",
```

```
        "annotations": {
            "kubernetes.io/service-account.name": "myserviceaccount"
        }
    },
    "type": "kubernetes.io/service-account-token"
}
kubectl create -f ./secret.json
kubectl describe secret mysecretname
```

To delete/invalidate a service account token

```
kubectl delete secret mysecretname
```

Service Account Controller

Service Account Controller manages ServiceAccount inside namespaces, and ensures a ServiceAccount named "default" exists in every active namespace.

Edit This Page

Authorization Overview

Learn more about Kubernetes authorization, including details about creating policies using the supported authorization modules.

- Determine Whether a Request is Allowed or Denied
- Review Your Request Attributes
- Determine the Request Verb
- Authorization Modules
- Using Flags for Your Authorization Module
- Privilege escalation via pod creation
- What's next

In Kubernetes, you must be authenticated (logged in) before your request can be authorized (granted permission to access). For information about authentication, see Accessing Control Overview.

Kubernetes expects attributes that are common to REST API requests. This means that Kubernetes authorization works with existing organization-wide or cloud-provider-wide access control systems which may handle other APIs besides the Kubernetes API.

Determine Whether a Request is Allowed or Denied

Kubernetes authorizes API requests using the API server. It evaluates all of the request attributes against all policies and allows or denies the request. All parts of an API request must be allowed by some policy in order to proceed. This means that permissions are denied by default.

(Although Kubernetes uses the API server, access controls and policies that depend on specific fields of specific kinds of objects are handled by Admission Controllers.)

When multiple authorization modules are configured, each is checked in sequence. If any authorizer approves or denies a request, that decision is immediately returned and no other authorizer is consulted. If all modules have no opinion on the request, then the request is denied. A deny returns an HTTP status code 403.

Review Your Request Attributes

Kubernetes reviews only the following API request attributes:

- **user** - The `user` string provided during authentication.
- **group** - The list of group names to which the authenticated user belongs.
- **extra** - A map of arbitrary string keys to string values, provided by the authentication layer.
- **API** - Indicates whether the request is for an API resource.
- **Request path** - Path to miscellaneous non-resource endpoints like `/api` or `/healthz`.
- **API request verb** - API verbs `get`, `list`, `create`, `update`, `patch`, `watch`, `proxy`, `redirect`, `delete`, and `deletecollection` are used for resource requests. To determine the request verb for a resource API endpoint, see Determine the request verb below.
- **HTTP request verb** - HTTP verbs `get`, `post`, `put`, and `delete` are used for non-resource requests.
- **Resource** - The ID or name of the resource that is being accessed (for resource requests only) – For resource requests using `get`, `update`, `patch`, and `delete` verbs, you must provide the resource name.
- **Subresource** - The subresource that is being accessed (for resource requests only).
- **Namespace** - The namespace of the object that is being accessed (for namespaced resource requests only).
- **API group** - The API group being accessed (for resource requests only). An empty string designates the core API group.

Determine the Request Verb

To determine the request verb for a resource API endpoint, review the HTTP verb used and whether or not the request acts on an individual resource or a collection of resources:

HTTP verb	request verb
POST	create
GET, HEAD	get (for individual resources), list (for collections)
PUT	update
PATCH	patch
DELETE	delete (for individual resources), deletecollection (for collections)

Kubernetes sometimes checks authorization for additional permissions using specialized verbs. For example:

- PodSecurityPolicy checks for authorization of the `use` verb on `podsecuritypolicies` resources in the `policy` API group.
- RBAC checks for authorization of the `bind` verb on `roles` and `clusterroles` resources in the `rbac.authorization.k8s.io` API group.
- Authentication layer checks for authorization of the `impersonate` verb on `users`, `groups`, and `serviceaccounts` in the core API group, and the `userextras` in the `authentication.k8s.io` API group.

Authorization Modules

- **Node** - A special-purpose authorizer that grants permissions to kubelets based on the pods they are scheduled to run. To learn more about using the Node authorization mode, see Node Authorization.
- **ABAC** - Attribute-based access control (ABAC) defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes, etc). To learn more about using the ABAC mode, see ABAC Mode.
- **RBAC** - Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. To learn more about using the RBAC mode, see RBAC Mode
    - When specified RBAC (Role-Based Access Control) uses the `rbac.authorization.k8s.io` API group to drive authorization decisions, allowing admins to dynamically configure permission policies through the Kubernetes API.

– To enable RBAC, start the apiserver with `--authorization-mode=RBAC`.
- **Webhook** - A WebHook is an HTTP callback: an HTTP POST that occurs when something happens; a simple event-notification via HTTP POST. A web application implementing WebHooks will POST a message to a URL when certain things happen. To learn more about using the Webhook mode, see Webhook Mode.

Checking API Access

`kubectl` provides the `auth can-i` subcommand for quickly querying the API authorization layer. The command uses the `SelfSubjectAccessReview` API to determine if the current user can perform a given action, and works regardless of the authorization mode used.

```
$ kubectl auth can-i create deployments --namespace dev
yes
$ kubectl auth can-i create deployments --namespace prod
no
```

Administrators can combine this with user impersonation to determine what action other users can perform.

```
$ kubectl auth can-i list secrets --namespace dev --as dave
no
```

`SelfSubjectAccessReview` is part of the `authorization.k8s.io` API group, which exposes the API server authorization to external services. Other resources in this group include:

- `SubjectAccessReview` - Access review for any user, not just the current one. Useful for delegating authorization decisions to the API server. For example, the kubelet and extension API servers use this to determine user access to their own APIs.
- `LocalSubjectAccessReview` - Like `SubjectAccessReview` but restricted to a specific namespace.
- `SelfSubjectRulesReview` - A review which returns the set of actions a user can perform within a namespace. Useful for users to quickly summarize their own access, or for UIs to hide/show actions.

These APIs can be queried by creating normal Kubernetes resources, where the response "status" field of the returned object is the result of the query.

```
$ kubectl create -f - -o yaml << EOF
apiVersion: authorization.k8s.io/v1
kind: SelfSubjectAccessReview
spec:
  resourceAttributes:
    group: apps
    resource: deployments
```

```
      verb: create
      namespace: dev
EOF

apiVersion: authorization.k8s.io/v1
kind: SelfSubjectAccessReview
metadata:
  creationTimestamp: null
spec:
  resourceAttributes:
    group: apps
    resource: deployments
    namespace: dev
    verb: create
status:
  allowed: true
  denied: false
```

Using Flags for Your Authorization Module

You must include a flag in your policy to indicate which authorization module your policies include:

The following flags can be used:

- `--authorization-mode=ABAC` Attribute-Based Access Control (ABAC) mode allows you to configure policies using local files.
- `--authorization-mode=RBAC` Role-based access control (RBAC) mode allows you to create and store policies using the Kubernetes API.
- `--authorization-mode=Webhook` WebHook is an HTTP callback mode that allows you to manage authorization using a remote REST endpoint.
- `--authorization-mode=Node` Node authorization is a special-purpose authorization mode that specifically authorizes API requests made by kubelets.
- `--authorization-mode=AlwaysDeny` This flag blocks all requests. Use this flag only for testing.
- `--authorization-mode=AlwaysAllow` This flag allows all requests. Use this flag only if you do not require authorization for your API requests.

You can choose more than one authorization module. Modules are checked in order so an earlier module has higher priority to allow or deny a request.

Privilege escalation via pod creation

Users who have the ability to create pods in a namespace can potentially escalate their privileges within that namespace. They can create pods that access their privileges within that namespace. They can create pods that access secrets the user cannot themselves read, or that run under a service account with different/greater permissions.

> **Caution:** System administrators, use care when granting access to pod creation. A user granted permission to create pods (or controllers that create pods) in the namespace can: read all secrets in the namespace; read all config maps in the namespace; and impersonate any service account in the namespace and take any action the account could take. This applies regardless of authorization mode.

What's next

- To learn more about Authentication, see **Authentication** in Controlling Access to the Kubernetes API.
- To learn more about Admission Control, see Using Admission Controllers.

Edit This Page

Using RBAC Authorization

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.

- API Overview
- Default Roles and Role Bindings
- Privilege Escalation Prevention and Bootstrapping
- Command-line Utilities
- Service Account Permissions
- Upgrading from 1.5
- Permissive RBAC Permissions

`RBAC` uses the `rbac.authorization.k8s.io` API group to drive authorization decisions, allowing admins to dynamically configure policies through the Kubernetes API.

As of 1.8, RBAC mode is stable and backed by the rbac.authorization.k8s.io/v1 API.

To enable RBAC, start the apiserver with `--authorization-mode=RBAC`.

API Overview

The RBAC API declares four top-level types which will be covered in this section. Users can interact with these resources as they would with any other API resource (via `kubectl`, API calls, etc.). For instance, `kubectl create -f (resource).yml` can be used with any of these examples, though readers who wish to follow along should review the section on bootstrapping first.

Role and ClusterRole

In the RBAC API, a role contains rules that represent a set of permissions. Permissions are purely additive (there are no "deny" rules). A role can be defined within a namespace with a `Role`, or cluster-wide with a `ClusterRole`.

A `Role` can only be used to grant access to resources within a single namespace. Here's an example `Role` in the "default" namespace that can be used to grant read access to pods:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups: [""] # "" indicates the core API group
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```

A `ClusterRole` can be used to grant the same permissions as a `Role`, but because they are cluster-scoped, they can also be used to grant access to:

- cluster-scoped resources (like nodes)
- non-resource endpoints (like "/healthz")
- namespaced resources (like pods) across all namespaces (needed to run `kubectl get pods --all-namespaces`, for example)

The following `ClusterRole` can be used to grant read access to secrets in any particular namespace, or across all namespaces (depending on how it is bound):

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  # "namespace" omitted since ClusterRoles are not namespaced
  name: secret-reader
rules:
- apiGroups: [""]
  resources: ["secrets"]
  verbs: ["get", "watch", "list"]
```

RoleBinding and ClusterRoleBinding

A role binding grants the permissions defined in a role to a user or set of users. It holds a list of subjects (users, groups, or service accounts), and a reference to the role being granted. Permissions can be granted within a namespace with a `RoleBinding`, or cluster-wide with a `ClusterRoleBinding`.

A `RoleBinding` may reference a `Role` in the same namespace. The following `RoleBinding` grants the "pod-reader" role to the user "jane" within the "default" namespace. This allows "jane" to read pods in the "default" namespace.

`roleRef` is how you will actually create the binding. The `kind` will be either `Role` or `ClusterRole`, and the `name` will reference the name of the specific `Role` or `ClusterRole` you want. In the example below, this RoleBinding is using `roleRef` to bind the user "jane" to the `Role` created above named `pod-reader`.

```
# This role binding allows "jane" to read pods in the "default" namespace.
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-pods
  namespace: default
subjects:
- kind: User
  name: jane # Name is case sensitive
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role #this must be Role or ClusterRole
  name: pod-reader # this must match the name of the Role or ClusterRole you wish to bind to
  apiGroup: rbac.authorization.k8s.io
```

A `RoleBinding` may also reference a `ClusterRole` to grant the permissions to namespaced resources defined in the `ClusterRole` within the `RoleBinding`'s namespace. This allows administrators to define a set of common roles for the entire cluster, then reuse them within multiple namespaces.

For instance, even though the following `RoleBinding` refers to a `ClusterRole`, "dave" (the subject, case sensitive) will only be able to read secrets in the "development" namespace (the namespace of the `RoleBinding`).

```
# This role binding allows "dave" to read secrets in the "development" namespace.
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-secrets
  namespace: development # This only grants permissions within the "development" namespace.
subjects:
- kind: User
```

```
  name: dave # Name is case sensitive
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: secret-reader
  apiGroup: rbac.authorization.k8s.io
```

Finally, a `ClusterRoleBinding` may be used to grant permission at the cluster
level and in all namespaces. The following `ClusterRoleBinding` allows any user
in the group "manager" to read secrets in any namespace.

```
# This cluster role binding allows anyone in the "manager" group to read secrets in any name
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: read-secrets-global
subjects:
- kind: Group
  name: manager # Name is case sensitive
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: secret-reader
  apiGroup: rbac.authorization.k8s.io
```

Referring to Resources

Most resources are represented by a string representation of their name, such as
"pods", just as it appears in the URL for the relevant API endpoint. However,
some Kubernetes APIs involve a "subresource", such as the logs for a pod. The
URL for the pods logs endpoint is:

```
GET /api/v1/namespaces/{namespace}/pods/{name}/log
```

In this case, "pods" is the namespaced resource, and "log" is a subresource of
pods. To represent this in an RBAC role, use a slash to delimit the resource
and subresource. To allow a subject to read both pods and pod logs, you would
write:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: pod-and-pod-logs-reader
rules:
- apiGroups: [""]
  resources: ["pods", "pods/log"]
```

```
    verbs: ["get", "list"]
```

Resources can also be referred to by name for certain requests through the
`resourceNames` list. When specified, requests using the "get", "delete", "up-
date", and "patch" verbs can be restricted to individual instances of a resource.
To restrict a subject to only "get" and "update" a single configmap, you would
write:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: configmap-updater
rules:
- apiGroups: [""]
  resources: ["configmaps"]
  resourceNames: ["my-configmap"]
  verbs: ["update", "get"]
```

Notably, if `resourceNames` are set, then the verb must not be list, watch, create,
or deletecollection. Because resource names are not present in the URL for
create, list, watch, and deletecollection API requests, those verbs would not be
allowed by a rule with `resourceNames` set, since the `resourceNames` portion of
the rule would not match the request.

Aggregated ClusterRoles

As of 1.9, ClusterRoles can be created by combining other ClusterRoles using an
`aggregationRule`. The permissions of aggregated ClusterRoles are controller-
managed, and filled in by unioning the rules of any ClusterRole that matches
the provided label selector. An example aggregated ClusterRole:

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: monitoring
aggregationRule:
  clusterRoleSelectors:
  - matchLabels:
      rbac.example.com/aggregate-to-monitoring: "true"
rules: [] # Rules are automatically filled in by the controller manager.
```

Creating a ClusterRole that matches the label selector will add rules to
the aggregated ClusterRole. In this case rules can be added to the "mon-
itoring" ClusterRole by creating another ClusterRole that has the label
`rbac.example.com/aggregate-to-monitoring: true`.

```
kind: ClusterRole
```

```
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: monitoring-endpoints
  labels:
    rbac.example.com/aggregate-to-monitoring: "true"
# These rules will be added to the "monitoring" role.
rules:
- apiGroups: [""]
  resources: ["services", "endpoints", "pods"]
  verbs: ["get", "list", "watch"]
```

The default user-facing roles (described below) use ClusterRole aggregation. This lets admins include rules for custom resources, such as those served by CustomResourceDefinitions or Aggregated API servers, on the default roles.

For example, the following ClusterRoles let the "admin" and "edit" default roles manage the custom resource "CronTabs" and the "view" role perform read-only actions on the resource.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: aggregate-cron-tabs-edit
  labels:
    # Add these permissions to the "admin" and "edit" default roles.
    rbac.authorization.k8s.io/aggregate-to-admin: "true"
    rbac.authorization.k8s.io/aggregate-to-edit: "true"
rules:
- apiGroups: ["stable.example.com"]
  resources: ["crontabs"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
---
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: aggregate-cron-tabs-view
  labels:
    # Add these permissions to the "view" default role.
    rbac.authorization.k8s.io/aggregate-to-view: "true"
rules:
- apiGroups: ["stable.example.com"]
  resources: ["crontabs"]
  verbs: ["get", "list", "watch"]
```

Role Examples

Only the `rules` section is shown in the following examples.

Allow reading the resource "pods" in the core API group:

```
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
```

Allow reading/writing "deployments" in both the "extensions" and "apps" API groups:

```
rules:
- apiGroups: ["extensions", "apps"]
  resources: ["deployments"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
```

Allow reading "pods" and reading/writing "jobs":

```
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["batch", "extensions"]
  resources: ["jobs"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
```

Allow reading a `ConfigMap` named "my-config" (must be bound with a `RoleBinding` to limit to a single `ConfigMap` in a single namespace):

```
rules:
- apiGroups: [""]
  resources: ["configmaps"]
  resourceNames: ["my-config"]
  verbs: ["get"]
```

Allow reading the resource "nodes" in the core group (because a `Node` is cluster-scoped, this must be in a `ClusterRole` bound with a `ClusterRoleBinding` to be effective):

```
rules:
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["get", "list", "watch"]
```

Allow "GET" and "POST" requests to the non-resource endpoint "/healthz" and all subpaths (must be in a `ClusterRole` bound with a `ClusterRoleBinding` to be effective):

```
rules:
- nonResourceURLs: ["/healthz", "/healthz/*"] # '*' in a nonResourceURL is a suffix glob mat
  verbs: ["get", "post"]
```

Referring to Subjects

A `RoleBinding` or `ClusterRoleBinding` binds a role to *subjects*. Subjects can be groups, users or service accounts.

Users are represented by strings. These can be plain usernames, like "alice", email-style names, like "bob@example.com", or numeric IDs represented as a string. It is up to the Kubernetes admin to configure the authentication modules to produce usernames in the desired format. The RBAC authorization system does not require any particular format. However, the prefix `system:` is reserved for Kubernetes system use, and so the admin should ensure usernames do not contain this prefix by accident.

Group information in Kubernetes is currently provided by the Authenticator modules. Groups, like users, are represented as strings, and that string has no format requirements, other than that the prefix `system:` is reserved.

Service Accounts have usernames with the `system:serviceaccount:` prefix and belong to groups with the `system:serviceaccounts:` prefix.

Role Binding Examples

Only the `subjects` section of a `RoleBinding` is shown in the following examples.

For a user named "alice@example.com":

```
subjects:
- kind: User
  name: "alice@example.com"
  apiGroup: rbac.authorization.k8s.io
```

For a group named "frontend-admins":

```
subjects:
- kind: Group
  name: "frontend-admins"
  apiGroup: rbac.authorization.k8s.io
```

For the default service account in the kube-system namespace:

```
subjects:
- kind: ServiceAccount
  name: default
  namespace: kube-system
```

For all service accounts in the "qa" namespace:

```
subjects:
- kind: Group
  name: system:serviceaccounts:qa
  apiGroup: rbac.authorization.k8s.io
```

For all service accounts everywhere:

```
subjects:
- kind: Group
  name: system:serviceaccounts
  apiGroup: rbac.authorization.k8s.io
```

For all authenticated users (version 1.5+):

```
subjects:
- kind: Group
  name: system:authenticated
  apiGroup: rbac.authorization.k8s.io
```

For all unauthenticated users (version 1.5+):

```
subjects:
- kind: Group
  name: system:unauthenticated
  apiGroup: rbac.authorization.k8s.io
```

For all users (version 1.5+):

```
subjects:
- kind: Group
  name: system:authenticated
  apiGroup: rbac.authorization.k8s.io
- kind: Group
  name: system:unauthenticated
  apiGroup: rbac.authorization.k8s.io
```

Default Roles and Role Bindings

API servers create a set of default `ClusterRole` and `ClusterRoleBinding` objects. Many of these are `system:` prefixed, which indicates that the resource is "owned" by the infrastructure. Modifications to these resources can result in non-functional clusters. One example is the `system:node` ClusterRole. This role defines permissions for kubelets. If the role is modified, it can prevent kubelets from working.

All of the default cluster roles and rolebindings are labeled with `kubernetes.io/bootstrapping=rbac-default`

Auto-reconciliation

At each start-up, the API server updates default cluster roles with any missing permissions, and updates default cluster role bindings with any missing subjects. This allows the cluster to repair accidental modifications, and to keep roles and rolebindings up-to-date as permissions and subjects change in new releases.

To opt out of this reconciliation, set the `rbac.authorization.kubernetes.io/autoupdate` annotation on a default cluster role or rolebinding to `false`. Be aware that missing default permissions and subjects can result in non-functional clusters.

Auto-reconciliation is enabled in Kubernetes version 1.6+ when the RBAC authorizer is active.

Discovery Roles

Default role bindings authorize unauthenticated and authenticated users to read API information that is deemed safe to be publicly accessible (including CustomResourceDefinitions). To disable anonymous unauthenticated access add `--anonymous-auth=false` to the API server configuration.

To view the configuration of these roles via `kubectl` run:

```
kubectl get clusterroles system:discovery -o yaml
```

NOTE: editing the role is not recommended as changes will be overwritten on API server restart via auto-reconciliation (see above).

Default ClusterRole	Default ClusterRoleBinding	Description
system:basic-user	**system:authenticated** and **system:unauthenticated** groups	Allows a user read-only access to basic information about themselve
system:discovery	**system:authenticated** and **system:unauthenticated** groups	Allows read-only access to API discovery endpoints needed to discov

User-facing Roles

Some of the default roles are not `system:` prefixed. These are intended to be user-facing roles. They include super-user roles (`cluster-admin`), roles intended to be granted cluster-wide using ClusterRoleBindings (`cluster-status`), and roles intended to be granted within particular namespaces using RoleBindings (`admin`, `edit`, `view`).

As of 1.9, user-facing roles use ClusterRole Aggregation to allow admins to include rules for custom resources on these roles. To add rules to the "admin", "edit", or "view" role, create a ClusterRole with one or more of the following labels:

```
metadata:
```

```
labels:
  rbac.authorization.k8s.io/aggregate-to-admin: "true"
  rbac.authorization.k8s.io/aggregate-to-edit: "true"
  rbac.authorization.k8s.io/aggregate-to-view: "true"
```

Default ClusterRole	Default ClusterRoleBinding	Description
cluster-admin	**system:masters** group	Allows super-user access to perform any action on any resource. Wh
admin	None	Allows admin access, intended to be granted within a namespace us
edit	None	Allows read/write access to most objects in a namespace. It does no
view	None	Allows read-only access to see most objects in a namespace. It does

Core Component Roles

Default ClusterRole	Default ClusterRoleBinding	Description
system:kube-scheduler	**system:kube-scheduler** user	Allows access to the resources required by the kube-scheduler comp
system:volume-scheduler	**system:kube-scheduler** user	Allows access to the volume resources required by the kube-schedule
system:kube-controller-manager	**system:kube-controller-manager** user	Allows access to the resources required by the kube-controller-mana
system:node	None in 1.8+	Allows access to resources required by the kubelet component, **inclu**
system:node-proxier	**system:kube-proxy** user	Allows access to the resources required by the kube-proxy componen

Other Component Roles

Default ClusterRole	Default ClusterRoleBinding	Description
system:auth-delegator	None	Allows delegated authentication and authorization checks. This is c
system:heapster	None	Role for the Heapster component.
system:kube-aggregator	None	Role for the kube-aggregator component.

Default ClusterRole	Default ClusterRoleBinding	Description
system:kube-dns	**kube-dns** service account in the **kube-system** namespace	Role for the kube-dns component.
system:kubelet-api-admin	None	Allows full access to the kubelet API.
system:node-bootstrapper	None	Allows access to the resources required to perform Kubelet TLS boo
system:node-problem-detector	None	Role for the node-problem-detector component.
system:persistent-volume-provisioner	None	Allows access to the resources required by most dynamic volume pr

Controller Roles

The Kubernetes controller manager runs core control loops. When invoked with `--use-service-account-credentials`, each control loop is started using a separate service account. Corresponding roles exist for each control loop, prefixed with `system:controller:`. If the controller manager is not started with `--use-service-account-credentials`, it runs all control loops using its own credential, which must be granted all the relevant roles. These roles include:

- system:controller:attachdetach-controller
- system:controller:certificate-controller
- system:controller:cronjob-controller
- system:controller:daemon-set-controller
- system:controller:deployment-controller
- system:controller:disruption-controller
- system:controller:endpoint-controller
- system:controller:generic-garbage-collector
- system:controller:horizontal-pod-autoscaler
- system:controller:job-controller
- system:controller:namespace-controller
- system:controller:node-controller
- system:controller:persistent-volume-binder
- system:controller:pod-garbage-collector
- system:controller:pv-protection-controller
- system:controller:pvc-protection-controller
- system:controller:replicaset-controller
- system:controller:replication-controller
- system:controller:resourcequota-controller

137

- system:controller:route-controller
- system:controller:service-account-controller
- system:controller:service-controller
- system:controller:statefulset-controller
- system:controller:ttl-controller

Privilege Escalation Prevention and Bootstrapping

The RBAC API prevents users from escalating privileges by editing roles or role bindings. Because this is enforced at the API level, it applies even when the RBAC authorizer is not in use.

A user can only create/update a role if at least one of the following things is true:

1. they already have all the permissions contained in the role, at the same scope as the object being modified (cluster-wide for a `ClusterRole`, within the same namespace or cluster-wide for a `Role`)
2. they are given explicit permission to perform the `escalate` verb on the `roles` or `clusterroles` resource in the `rbac.authorization.k8s.io` API group (Kubernetes 1.12 and newer)

For example, if "user-1" does not have the ability to list secrets cluster-wide, they cannot create a `ClusterRole` containing that permission. To allow a user to create/update roles:

1. Grant them a role that allows them to create/update `Role` or `ClusterRole` objects, as desired.
2. Grant them permission to include specific permissions in the roles the create/update:
   - implicitly, by giving them those permissions (if they attempt to create or modify a `Role` or `ClusterRole` with permissions they themselves have not been granted, the API request will be forbidden)
   - or explicitly allow specifying any permission in a `Role` or `ClusterRole` by giving them permission to perform the `escalate` verb on `roles` or `clusterroles` resources in the `rbac.authorization.k8s.io` API group (Kubernetes 1.12 and newer)

A user can only create/update a role binding if they already have all the permissions contained in the referenced role (at the same scope as the role binding) *or* if they've been given explicit permission to perform the `bind` verb on the referenced role. For example, if "user-1" does not have the ability to list secrets cluster-wide, they cannot create a `ClusterRoleBinding` to a role that grants that permission. To allow a user to create/update role bindings:

1. Grant them a role that allows them to create/update `RoleBinding` or `ClusterRoleBinding` objects, as desired.
2. Grant them permissions needed to bind a particular role:

- implicitly, by giving them the permissions contained in the role.
- explicitly, by giving them permission to perform the `bind` verb on the particular role (or cluster role).

For example, this cluster role and role binding would allow "user-1" to grant other users the `admin`, `edit`, and `view` roles in the "user-1-namespace" namespace:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: role-grantor
rules:
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["rolebindings"]
  verbs: ["create"]
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["clusterroles"]
  verbs: ["bind"]
  resourceNames: ["admin","edit","view"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: role-grantor-binding
  namespace: user-1-namespace
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: role-grantor
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: user-1
```

When bootstrapping the first roles and role bindings, it is necessary for the initial user to grant permissions they do not yet have. To bootstrap initial roles and role bindings:

- Use a credential with the `system:masters` group, which is bound to the `cluster-admin` super-user role by the default bindings.
- If your API server runs with the insecure port enabled (`--insecure-port`), you can also make API calls via that port, which does not enforce authentication or authorization.

Command-line Utilities

Two `kubectl` commands exist to grant roles within a namespace or across the entire cluster.

`kubectl create rolebinding`

Grants a `Role` or `ClusterRole` within a specific namespace. Examples:

- Grant the `admin ClusterRole` to a user named "bob" in the namespace "acme":

  `kubectl create rolebinding bob-admin-binding --clusterrole=admin --user=bob --namespace`

- Grant the `view ClusterRole` to a service account named "myapp" in the namespace "acme":

  `kubectl create rolebinding myapp-view-binding --clusterrole=view --serviceaccount=acme:`

`kubectl create clusterrolebinding`

Grants a `ClusterRole` across the entire cluster, including all namespaces. Examples:

- Grant the `cluster-admin ClusterRole` to a user named "root" across the entire cluster:

  `kubectl create clusterrolebinding root-cluster-admin-binding --clusterrole=cluster-admi`

- Grant the `system:node ClusterRole` to a user named "kubelet" across the entire cluster:

  `kubectl create clusterrolebinding kubelet-node-binding --clusterrole=system:node --user`

- Grant the `view ClusterRole` to a service account named "myapp" in the namespace "acme" across the entire cluster:

  `kubectl create clusterrolebinding myapp-view-binding --clusterrole=view --serviceaccoun`

See the CLI help for detailed usage.

Service Account Permissions

Default RBAC policies grant scoped permissions to control-plane components, nodes, and controllers, but grant *no permissions* to service accounts outside the `kube-system` namespace (beyond discovery permissions given to all authenticated users).

This allows you to grant particular roles to particular service accounts as needed. Fine-grained role bindings provide greater security, but require more effort to administrate. Broader grants can give unnecessary (and potentially escalating) API access to service accounts, but are easier to administrate.

In order from most secure to least secure, the approaches are:

1. Grant a role to an application-specific service account (best practice)

   This requires the application to specify a `serviceAccountName` in its pod spec, and for the service account to be created (via the API, application manifest, `kubectl create serviceaccount`, etc.).

   For example, grant read-only permission within "my-namespace" to the "my-sa" service account:

   ```
   kubectl create rolebinding my-sa-view \
     --clusterrole=view \
     --serviceaccount=my-namespace:my-sa \
     --namespace=my-namespace
   ```

2. Grant a role to the "default" service account in a namespace

   If an application does not specify a `serviceAccountName`, it uses the "default" service account.

   > **Note:** Permissions given to the "default" service account are available to any pod in the namespace that does not specify a `serviceAccountName`.

   For example, grant read-only permission within "my-namespace" to the "default" service account:

   ```
   kubectl create rolebinding default-view \
     --clusterrole=view \
     --serviceaccount=my-namespace:default \
     --namespace=my-namespace
   ```

   Many add-ons currently run as the "default" service account in the `kube-system` namespace. To allow those add-ons to run with super-user access, grant cluster-admin permissions to the "default" service account in the `kube-system` namespace.

   > **Note:** Enabling this means the `kube-system` namespace contains secrets that grant super-user access to the API.

   ```
   kubectl create clusterrolebinding add-on-cluster-admin \
     --clusterrole=cluster-admin \
     --serviceaccount=kube-system:default
   ```

3. Grant a role to all service accounts in a namespace

If you want all applications in a namespace to have a role, no matter what service account they use, you can grant a role to the service account group for that namespace.

For example, grant read-only permission within "my-namespace" to all service accounts in that namespace:

```
kubectl create rolebinding serviceaccounts-view \
  --clusterrole=view \
  --group=system:serviceaccounts:my-namespace \
  --namespace=my-namespace
```

4. Grant a limited role to all service accounts cluster-wide (discouraged)

If you don't want to manage permissions per-namespace, you can grant a cluster-wide role to all service accounts.

For example, grant read-only permission across all namespaces to all service accounts in the cluster:

```
kubectl create clusterrolebinding serviceaccounts-view \
  --clusterrole=view \
 --group=system:serviceaccounts
```

5. Grant super-user access to all service accounts cluster-wide (strongly discouraged)

If you don't care about partitioning permissions at all, you can grant super-user access to all service accounts.

Warning:

```
This allows any user with read access
to secrets or the ability to create a pod to access super-user
credentials.
```

```
kubectl create clusterrolebinding serviceaccounts-cluster-admin \
  --clusterrole=cluster-admin \
  --group=system:serviceaccounts
```

Upgrading from 1.5

Prior to Kubernetes 1.6, many deployments used very permissive ABAC policies, including granting full API access to all service accounts.

Default RBAC policies grant scoped permissions to control-plane components, nodes, and controllers, but grant *no permissions* to service accounts outside the `kube-system` namespace (beyond discovery permissions given to all authenticated users).

While far more secure, this can be disruptive to existing workloads expecting to automatically receive API permissions. Here are two approaches for managing this transition:

Parallel Authorizers

Run both the RBAC and ABAC authorizers, and specify a policy file that contains the legacy ABAC policy:

```
--authorization-mode=RBAC,ABAC --authorization-policy-file=mypolicy.json
```

The RBAC authorizer will attempt to authorize requests first. If it denies an API request, the ABAC authorizer is then run. This means that any request allowed by *either* the RBAC or ABAC policies is allowed.

When the apiserver is run with a log level of 5 or higher for the RBAC component (`--vmodule=rbac*=5` or `--v=5`), you can see RBAC denials in the apiserver log (prefixed with `RBAC DENY:`). You can use that information to determine which roles need to be granted to which users, groups, or service accounts. Once you have granted roles to service accounts and workloads are running with no RBAC denial messages in the server logs, you can remove the ABAC authorizer.

Permissive RBAC Permissions

You can replicate a permissive policy using RBAC role bindings.

> **Warning:**
>
> The following policy allows **ALL** service accounts to act as cluster administrators. Any application running in a container receives service account credentials automatically, and could perform any action against the API, including viewing secrets and modifying permissions. This is not a recommended policy.
>
> ```
> kubectl create clusterrolebinding permissive-binding \
>   --clusterrole=cluster-admin \
>   --user=admin \
>   --user=kubelet \
>   --group=system:serviceaccounts
> ```

Edit This Page

Using ABAC Authorization

Attribute-based access control (ABAC) defines an access control paradigm whereby access rights are granted to users through the use of policies which

combine attributes together.

- Policy File Format
- Authorization Algorithm
- Kubectl
- Examples
- A quick note on service accounts

Policy File Format

To enable `ABAC` mode, specify `--authorization-policy-file=SOME_FILENAME` and `--authorization-mode=ABAC` on startup.

The file format is one JSON object per line. There should be no enclosing list or map, just one map per line.

Each line is a "policy object", where each such object is a map with the following properties:

- Versioning properties:
  - `apiVersion`, type string; valid values are "abac.authorization.kubernetes.io/v1beta1". Allows versioning and conversion of the policy format.
  - `kind`, type string: valid values are "Policy". Allows versioning and conversion of the policy format.
- `spec` property set to a map with the following properties:
  - Subject-matching properties:
    * `user`, type string; the user-string from `--token-auth-file`. If you specify `user`, it must match the username of the authenticated user.
    * `group`, type string; if you specify `group`, it must match one of the groups of the authenticated user. `system:authenticated` matches all authenticated requests. `system:unauthenticated` matches all unauthenticated requests.
  - Resource-matching properties:
    * `apiGroup`, type string; an API group.
    * Ex: `extensions`
    * Wildcard: `*` matches all API groups.
    * `namespace`, type string; a namespace.
    * Ex: `kube-system`
    * Wildcard: `*` matches all resource requests.
    * `resource`, type string; a resource type
    * Ex: `pods`
    * Wildcard: `*` matches all resource requests.
  - Non-resource-matching properties:
    * `nonResourcePath`, type string; non-resource request paths.
    * Ex: `/version` or `/apis`
    * Wildcard:

144

· `*` matches all non-resource requests.
· `/foo/*` matches all subpaths of `/foo/`.
  - `readonly`, type boolean, when true, means that the Resource-matching policy only applies to get, list, and watch operations, Non-resource-matching policy only applies to get operation.

Note:

An unset property is the same as a property set to the zero value for its type (e.g. empty string, 0, false). However, unset should be preferred for readability.

In the future, policies may be expressed in a JSON format, and managed via a REST interface.

Authorization Algorithm

A request has attributes which correspond to the properties of a policy object.

When a request is received, the attributes are determined. Unknown attributes are set to the zero value of its type (e.g. empty string, 0, false).

A property set to `"*"` will match any value of the corresponding attribute.

The tuple of attributes is checked for a match against every policy in the policy file. If at least one line matches the request attributes, then the request is authorized (but may fail later validation).

To permit any authenticated user to do something, write a policy with the group property set to `"system:authenticated"`.

To permit any unauthenticated user to do something, write a policy with the group property set to `"system:unauthenticated"`.

To permit a user to do anything, write a policy with the apiGroup, namespace, resource, and nonResourcePath properties set to `"*"`.

Kubectl

Kubectl uses the `/api` and `/apis` endpoints of api-server to negotiate client/server versions. To validate objects sent to the API by create/update operations, kubectl queries certain swagger resources. For API version `v1` those would be `/swaggerapi/api/v1` & `/swaggerapi/experimental/v1`.

When using ABAC authorization, those special resources have to be explicitly exposed via the `nonResourcePath` property in a policy (see examples below):

- `/api`, `/api/*`, `/apis`, and `/apis/*` for API version negotiation.
- `/version` for retrieving the server version via `kubectl version`.

- `/swaggerapi/*` for create/update operations.

To inspect the HTTP calls involved in a specific kubectl operation you can turn up the verbosity:

```
kubectl --v=8 version
```

Examples

1. Alice can do anything to all resources:

   {"apiVersion": "abac.authorization.kubernetes.io/v1beta1", "kind": "Policy", "spec": {"

2. The Kubelet can read any pods:

   {"apiVersion": "abac.authorization.kubernetes.io/v1beta1", "kind": "Policy", "spec": {"

3. The Kubelet can read and write events:

   {"apiVersion": "abac.authorization.kubernetes.io/v1beta1", "kind": "Policy", "spec": {"

4. Bob can just read pods in namespace "projectCaribou":

   {"apiVersion": "abac.authorization.kubernetes.io/v1beta1", "kind": "Policy", "spec": {"

5. Anyone can make read-only requests to all non-resource paths:

   {"apiVersion": "abac.authorization.kubernetes.io/v1beta1", "kind": "Policy", "spec": {"
   {"apiVersion": "abac.authorization.kubernetes.io/v1beta1", "kind": "Policy", "spec": {"

Complete file example

A quick note on service accounts

Every service account has a corresponding ABAC username, and that service account's user name is generated according to the naming convention:

```
system:serviceaccount:<namespace>:<serviceaccountname>
```

Creating a new namespace leads to the creation of a new service account in the following format:

```
system:serviceaccount:<namespace>:default
```

For example, if you wanted to grant the default service account (in the `kube-system` namespace) full privilege to the API using ABAC, you would add this line to your policy file:

{"apiVersion":"abac.authorization.kubernetes.io/v1beta1","kind":"Policy","spec":{"user":"sys

The apiserver will need to be restarted to pickup the new policy lines.

Edit This Page

Using Node Authorization

Node authorization is a special-purpose authorization mode that specifically authorizes API requests made by kubelets.

- Overview
- Migration considerations

Overview

The Node authorizer allows a kubelet to perform API operations. This includes:

Read operations:

- services
- endpoints
- nodes
- pods
- secrets, configmaps, persistent volume claims and persistent volumes related to pods bound to the kubelet's node

Write operations:

- nodes and node status (enable the `NodeRestriction` admission plugin to limit a kubelet to modify its own node)
- pods and pod status (enable the `NodeRestriction` admission plugin to limit a kubelet to modify pods bound to itself)
- events

Auth-related operations:

- read/write access to the certificationsigningrequests API for TLS bootstrapping
- the ability to create tokenreviews and subjectaccessreviews for delegated authentication/authorization checks

In future releases, the node authorizer may add or remove permissions to ensure kubelets have the minimal set of permissions required to operate correctly.

In order to be authorized by the Node authorizer, kubelets must use a credential that identifies them as being in the `system:nodes` group, with a username of `system:node:<nodeName>`. This group and user name format match the identity created for each kubelet as part of kubelet TLS bootstrapping.

To enable the Node authorizer, start the apiserver with `--authorization-mode=Node`.

To limit the API objects kubelets are able to write, enable the NodeRestriction admission plugin by starting the apiserver with `--enable-admission-plugins=...,NodeRestriction,...`

Migration considerations

Kubelets outside the `system:nodes` group

Kubelets outside the `system:nodes` group would not be authorized by the `Node` authorization mode, and would need to continue to be authorized via whatever mechanism currently authorizes them. The node admission plugin would not restrict requests from these kubelets.

Kubelets with undifferentiated usernames

In some deployments, kubelets have credentials that place them in the `system:nodes` group, but do not identify the particular node they are associated with, because they do not have a username in the `system:node:...` format. These kubelets would not be authorized by the `Node` authorization mode, and would need to continue to be authorized via whatever mechanism currently authorizes them.

The `NodeRestriction` admission plugin would ignore requests from these kubelets, since the default node identifier implementation would not consider that a node identity.

Upgrades from previous versions using RBAC

Upgraded pre-1.7 clusters using RBAC will continue functioning as-is because the `system:nodes` group binding will already exist.

If a cluster admin wishes to start using the `Node` authorizer and `NodeRestriction` admission plugin to limit node access to the API, that can be done non-disruptively:

1. Enable the `Node` authorization mode (`--authorization-mode=Node,RBAC`) and the `NodeRestriction` admission plugin
2. Ensure all kubelets' credentials conform to the group/username requirements
3. Audit apiserver logs to ensure the `Node` authorizer is not rejecting requests from kubelets (no persistent `NODE DENY` messages logged)
4. Delete the `system:node` cluster role binding

RBAC Node Permissions

In 1.6, the `system:node` cluster role was automatically bound to the `system:nodes` group when using the RBAC Authorization mode.

In 1.7, the automatic binding of the `system:nodes` group to the `system:node` role is deprecated because the node authorizer accomplishes the same purpose with the benefit of additional restrictions on secret and configmap access. If the `Node` and `RBAC` authorization modes are both enabled, the automatic binding of the `system:nodes` group to the `system:node` role is not created in 1.7.

In 1.8, the binding will not be created at all.

When using RBAC, the `system:node` cluster role will continue to be created, for compatibility with deployment methods that bind other users or groups to that role.

Edit This Page

Webhook Mode

A WebHook is an HTTP callback: an HTTP POST that occurs when something happens; a simple event-notification via HTTP POST. A web application implementing WebHooks will POST a message to a URL when certain things happen.

- Configuration File Format
- Request Payloads

When specified, mode `Webhook` causes Kubernetes to query an outside REST service when determining user privileges.

Configuration File Format

Mode `Webhook` requires a file for HTTP configuration, specify by the `--authorization-webhook-config-file=SOME_FILENAME` flag.

The configuration file uses the kubeconfig file format. Within the file "users" refers to the API Server webhook and "clusters" refers to the remote service.

A configuration example which uses HTTPS client auth:

```
# Kubernetes API version
apiVersion: v1
# kind of the API object
kind: Config
# clusters refers to the remote service.
clusters:
  - name: name-of-remote-authz-service
    cluster:
      # CA for verifying the remote service.
      certificate-authority: /path/to/ca.pem
```

```
        # URL of remote service to query. Must use 'https'. May not include parameters.
        server: https://authz.example.com/authorize

# users refers to the API Server's webhook configuration.
users:
  - name: name-of-api-server
    user:
      client-certificate: /path/to/cert.pem # cert for the webhook plugin to use
      client-key: /path/to/key.pem           # key matching the cert

# kubeconfig files require a context. Provide one for the API Server.
current-context: webhook
contexts:
- context:
    cluster: name-of-remote-authz-service
    user: name-of-api-server
  name: webhook
```

Request Payloads

When faced with an authorization decision, the API Server POSTs a JSON- seri-
alized `authorization.k8s.io/v1beta1 SubjectAccessReview` object describ-
ing the action. This object contains fields describing the user attempting to
make the request, and either details about the resource being accessed or re-
quests attributes.

Note that webhook API objects are subject to the same versioning compati-
bility rules as other Kubernetes API objects. Implementers should be aware
of looser compatibility promises for beta objects and check the "apiVersion"
field of the request to ensure correct deserialization. Additionally, the API
Server must enable the `authorization.k8s.io/v1beta1` API extensions group
(`--runtime-config=authorization.k8s.io/v1beta1=true`).

An example request body:

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "spec": {
    "resourceAttributes": {
      "namespace": "kittensandponies",
      "verb": "get",
      "group": "unicorn.example.org",
      "resource": "pods"
    },
    "user": "jane",
```

```
    "group": [
      "group1",
      "group2"
    ]
  }
}
```

The remote service is expected to fill the `status` field of the request and respond to either allow or disallow access. The response body's `spec` field is ignored and may be omitted. A permissive response would return:

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "status": {
    "allowed": true
  }
}
```

To disallow access, the remote service would return:

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "status": {
    "allowed": false,
    "reason": "user does not have read access to the namespace"
  }
}
```

Access to non-resource paths are sent as:

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "spec": {
    "nonResourceAttributes": {
      "path": "/debug",
      "verb": "get"
    },
    "user": "jane",
    "group": [
      "group1",
      "group2"
    ]
  }
}
```

Non-resource paths include: `/api`, `/apis`, `/metrics`, `/resetMetrics`, `/logs`,

`/debug`, `/healthz`, `/swagger-ui/`, `/swaggerapi/`, `/ui`, and `/version`. Clients require access to `/api`, `/api/*`, `/apis`, `/apis/*`, and `/version` to discover what resources and versions are present on the server. Access to other non-resource paths can be disallowed without restricting access to the REST api.

For further documentation refer to the authorization.v1beta1 API objects and webhook.go.

Edit This Page

Well-Known Labels, Annotations and Taints

Kubernetes reserves all labels and annotations in the kubernetes.io namespace.

This document serves both as a reference to the values, and as a coordination point for assigning values.

- beta.kubernetes.io/arch
- beta.kubernetes.io/os
- kubernetes.io/hostname
- beta.kubernetes.io/instance-type
- failure-domain.beta.kubernetes.io/region
- failure-domain.beta.kubernetes.io/zone

beta.kubernetes.io/arch

Example: `beta.kubernetes.io/arch=amd64`

Used on: Node

Kubelet populates this with `runtime.GOARCH` as defined by Go. This can be handy if you are mixing arm and x86 nodes, for example.

beta.kubernetes.io/os

Example: `beta.kubernetes.io/os=linux`

Used on: Node

Kubelet populates this with `runtime.GOOS` as defined by Go. This can be handy if you are mixing operating systems in your cluster (although currently Linux is the only OS supported by Kubernetes).

kubernetes.io/hostname

Example: `kubernetes.io/hostname=ip-172-20-114-199.ec2.internal`

Used on: Node

Kubelet populates this with the hostname. Note that the hostname can be changed from the "actual" hostname by passing the `--hostname-override` flag to kubelet.

beta.kubernetes.io/instance-type

Example: `beta.kubernetes.io/instance-type=m3.medium`

Used on: Node

Kubelet populates this with the instance type as defined by the `cloudprovider`. It will not be set if not using a cloudprovider. This can be handy if you want to target certain workloads to certain instance types, but typically you want to rely on the Kubernetes scheduler to perform resource-based scheduling, and you should aim to schedule based on properties rather than on instance types (e.g. require a GPU, instead of requiring a `g2.2xlarge`)

failure-domain.beta.kubernetes.io/region

See failure-domain.beta.kubernetes.io/zone.

failure-domain.beta.kubernetes.io/zone

Example:

`failure-domain.beta.kubernetes.io/region=us-east-1`

`failure-domain.beta.kubernetes.io/zone=us-east-1c`

Used on: Node, PersistentVolume

On the Node: Kubelet populates this with the zone information as defined by the `cloudprovider`. It will not be set if not using a `cloudprovider`, but you should consider setting it on the nodes if it makes sense in your topology.

On the PersistentVolume: The `PersistentVolumeLabel` admission controller will automatically add zone labels to PersistentVolumes, on GCE and AWS.

Kubernetes will automatically spread the pods in a replication controller or service across nodes in a single-zone cluster (to reduce the impact of failures). With multiple-zone clusters, this spreading behaviour is extended across zones

(to reduce the impact of zone failures). This is achieved via SelectorSpreadPriority.

This is a best-effort placement, and so if the zones in your cluster are heterogeneous (e.g. different numbers of nodes, different types of nodes, or different pod resource requirements), this might prevent equal spreading of your pods across zones. If desired, you can use homogenous zones (same number and types of nodes) to reduce the probability of unequal spreading.

The scheduler (via the VolumeZonePredicate predicate) will also ensure that pods that claim a given volume are only placed into the same zone as that volume, as volumes cannot be attached across zones.

The actual values of zone and region don't matter, and nor is the meaning of the hierarchy rigidly defined. The expectation is that failures of nodes in different zones should be uncorrelated unless the entire region has failed. For example, zones should typically avoid sharing a single network switch. The exact mapping depends on your particular infrastructure - a three-rack installation will choose a very different setup to a multi-datacenter configuration.

If `PersistentVolumeLabel` does not support automatic labeling of your PersistentVolumes, you should consider adding the labels manually (or adding support to `PersistentVolumeLabel`), if you want the scheduler to prevent pods from mounting volumes in a different zone. If your infrastructure doesn't have this constraint, you don't need to add the zone labels to the volumes at all.

Edit This Page

Well-Known Labels, Annotations and Taints

Kubernetes reserves all labels and annotations in the kubernetes.io namespace.

This document serves both as a reference to the values, and as a coordination point for assigning values.

- beta.kubernetes.io/arch
- beta.kubernetes.io/os
- kubernetes.io/hostname
- beta.kubernetes.io/instance-type
- failure-domain.beta.kubernetes.io/region
- failure-domain.beta.kubernetes.io/zone

beta.kubernetes.io/arch

Example: `beta.kubernetes.io/arch=amd64`

Used on: Node

Kubelet populates this with `runtime.GOARCH` as defined by Go. This can be handy if you are mixing arm and x86 nodes, for example.

beta.kubernetes.io/os

Example: `beta.kubernetes.io/os=linux`

Used on: Node

Kubelet populates this with `runtime.GOOS` as defined by Go. This can be handy if you are mixing operating systems in your cluster (although currently Linux is the only OS supported by Kubernetes).

kubernetes.io/hostname

Example: `kubernetes.io/hostname=ip-172-20-114-199.ec2.internal`

Used on: Node

Kubelet populates this with the hostname. Note that the hostname can be changed from the "actual" hostname by passing the `--hostname-override` flag to kubelet.

beta.kubernetes.io/instance-type

Example: `beta.kubernetes.io/instance-type=m3.medium`

Used on: Node

Kubelet populates this with the instance type as defined by the `cloudprovider`. It will not be set if not using a cloudprovider. This can be handy if you want to target certain workloads to certain instance types, but typically you want to rely on the Kubernetes scheduler to perform resource-based scheduling, and you should aim to schedule based on properties rather than on instance types (e.g. require a GPU, instead of requiring a `g2.2xlarge`)

failure-domain.beta.kubernetes.io/region

See failure-domain.beta.kubernetes.io/zone.

failure-domain.beta.kubernetes.io/zone

Example:

`failure-domain.beta.kubernetes.io/region=us-east-1`

```
failure-domain.beta.kubernetes.io/zone=us-east-1c
```

Used on: Node, PersistentVolume

On the Node: Kubelet populates this with the zone information as defined by the `cloudprovider`. It will not be set if not using a `cloudprovider`, but you should consider setting it on the nodes if it makes sense in your topology.

On the PersistentVolume: The `PersistentVolumeLabel` admission controller will automatically add zone labels to PersistentVolumes, on GCE and AWS.

Kubernetes will automatically spread the pods in a replication controller or service across nodes in a single-zone cluster (to reduce the impact of failures). With multiple-zone clusters, this spreading behaviour is extended across zones (to reduce the impact of zone failures). This is achieved via SelectorSpreadPriority.

This is a best-effort placement, and so if the zones in your cluster are heterogeneous (e.g. different numbers of nodes, different types of nodes, or different pod resource requirements), this might prevent equal spreading of your pods across zones. If desired, you can use homogenous zones (same number and types of nodes) to reduce the probability of unequal spreading.

The scheduler (via the VolumeZonePredicate predicate) will also ensure that pods that claim a given volume are only placed into the same zone as that volume, as volumes cannot be attached across zones.

The actual values of zone and region don't matter, and nor is the meaning of the hierarchy rigidly defined. The expectation is that failures of nodes in different zones should be uncorrelated unless the entire region has failed. For example, zones should typically avoid sharing a single network switch. The exact mapping depends on your particular infrastructure - a three-rack installation will choose a very different setup to a multi-datacenter configuration.

If `PersistentVolumeLabel` does not support automatic labeling of your PersistentVolumes, you should consider adding the labels manually (or adding support to `PersistentVolumeLabel`), if you want the scheduler to prevent pods from mounting volumes in a different zone. If your infrastructure doesn't have this constraint, you don't need to add the zone labels to the volumes at all.

Edit This Page

v1.12

Kubernetes API v1.12

Edit This Page

Top Level API Objects

Top Level API Objects

- v1.Service
- v1.ServiceList
- v1.Event
- v1.EventList
- v1.Namespace
- v1.NamespaceList
- v1.Secret
- v1.SecretList
- v1.ConfigMap
- v1.ConfigMapList

Definitions

v1.APIResourceList

APIResourceList is a list of APIResource, it is used to expose the name of the resources supported in a specific group and version, and if the resource is namespaced.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
groupVersion	groupVersion is the group and version this APIResourceList is for.	true	string	
resources	resources contains the name of the resources and if they are namespaced.	true	v1.APIResource array	

v1.NamespaceList

NamespaceList is a list of Namespaces.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard list metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
items	Items is the list of Namespace objects in the list. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ namespaces/	true	v1.Namespace array	

v1.ListMeta

ListMeta describes metadata that synthetic resources must have, including lists and various status objects. A resource may have only one of {ObjectMeta, ListMeta}.

Name	Description	Required	Schema	Default
selfLink	selfLink is a URL representing this object. Populated by the system. Read-only.	false	string	

Name	Description	Required	Schema	Default
resourceVersion	String that identifies the server's internal version of this object that can be used by clients to determine when objects have changed. Value must be treated as opaque by clients and passed unmodified back to the server. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# concurrency-control-and-consistency	false	string	

Name	Description	Required	Schema	Default
continue	continue may be set if the user set a limit on the number of items returned, and indicates that the server has more data available. The value is opaque and may be used to issue another request to the endpoint that served this list to retrieve the next set of available objects. Continuing a list may not be possible if the server configuration has changed or more than a few minutes have passed. The resourceVersion field returned when using this continue value will be identical to the value in the first response.	false	string	

Name	Description	Required	Schema	Default

v1.Namespace

Namespace provides a scope for Names. Use of multiple namespaces is optional.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard object's metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	Spec defines the behavior of the Namespace. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1.NamespaceSpec	
status	Status describes the current status of a Namespace. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1.NamespaceStatus	

v1.Initializers

Initializers tracks the progress of initialization.

Name	Description	Required	Schema	Default
pending	Pending is a list of initializers that must execute in order before this object is visible. When the last pending initializer is removed, and no failing result is set, the initializers struct will be set to nil and the object is considered as initialized and visible to all clients.	true	v1.Initializer array	
result	If result is set with the Failure field, the object will be persisted to storage and then deleted, ensuring that other clients can observe the deletion.	false	v1.Status	

v1.Preconditions

Preconditions must be fulfilled before an operation (update, delete, etc.) is carried out.

Name	Description	Required	Schema	Default
uid	Specifies the target UID.	false	types.UID	

v1.Status

Status is a return value for calls that don't return other objects.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
status	Status of the operation. One of: "Success" or "Failure". More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	string	
message	A human-readable description of the status of this operation.	false	string	
reason	A machine-readable description of why this operation is in the "Failure" status. If this value is empty there is no information available. A Reason clarifies an HTTP status code but does not override it.	false	string	

Name	Description	Required	Schema	Default
details	Extended data associated with the reason. Each reason may define its own extended details. This field is optional and the data returned is not guaranteed to conform to any schema except that defined by the reason type.	false	v1.StatusDetails	
code	Suggested HTTP return code for this status, 0 if not set.	false	integer (int32)	

v1.ServiceStatus

ServiceStatus represents the current status of a service.

Name	Description	Required	Schema	Default
loadBalancer	LoadBalancer contains the current status of the load-balancer, if one is present.	false	v1.LoadBalancerStatus	

v1.Secret

Secret holds secret data of a certain type. The total bytes of the values in the Data field must be less than MaxSecretSize bytes.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
data	Data contains the secret data. Each key must consist of alphanumeric characters, -, _ or .. The serialized form of the secret data is a base64 encoded string, representing the arbitrary (possibly non-string) data value here. Described in https://tools.ietf.org/html/rfc4648#section-4	false	object	

Name	Description	Required	Schema	Default
stringData	stringData allows specifying non-binary secret data in string form. It is provided as a write-only convenience method. All keys and values are merged into the data field on write, overwriting any existing values. It is never output when reading from the API.	false	object	
type	Used to facilitate programmatic handling of secret data.	false	string	

v1.WatchEvent

Name	Description	Required	Schema	Default
type		true	string	
object		true	string	

v1.Event

Event is a report of an event somewhere in the cluster.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	true	v1.ObjectMeta	
involvedObject	The object that this event is about.	true	v1.ObjectReference	

Name	Description	Required	Schema	Default
reason	This should be a short, machine understandable string that gives the reason for the transition into the object's current status.	false	string	
message	A human-readable description of the status of this operation.	false	string	
source	The component reporting this event. Should be a short machine understandable string.	false	v1.EventSource	
firstTimestamp	The time at which the event was first recorded. (Time of server receipt is in TypeMeta.)	false	string	
lastTimestamp	The time at which the most recent occurrence of this event was recorded.	false	string	

Name	Description	Required	Schema	Default
count	The number of times this event has occurred.	false	integer (int32)	
type	Type of this event (Normal, Warning), new types could be added in the future	false	string	
eventTime	Time when this Event was first observed.	false	string	
series	Data about the Event series this event represents or nil if it's a singleton Event.	false	v1.EventSeries	
action	What action was taken/failed regarding to the Regarding object.	false	string	
related	Optional secondary object for more complex actions.	false	v1.ObjectReference	
reportingComponent	Name of the controller that emitted this Event, e.g. `kubernetes.io/kubelet`.	true	string	

Name	Description	Required	Schema	Default
reportingInstance	ID of the controller instance, e.g. `kubelet-xyzf`.	true	string	

v1.LoadBalancerIngress

LoadBalancerIngress represents the status of a load-balancer ingress point: traffic intended for the service should be sent to an ingress point.

Name	Description	Required	Schema	Default
ip	IP is set for load-balancer ingress points that are IP based (typically GCE or OpenStack load-balancers)	false	string	
hostname	Hostname is set for load-balancer ingress points that are DNS based (typically AWS load-balancers)	false	string	

v1.DeletionPropagation

v1.NamespaceStatus

NamespaceStatus is information about the current status of a Namespace.

Name	Description	Required	Schema	Default
phase	Phase is the current lifecycle phase of the namespace. More info: https: //kubernetes. io/docs/ tasks/ administer-cluster/ namespaces/	false	string	

v1.ServiceList

ServiceList holds a list of services.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen- tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	false	v1.ListMeta	
items	List of services	true	v1.Service array	

v1.NamespaceSpec

NamespaceSpec describes the attributes on a Namespace.

184

Name	Description	Required	Schema	Default
finalizers	Finalizers is an opaque list of values that must be empty to permanently remove object from storage. More info: https: //kubernetes. io/docs/ tasks/ administer- cluster/ namespaces/	false	v1.FinalizerName array	

v1.Service

Service is a named abstraction of software service (for example, mysql) consisting of local port (for example 3306) that the proxy listens on, and the selector that determines which pods will answer requests sent through the proxy.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	Spec defines the behavior of a service. https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#spec- and-status	false	v1.ServiceSpec	
status	Most recently observed status of the service. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#spec- and-status	false	v1.ServiceStatus	

v1.Patch

Patch is provided to give a concrete name and type to the Kubernetes PATCH request body.

v1.ConfigMapList

ConfigMapList is a resource containing a list of ConfigMap objects.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ListMeta	
items	Items is the list of ConfigMaps.	true	v1.ConfigMap array	

v1.DeleteOptions

DeleteOptions may be provided when deleting an API object.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	

Name	Description	Required	Schema	Default
gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int64)	
preconditions	Must be fulfilled before a deletion is carried out. If not possible, a 409 Conflict status will be returned.	false	v1.Preconditions	

Name	Description	Required	Schema	Default
orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	false

Name	Description	Required	Schema	Default
propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all dependents in the foreground.	false	v1.DeletionPropagation	

v1.EventSeries

EventSeries contain information on series of events, i.e. thing that was/is happening continously for some time.

Name	Description	Required	Schema	Default
count	Number of occurrences in this series up to the last heartbeat time	false	integer (int32)	
lastObservedTime	Time of the last occurence observed	false	string	
state	State of this Series: Ongoing or Finished	false	string	

v1.StatusDetails

StatusDetails is a set of additional properties that MAY be set by the server to provide additional information about a response. The Reason field of a Status object defines what attributes will be set. Clients must ignore fields that do not match the defined type of each attribute, and should assume that any attribute may be empty, invalid, or under defined.

Name	Description	Required	Schema	Default
name	The name attribute of the resource associated with the status StatusReason (when there is a single name which can be described).	false	string	

Name	Description	Required	Schema	Default
group	The group attribute of the resource associated with the status StatusReason.	false	string	
kind	The kind attribute of the resource associated with the status StatusReason. On some operations may differ from the requested resource Kind. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	
uid	UID of the resource. (when there is a single resource which can be described). More info: http: //kubernetes. io/docs/user-guide/ identifiers# uids	false	string	

Name	Description	Required	Schema	Default
causes	The Causes array includes more details associated with the Sta- tusReason failure. Not all Status- Reasons may provide detailed causes.	false	v1.StatusCause array	
retryAfterSeconds	If specified, the time in seconds before the operation should be retried. Some errors may indicate the client must take an alternate action - for those errors this field may indicate how long to wait before taking the alternate action.	false	integer (int32)	

v1.ConfigMap

ConfigMap holds configuration data for pods to consume.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
data	Data contains the configuration data. Each key must consist of alphanumeric characters, -, _ or .. Values with non-UTF-8 byte sequences must use the BinaryData field. The keys stored in Data must not overlap with the keys in the BinaryData field, this is enforced during validation process.	false	object	

Name	Description	Required	Schema	Default
binaryData	BinaryData contains the binary data. Each key must consist of alphanumeric characters, -, _ or .. BinaryData can contain byte sequences that are not in the UTF-8 range. The keys stored in BinaryData must not overlap with the ones in the Data field, this is enforced during validation process. Using this field will require 1.10+ apiserver and kubelet.	false	object	

v1.Initializer

Initializer is information about an initializer that has not yet completed.

Name	Description	Required	Schema	Default
name	name of the process that is responsible for initializing this object.	true	string	

v1.ObjectReference

ObjectReference contains enough information to let you inspect or modify the referred object.

Name	Description	Required	Schema	Default
kind	Kind of the referent. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	
namespace	Namespace of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ namespaces/	false	string	

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ names/ #names	false	string	
uid	UID of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ names/#uids	false	string	
apiVersion	API version of the referent.	false	string	
resourceVersion	Specific resourceVersion to which this reference is made, if any. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# concurrency-control-and-consistency	false	string	

Name	Description	Required	Schema	Default
fieldPath	If referring to a piece of an object instead of an entire object, this string should contain a valid JSON/Go field access statement, such as desiredState.manifest.containers[2]. For example, if the object reference is to a container within a pod, this would take on a value like: "spec.containers{name}" (where "name" refers to the name of the container that triggered the event) or if no container name is specified "spec.containers[2]" (container with index 2 in this pod). This syntax is chosen only to have some well-defined way of referencing a part of an object.	false	string	

Name	Description	Required	Schema	Default

v1.LoadBalancerStatus

LoadBalancerStatus represents the status of a load-balancer.

Name	Description	Required	Schema	Default
ingress	Ingress is a list containing ingress points for the load-balancer. Traffic intended for the service should be sent to these ingress points.	false	v1.LoadBalancerIngress array	

v1.SecretList

SecretList is a list of Secret.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
items	Items is a list of secret objects. More info: https: //kubernetes. io/docs/ concepts/ configuration/ secret	true	v1.Secret array	

v1.FinalizerName

v1.ServicePort

ServicePort contains information on service's port.

Name	Description	Required	Schema	Default
name	The name of this port within the service. This must be a DNS_LABEL. All ports within a ServiceSpec must have unique names. This maps to the *Name* field in Endpoint-Port objects. Optional if only one ServicePort is defined on this service.	false	string	

Name	Description	Required	Schema	Default
protocol	The IP protocol for this port. Supports "TCP" and "UDP". Default is TCP.	false	string	
port	The port that will be exposed by this service.	true	integer (int32)	

Name	Description	Required	Schema	Default
targetPort	Number or name of the port to access on the pods targeted by the service. Number must be in the range 1 to 65535. Name must be an IANA_SVC_NAME. If this is a string, it will be looked up as a named port in the target Pod's container ports. If this is not specified, the value of the *port* field is used (an identity map). This field is ignored for services with clusterIP=None, and should be omitted or set equal to the *port* field. More info: https://kubernetes.io/docs/concepts/services-networking/service/#defining-a-service	false	string	

211

Name	Description	Required	Schema	Default
nodePort	The port on each node on which this service is exposed when type=NodePort or LoadBalancer. Usually assigned by the system. If specified, it will be allocated to the service if unused or else creation of the service will fail. Default is to auto-allocate a port if the ServiceType of this Service requires one. More info: https: //kubernetes. io/docs/ concepts/ services- networking/ service/ #nodeport	false	integer (int32)	

v1.OwnerReference

OwnerReference contains enough information to let you identify an owning object. Currently, an owning object must be in the same namespace, so there is no namespace field.

Name	Description	Required	Schema	Default
apiVersion	API version of the referent.	true	string	
kind	Kind of the referent. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	true	string	
name	Name of the referent. More info: http: //kubernetes. io/docs/user-guide/ identifiers# names	true	string	
uid	UID of the referent. More info: http: //kubernetes. io/docs/user-guide/ identifiers# uids	true	string	
controller	If true, this reference points to the managing controller.	false	boolean	false

Name	Description	Required	Schema	Default
blockOwnerDeletion	If true, AND if the owner has the "foreground-Deletion" finalizer, then the owner cannot be deleted from the key-value store until this reference is removed. Defaults to false. To set this field, a user needs "delete" permission of the owner, otherwise 422 (Unprocessable Entity) will be returned.	false	boolean	false

v1.ObjectMeta

ObjectMeta is metadata that all persisted resources must have, which includes all objects users must create.

Name	Description	Required	Schema	Default
name	Name must be unique within a namespace. Is required when creating resources, although some resources may allow a client to request the generation of an appropriate name automatically. Name is primarily intended for creation idempotence and configuration definition. Cannot be updated. More info: http://kubernetes.io/docs/user-guide/identifiers#names	false	string	

Name	Description	Required	Schema	Default
generateName	GenerateName is an optional prefix, used by the server, to generate a unique name ONLY IF the Name field has not been provided. If this field is used, the name returned to the client will be different than the name passed. This value will also be combined with a unique suffix. The provided value has the same validation rules as the Name field, and may be truncated by the length of the suffix required to make the value unique on the server. If this field is specified and the generated name exists, the server will NOT return a 409 - instead, it will either return 201 Created or 500 with	false	string	

Name	Description	Required	Schema	Default
namespace	Namespace defines the space within each name must be unique. An empty namespace is equivalent to the "default" namespace, but "default" is the canonical representation. Not all objects are required to be scoped to a namespace - the value of this field for those objects will be empty. Must be a DNS_LABEL. Cannot be updated. More info: http://kubernetes.io/docs/user-guide/namespaces	false	string	
selfLink	SelfLink is a URL representing this object. Populated by the system. Read-only.	false	string	

Name	Description	Required	Schema	Default
uid	UID is the unique in time and space value for this object. It is typically generated by the server on successful creation of a resource and is not allowed to change on PUT operations. Populated by the system. Read-only. More info: http: //kubernetes. io/docs/user-guide/ identifiers# uids	false	string	

Name	Description	Required	Schema	Default
resourceVersion	An opaque value that represents the internal version of this object that can be used by clients to determine when objects have changed. May be used for optimistic concurrency, change detection, and the watch operation on a resource or set of resources. Clients must treat these values as opaque and passed unmodified back to the server. They may only be valid for a particular resource or set of resources. Populated by the system. Read-only. Value must be treated as opaque by clients and . More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#	false	string	

Name	Description	Required	Schema	Default
generation	A sequence number representing a specific generation of the desired state. Populated by the system. Read-only.	false	integer (int64)	

Name	Description	Required	Schema	Default
creationTimestamp	CreationTimestamp is a timestamp representing the server time when this object was created. It is not guaranteed to be set in happens-before order across separate operations. Clients may not set this value. It is represented in RFC3339 form and is in UTC. Populated by the system. Read-only. Null for lists. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	string	

Name	Description	Required	Schema	Default
deletionTimestamp	DeletionTimestamp is RFC 3339 date and time at which this resource will be deleted. This field is set by the server when a graceful deletion is requested by the user, and is not directly settable by a client. The resource is expected to be deleted (no longer visible from resource lists, and not reachable by name) after the time in this field, once the finalizers list is empty. As long as the finalizers list contains items, deletion is blocked. Once the deletionTimestamp is set, this value may not be unset or be set further into the future, although it may be shortened or the resource may be deleted prior to this time.	false	string	

Name	Description	Required	Schema	Default
deletionGracePeriodSeconds	Number of seconds allowed for this object to gracefully terminate before it will be removed from the system. Only set when deletion-Timestamp is also set. May only be shortened. Read-only.	false	integer (int64)	
labels	Map of string keys and values that can be used to organize and categorize (scope and select) objects. May match selectors of replication controllers and services. More info: http://kubernetes.io/docs/user-guide/labels	false	object	

Name	Description	Required	Schema	Default
annotations	Annotations is an unstructured key value map stored with a resource that may be set by external tools to store and retrieve arbitrary metadata. They are not queryable and should be preserved when modifying objects. More info: http://kubernetes.io/docs/user-guide/annotations	false	object	

Name	Description	Required	Schema	Default
ownerReferences	List of objects depended by this object. If ALL objects in the list have been deleted, this object will be garbage collected. If this object is managed by a controller, then an entry in this list will point to this controller, with the controller field set to true. There cannot be more than one managing controller.	false	v1.OwnerReference array	

Name	Description	Required	Schema	Default
initializers	An initializer is a controller which enforces some system invariant at object creation time. This field is a list of initializers that have not yet acted on this object. If nil or empty, this object has been completely initialized. Otherwise, the object is considered uninitialized and is hidden (in list/watch and get calls) from clients that haven't explicitly asked to observe uninitialized objects. When an object is created, the system will populate this list with the current set of initializers. Only privileged users may set or modify this list. Once it is empty, it may not be modified further by	false	v1.Initializers	

Name	Description	Required	Schema	Default
finalizers	Must be empty before the object is deleted from the registry. Each entry is an identifier for the responsible component that will remove the entry from the list. If the deletion-Timestamp of the object is non-nil, entries in this list can only be removed.	false	string array	

Name	Description	Required	Schema	Default
clusterName	The name of the cluster which the object belongs to. This is used to distinguish resources with same name and namespace in different clusters. This field is not set anywhere right now and apiserver is going to ignore it if set in create or update request.	false	string	

v1.EventList

EventList is a list of events.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	v1.ListMeta	
items	List of events	true	v1.Event array	

v1.ClientIPConfig

ClientIPConfig represents the configurations of Client IP based session affinity.

Name	Description	Required	Schema	Default
timeoutSeconds	timeoutSeconds specifies the seconds of ClientIP type session sticky time. The value must be >0 && 86400(for 1 day) if ServiceAffinity == "ClientIP". Default value is 10800(for 3 hours).	false	integer (int32)	

v1.APIResource

APIResource specifies the name of a resource and whether it is namespaced.

Name	Description	Required	Schema	Default
name	name is the plural name of the resource.	true	string	

Name	Description	Required	Schema	Default
singularName	singularName is the singular name of the resource. This allows clients to handle plural and singular opaquely. The singularName is more correct for reporting status on a single item and both singular and plural are allowed from the kubectl CLI interface.	true	string	
namespaced	namespaced indicates if a resource is namespaced or not.	true	boolean	false

Name	Description	Required	Schema	Default
group	group is the preferred group of the resource. Empty implies the group of the containing resource list. For subresources, this may have a different value, for example: Scale".	false	string	
version	version is the preferred version of the resource. Empty implies the version of the containing resource list For subresources, this may have a different value, for example: v1 (while inside a v1beta1 version of the core resource's group)".	false	string	

Name	Description	Required	Schema	Default
kind	kind is the kind for the resource (e.g. *Foo* is the kind for a resource *foo*)	true	string	
verbs	verbs is a list of supported kube verbs (this includes get, list, watch, create, update, patch, delete, deletecollection, and proxy)	true	string array	
shortNames	shortNames is a list of suggested short names of the resource.	false	string array	
categories	categories is a list of the grouped resources this resource belongs to (e.g. *all*)	false	string array	

v1.ServiceSpec

ServiceSpec describes the attributes that a user creates on a service.

Name	Description	Required	Schema	Default
ports	The list of ports that are exposed by this service. More info: https: //kubernetes. io/docs/ concepts/ services- networking/ service/ #virtual-ips- and-service- proxies	false	v1.ServicePort array	

Name	Description	Required	Schema	Default
selector	Route service traffic to pods with label keys and values matching this selector. If empty or not present, the service is assumed to have an external process managing its endpoints, which Kubernetes will not modify. Only applies to types ClusterIP, NodePort, and LoadBalancer. Ignored if type is ExternalName. More info: https: //kubernetes. io/docs/ concepts/ services-networking/ service/	false	object	

Name	Description	Required	Schema	Default
clusterIP	clusterIP is the IP address of the service and is usually assigned randomly by the master. If an address is specified manually and is not in use by others, it will be allocated to the service; otherwise, creation of the service will fail. This field can not be changed through updates. Valid values are "None", empty string (""), or a valid IP address. "None" can be specified for headless services when proxying is not required. Only applies to types ClusterIP, NodePort, and LoadBalancer. Ignored if type is ExternalName. More info: https://kubernetes.io/docs/concepts/services-networking/	false	string	

237

Name	Description	Required	Schema	Default
type	type determines how the Service is exposed. Defaults to ClusterIP. Valid options are External-Name, ClusterIP, NodePort, and LoadBalancer. "External-Name" maps to the specified externalName. "ClusterIP" allocates a cluster-internal IP address for load-balancing to endpoints. Endpoints are determined by the selector or if that is not specified, by manual construction of an Endpoints object. If clusterIP is "None", no virtual IP is allocated and the endpoints are published as a set of endpoints rather than a stable IP. "NodePort" builds on ClusterIP and allocates	false	string	

Name	Description	Required	Schema	Default
externalIPs	externalIPs is a list of IP addresses for which nodes in the cluster will also accept traffic for this service. These IPs are not managed by Kubernetes. The user is responsible for ensuring that traffic arrives at a node with this IP. A common example is external load-balancers that are not part of the Kubernetes system.	false	string array	

Name	Description	Required	Schema	Default
sessionAffinity	Supports "ClientIP" and "None". Used to maintain session affinity. Enable client IP based session affinity. Must be ClientIP or None. Defaults to None. More info: https: //kubernetes. io/docs/ concepts/ services-networking/ service/ #virtual-ips-and-service-proxies	false	string	

Name	Description	Required	Schema	Default
loadBalancerIP	Only applies to Service Type: LoadBalancer will get created with the IP specified in this field. This feature depends on whether the underlying cloud-provider supports specifying the loadBalancerIP when a load balancer is created. This field will be ignored if the cloud-provider does not support the feature.	false	string	

Name	Description	Required	Schema	Default
loadBalancerSourceRanges	If specified and supported by the platform, this will restrict traffic through the cloud-provider load-balancer will be restricted to the specified client IPs. This field will be ignored if the cloud-provider does not support the feature." More info: https://kubernetes.io/docs/tasks/access-application-cluster/configure-cloud-provider-firewall/	false	string array	

Name	Description	Required	Schema	Default
externalName	externalName is the external reference that kubedns or equivalent will return as a CNAME record for this service. No proxying will be involved. Must be a valid RFC-1123 hostname (https: //tools.ietf. org/html/ rfc1123) and requires Type to be ExternalName.	false	string	

Name	Description	Required	Schema	Default
externalTrafficPolicy	externalTrafficPolicy denotes if this Service desires to route external traffic to node-local or cluster-wide endpoints. "Local" preserves the client source IP and avoids a second hop for LoadBalancer and Nodeport type services, but risks potentially imbalanced traffic spreading. "Cluster" obscures the client source IP and may cause a second hop to another node, but should have good overall load-spreading.	false	string	

Name	Description	Required	Schema	Default
healthCheckNodePort	healthCheckNodePort specifies the healthcheck nodePort for the service. If not specified, HealthCheckNodePort is created by the service api backend with the allocated nodePort. Will use user-specified nodePort value if specified by the client. Only effects when Type is set to LoadBalancer and ExternalTrafficPolicy is set to Local.	false	integer (int32)	

Name	Description	Required	Schema	Default
publishNotReadyAddresses	publishNotReadyAddresses, when set to true, indicates that DNS implementations must publish the notReadyAddresses of subsets for the Endpoints associated with the Service. The default value is false. The primary use case for setting this field is to use a StatefulSet's Headless Service to propagate SRV records for its Pods without respect to their readiness for purpose of peer discovery. This field will replace the service.alpha.kubernetes.io/tolerate-unready-endpoints when that annotation is deprecated and all clients have been converted to use this field.	false	boolean	false

Name	Description	Required	Schema	Default
sessionAffinityConfig	sessionAffinityConfig contains the configurations of session affinity.	false	v1.SessionAffinityConfig	

v1.EventSource

EventSource contains information for an event.

Name	Description	Required	Schema	Default
component	Component from which the event is generated.	false	string	
host	Node name on which the event is generated.	false	string	

types.UID

v1.StatusCause

StatusCause provides more information about an api.Status failure, including cases when multiple errors are encountered.

Name	Description	Required	Schema	Default
reason	A machine-readable description of the cause of the error. If this value is empty there is no information available.	false	string	

Name	Description	Required	Schema	Default
message	A human-readable description of the cause of the error. This field may be presented as-is to a reader.	false	string	

Name	Description	Required	Schema	Default
field	The field of the resource that has caused this error, as named by its JSON serialization. May include dot and postfix notation for nested attributes. Arrays are zero-indexed. Fields may appear more than once in an array of causes due to fields having multiple errors. Optional. Examples: "name" - the field "name" on the current resource "items[0].name" - the field "name" on the first array entry in "items"	false	string	

v1.SessionAffinityConfig

SessionAffinityConfig represents the configurations of session affinity.

Name	Description	Required	Schema	Default
clientIP	clientIP contains the configurations of Client IP based session affinity.	false	v1.ClientIPConfig	

any

Represents an untyped JSON map - see the description of the field for more info about the structure of this object.

Edit This Page

Top Level API Objects

Top Level API Objects

- v1beta1.Deployment
- v1beta1.DeploymentList
- v1beta1.DeploymentRollback
- v1beta1.Scale
- v1beta1.DaemonSetList
- v1beta1.DaemonSet
- v1beta1.Ingress
- v1beta1.IngressList
- v1beta1.ReplicaSet
- v1beta1.ReplicaSetList

Definitions

v1beta1.DeploymentStatus

DeploymentStatus is the most recently observed status of the Deployment.

Name	Description	Required	Schema	Default
observedGeneration	The generation observed by the deployment controller.	false	integer (int64)	
replicas	Total number of non-terminated pods targeted by this deployment (their labels match the selector).	false	integer (int32)	
updatedReplicas	Total number of non-terminated pods targeted by this deployment that have the desired template spec.	false	integer (int32)	
readyReplicas	Total number of ready pods targeted by this deployment.	false	integer (int32)	
availableReplicas	Total number of available pods (ready for at least min-ReadySeconds) targeted by this deployment.	false	integer (int32)	

Name	Description	Required	Schema	Default
unavailableReplicas	Total number of unavailable pods targeted by this deployment. This is the total number of pods that are still required for the deployment to have 100% available capacity. They may either be pods that are running but not yet available or pods that still have not been created.	false	integer (int32)	
conditions	Represents the latest available observations of a deployment's current state.	false	v1beta1.DeploymentCondition array	

Name	Description	Required	Schema	Default
collisionCount	Count of hash collisions for the Deployment. The Deployment controller uses this field as a collision avoidance mechanism when it needs to create the name for the newest ReplicaSet.	false	integer (int32)	

v1.APIResourceList

APIResourceList is a list of APIResource, it is used to expose the name of the resources supported in a specific group and version, and if the resource is namespaced.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
groupVersion	groupVersion is the group and version this APIResourceList is for.	true	string	
resources	resources contains the name of the resources and if they are namespaced.	true	v1.APIResource array	

v1.Affinity

Affinity is a group of affinity scheduling rules.

Name	Description	Required	Schema	Default
nodeAffinity	Describes node affinity scheduling rules for the pod.	false	v1.NodeAffinity	
podAffinity	Describes pod affinity scheduling rules (e.g. co-locate this pod in the same node, zone, etc. as some other pod(s)).	false	v1.PodAffinity	
podAntiAffinity	Describes pod anti-affinity scheduling rules (e.g. avoid putting this pod in the same node, zone, etc. as some other pod(s)).	false	v1.PodAntiAffinity	

v1beta1.DaemonSetStatus

DaemonSetStatus represents the current status of a daemon set.

Name	Description	Required	Schema	Default
currentNumberScheduled	The number of nodes that are running at least 1 daemon pod and are supposed to run the daemon pod. More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ daemonset/	true	integer (int32)	
numberMisscheduled	The number of nodes that are running the daemon pod, but are not supposed to run the daemon pod. More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ daemonset/	true	integer (int32)	

Name	Description	Required	Schema	Default
desiredNumberScheduled	The total number of nodes that should be running the daemon pod (including nodes correctly running the daemon pod). More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ daemonset/	true	integer (int32)	
numberReady	The number of nodes that should be running the daemon pod and have one or more of the daemon pod running and ready.	true	integer (int32)	
observedGeneration	The most recent generation observed by the daemon set controller.	false	integer (int64)	
updatedNumberScheduled	The total number of nodes that are running updated daemon pod	false	integer (int32)	

Name	Description	Required	Schema	Default
numberAvailable	The number of nodes that should be running the daemon pod and have one or more of the daemon pod running and available (ready for at least spec.minReadySeconds)	false	integer (int32)	
numberUnavailable	The number of nodes that should be running the daemon pod and have none of the daemon pod running and available (ready for at least spec.minReadySeconds)	false	integer (int32)	
collisionCount	Count of hash collisions for the DaemonSet. The DaemonSet controller uses this field as a collision avoidance mechanism when it needs to create the name for the newest ControllerRevision.	false	integer (int32)	

Name	Description	Required	Schema	Default
conditions	Represents the latest available observations of a DaemonSet's current state.	false	v1beta1.DaemonSetCondition array	

v1.NodeSelectorTerm

A null or empty node selector term matches no objects.

Name	Description	Required	Schema	Default
matchExpressions	Required. A list of node selector requirements. The requirements are ANDed.	true	v1.NodeSelectorRequirement array	

v1.Preconditions

Preconditions must be fulfilled before an operation (update, delete, etc.) is carried out.

Name	Description	Required	Schema	Default
uid	Specifies the target UID.	false	types.UID	

v1.ObjectFieldSelector

ObjectFieldSelector selects an APIVersioned field of an object.

Name	Description	Required	Schema	Default
apiVersion	Version of the schema the FieldPath is written in terms of, defaults to "v1".	false	string	
fieldPath	Path of the field to select in the specified API version.	true	string	

v1.SELinuxOptions

SELinuxOptions are the labels to be applied to the container

Name	Description	Required	Schema	Default
user	User is a SELinux user label that applies to the container.	false	string	
role	Role is a SELinux role label that applies to the container.	false	string	
type	Type is a SELinux type label that applies to the container.	false	string	

Name	Description	Required	Schema	Default
level	Level is SELinux level label that applies to the container.	false	string	

v1beta1.IngressSpec

IngressSpec describes the Ingress the user wishes to exist.

Name	Description	Required	Schema	Default
backend	A default backend capable of servicing requests that don't match any rule. At least one of *backend* or *rules* must be specified. This field is optional to allow the loadbalancer controller or defaulting logic to specify a global default.	false	v1beta1.IngressBackend	

Name	Description	Required	Schema	Default
tls	TLS configuration. Currently the Ingress only supports a single TLS port, 443. If multiple members of this list specify different hosts, they will be multiplexed on the same port according to the hostname specified through the SNI TLS extension, if the ingress controller fulfilling the ingress supports SNI.	false	v1beta1.IngressTLS array	
rules	A list of host rules used to configure the Ingress. If unspecified, or no rule matches, all traffic is sent to the default backend.	false	v1beta1.IngressRule array	

v1.VolumeMount

VolumeMount describes a mounting of a Volume within a container.

Name	Description	Required	Schema	Default
name	This must match the Name of a Volume.	true	string	
readOnly	Mounted read-only if true, read-write otherwise (false or unspecified). Defaults to false.	false	boolean	false
mountPath	Path within the container at which the volume should be mounted. Must not contain :.	true	string	
subPath	Path within the volume from which the container's volume should be mounted. Defaults to "" (volume's root).	false	string	

Name	Description	Required	Schema	Default
mountPropagation	mountPropagation determines how mounts are propagated from the host to container and the other way around. When not set, MountPropagationHost-ToContainer is used. This field is alpha in 1.8 and can be reworked or removed in a future release.	false	v1.MountPropagationMode	

v1.MountPropagationMode

v1.DownwardAPIProjection

Represents downward API info for projecting into a projected volume. Note that this is identical to a downwardAPI volume source without the default mode.

Name	Description	Required	Schema	Default
items	Items is a list of DownwardAPIVolume file	false	v1.DownwardAPIVolumeFile array	

v1.LabelSelector

A label selector is a label query over a set of resources. The result of matchLabels and matchExpressions are ANDed. An empty label selector matches all objects. A null label selector matches no objects.

Name	Description	Required	Schema	Default
matchLabels	matchLabels is a map of {key,value} pairs. A single {key,value} in the matchLabels map is equivalent to an element of matchExpressions, whose key field is "key", the operator is "In", and the values array contains only "value". The requirements are ANDed.	false	object	
matchExpressions	matchExpressions is a list of label selector requirements. The requirements are ANDed.	false	v1.LabelSelectorRequirement array	

v1beta1.IngressBackend

IngressBackend describes all endpoints for a given service and port.

Name	Description	Required	Schema	Default
serviceName	Specifies the name of the referenced service.	true	string	

Name	Description	Required	Schema	Default
servicePort	Specifies the port of the referenced service.	true	string	

v1beta1.ReplicaSetList

ReplicaSetList is a collection of ReplicaSets.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
items	List of ReplicaSets. More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ replicationcontroller	true	v1beta1.ReplicaSet array	

v1.CephFSVolumeSource

Represents a Ceph Filesystem mount that lasts the lifetime of a pod Cephfs volumes do not support ownership management or SELinux relabeling.

Name	Description	Required	Schema	Default
monitors	Required: Monitors is a collection of Ceph monitors More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ cephfs/ README. md#how-to- use-it	true	string array	
path	Optional: Used as the mounted root, rather than the full Ceph tree, default is /	false	string	

Name	Description	Required	Schema	Default
user	Optional: User is the rados user name, default is admin More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ cephfs/ README. md#how-to-use-it	false	string	
secretFile	Optional: SecretFile is the path to key ring for User, default is /etc/ceph/user.secret More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ cephfs/ README. md#how-to-use-it	false	string	

Name	Description	Required	Schema	Default
secretRef	Optional: SecretRef is reference to the authentication secret for User, default is empty. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ cephfs/ README. md#how-to-use-it	false	v1.LocalObjectReference	
readOnly	Optional: Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ cephfs/ README. md#how-to-use-it	false	boolean	false

v1beta1.IngressStatus

IngressStatus describe the current state of the Ingress.

Name	Description	Required	Schema	Default
loadBalancer	LoadBalancer contains the current status of the load-balancer.	false	v1.LoadBalancerStatus	

v1.DownwardAPIVolumeSource

DownwardAPIVolumeSource represents a volume containing downward API info. Downward API volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
items	Items is a list of downward API volume file	false	v1.DownwardAPIVolumeFile array	

Name	Description	Required	Schema	Default
defaultMode	Optional: mode bits to use on created files by default. Must be a value between 0 and 0777. Defaults to 0644. Directories within the path are not affected by this setting. This might be in conflict with other options that affect the file mode, like fsGroup, and the result can be other mode bits set.	false	integer (int32)	

v1beta1.ReplicaSetCondition

ReplicaSetCondition describes the state of a replica set at a certain point.

Name	Description	Required	Schema	Default
type	Type of replica set condition.	true	string	
status	Status of the condition, one of True, False, Unknown.	true	string	

Name	Description	Required	Schema	Default
lastTransitionTime	The last time the condition transitioned from one status to another.	false	string	
reason	The reason for the condition's last transition.	false	string	
message	A human readable message indicating details about the transition.	false	string	

v1.GCEPersistentDiskVolumeSource

Represents a Persistent Disk resource in Google Compute Engine.

A GCE PD must exist before mounting to a container. The disk must also be in the same GCE project and zone as the kubelet. A GCE PD can only be mounted as read/write once or read-only many times. GCE PDs support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
pdName	Unique name of the PD resource in GCE. Used to identify the disk in GCE. More info: https://kubernetes.io/docs/concepts/storage/volumes#gcepersistentdisk	true	string	

Name	Description	Required	Schema	Default
fsType	Filesystem type of the volume that you want to mount. Tip: Ensure that the filesystem type is supported by the host operating system. Examples: "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified. More info: https://kubernetes.io/docs/concepts/storage/volumes#gcepersistentdisk	false	string	

Name	Description	Required	Schema	Default
partition	The partition in the volume that you want to mount. If omitted, the default is to mount by volume name. Examples: For volume /dev/sda1, you specify the partition as "1". Similarly, the volume partition for /dev/sda is "0" (or you can leave the property empty). More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# gcepersistentdisk	false	integer (int32)	

Name	Description	Required	Schema	Default
readOnly	ReadOnly here will force the ReadOnly setting in VolumeMounts. Defaults to false. More info: https://kubernetes.io/docs/concepts/storage/volumes#gcepersistentdisk	false	boolean	false

v1beta1.RollingUpdateDeployment

Spec to control the desired behavior of rolling update.

Name	Description	Required	Schema	Default
maxUnavailable	The maximum number of pods that can be unavailable during the update. Value can be an absolute number (ex: 5) or a percentage of desired pods (ex: 10%). Absolute number is calculated from percentage by rounding down. This can not be 0 if MaxSurge is 0. By default, a fixed value of 1 is used. Example: when this is set to 30%, the old RC can be scaled down to 70% of desired pods immediately when the rolling update starts. Once new pods are ready, old RC can be scaled down further, followed by scaling up the new RC, ensuring that the total number of pods available at	false	string	

Name	Description	Required	Schema	Default
maxSurge	The maximum number of pods that can be scheduled above the desired number of pods. Value can be an absolute number (ex: 5) or a percentage of desired pods (ex: 10%). This can not be 0 if MaxUnavailable is 0. Absolute number is calculated from percentage by rounding up. By default, a value of 1 is used. Example: when this is set to 30%, the new RC can be scaled up immediately when the rolling update starts, such that the total number of old and new pods do not exceed 130% of desired pods. Once old pods have been killed, new RC can be scaled up further,	false	string	

Name	Description	Required	Schema	Default

v1beta1.HTTPIngressRuleValue

HTTPIngressRuleValue is a list of http selectors pointing to backends. In the example: http://%3Chost%3E/%3Cpath%3E?%3Csearchpart%3E → backend where parts of the url correspond to RFC 3986, this resource will be used to match against everything after the last / and before the first *?* or *#*.

Name	Description	Required	Schema	Default
paths	A collection of paths that map requests to backends.	true	v1beta1.HTTPIngressPath array	

v1.ConfigMapVolumeSource

Adapts a ConfigMap into a volume.

The contents of the target ConfigMap's Data field will be presented in a volume as files using the keys in the Data field as the file names, unless the items element is populated with specific mappings of keys to paths. ConfigMap volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/ #names	false	string	

Name	Description	Required	Schema	Default
items	If unspecified, each key-value pair in the Data field of the referenced ConfigMap will be projected into the volume as a file whose name is the key and content is the value. If specified, the listed keys will be projected into the specified paths, and unlisted keys will not be present. If a key is specified which is not present in the ConfigMap, the volume setup will error unless it is marked optional. Paths must be relative and may not contain the .. path or start with ...	false	v1.KeyToPath array	

Name	Description	Required	Schema	Default
defaultMode	Optional: mode bits to use on created files by default. Must be a value between 0 and 0777. Defaults to 0644. Directories within the path are not affected by this setting. This might be in conflict with other options that affect the file mode, like fsGroup, and the result can be other mode bits set.	false	integer (int32)	
optional	Specify whether the ConfigMap or it's keys must be defined	false	boolean	false

v1.GitRepoVolumeSource

Represents a volume that is populated with the contents of a git repository. Git repo volumes do not support ownership management. Git repo volumes support SELinux relabeling.

Name	Description	Required	Schema	Default
repository	Repository URL	true	string	

Name	Description	Required	Schema	Default
revision	Commit hash for the specified revision.	false	string	
directory	Target directory name. Must not contain or start with ... If . is supplied, the volume directory will be the git repository. Otherwise, if specified, the volume will contain the git repository in the subdirectory with the given name.	false	string	

v1.SecretEnvSource

SecretEnvSource selects a Secret to populate the environment variables with.

The contents of the target Secret's Data field will represent the key-value pairs as environment variables.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ names/ #names	false	string	
optional	Specify whether the Secret must be defined	false	boolean	false

v1.PortworxVolumeSource

PortworxVolumeSource represents a Portworx volume resource.

Name	Description	Required	Schema	Default
volumeID	VolumeID uniquely identifies a Portworx volume	true	string	

Name	Description	Required	Schema	Default
fsType	FSType represents the filesystem type to mount Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs". Implicitly inferred to be "ext4" if unspecified.	false	string	
readOnly	Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false

v1.Capabilities

Adds and removes POSIX capabilities from running containers.

Name	Description	Required	Schema	Default
add	Added capabilities	false	v1.Capability array	
drop	Removed capabilities	false	v1.Capability array	

v1.Initializer

Initializer is information about an initializer that has not yet completed.

Name	Description	Required	Schema	Default
name	name of the process that is responsible for initializing this object.	true	string	

v1.LocalObjectReference

LocalObjectReference contains enough information to let you locate the referenced object inside the same namespace.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/ #names	false	string	

v1.ProjectedVolumeSource

Represents a projected volume source

Name	Description	Required	Schema	Default
sources	list of volume projections	true	v1.VolumeProjection array	

Name	Description	Required	Schema	Default
defaultMode	Mode bits to use on created files by default. Must be a value between 0 and 0777. Directories within the path are not affected by this setting. This might be in conflict with other options that affect the file mode, like fsGroup, and the result can be other mode bits set.	false	integer (int32)	

v1.ExecAction

ExecAction describes a "run in container" action.

Name	Description	Required	Schema	Default
command	Command is the command line to execute inside the container, the working directory for the command is root (/) in the container's filesystem. The command is simply exec'd, it is not run inside a shell, so traditional shell instructions (' | ', etc) won't work. To use a shell, you need to explicitly call out to that shell. Exit status of 0 is treated as live/healthy and non-zero is unhealthy.	false		string array

v1beta1.RollingUpdateDaemonSet

Spec to control the desired behavior of daemon set rolling update.

Name	Description	Required	Schema	Default
maxUnavailable	The maximum number of DaemonSet pods that can be unavailable during the update. Value can be an absolute number (ex: 5) or a percentage of total number of DaemonSet pods at the start of the update (ex: 10%). Absolute number is calculated from percentage by rounding up. This cannot be 0. Default value is 1. Example: when this is set to 30%, at most 30% of the total number of nodes that should be running the daemon pod (i.e. status.desiredNumberScheduled) can have their pods stopped for an update at any given time. The update starts by stopping at most 30% of those DaemonSet	false	string	

Name	Description	Required	Schema	Default

v1.ObjectMeta

ObjectMeta is metadata that all persisted resources must have, which includes all objects users must create.

Name	Description	Required	Schema	Default
name	Name must be unique within a namespace. Is required when creating resources, although some resources may allow a client to request the generation of an appropriate name automatically. Name is primarily intended for creation idempotence and configuration definition. Cannot be updated. More info: http://kubernetes.io/docs/user-guide/identifiers#names	false	string	

Name	Description	Required	Schema	Default
generateName	GenerateName is an optional prefix, used by the server, to generate a unique name ONLY IF the Name field has not been provided. If this field is used, the name returned to the client will be different than the name passed. This value will also be combined with a unique suffix. The provided value has the same validation rules as the Name field, and may be truncated by the length of the suffix required to make the value unique on the server. If this field is specified and the generated name exists, the server will NOT return a 409 - instead, it will either return 201 Created or 500 with	false	string	

Name	Description	Required	Schema	Default
namespace	Namespace defines the space within each name must be unique. An empty namespace is equivalent to the "default" namespace, but "default" is the canonical representation. Not all objects are required to be scoped to a namespace - the value of this field for those objects will be empty. Must be a DNS_LABEL. Cannot be updated. More info: http: //kubernetes. io/docs/user-guide/ namespaces	false	string	
selfLink	SelfLink is a URL representing this object. Populated by the system. Read-only.	false	string	

Name	Description	Required	Schema	Default
uid	UID is the unique in time and space value for this object. It is typically generated by the server on successful creation of a resource and is not allowed to change on PUT operations.

Populated by the system. Read-only. More info: http: //kubernetes. io/docs/user-guide/ identifiers# uids | false | string | |

Name	Description	Required	Schema	Default
resourceVersion	An opaque value that represents the internal version of this object that can be used by clients to determine when objects have changed. May be used for optimistic concurrency, change detection, and the watch operation on a resource or set of resources. Clients must treat these values as opaque and passed unmodified back to the server. They may only be valid for a particular resource or set of resources. Populated by the system. Read-only. Value must be treated as opaque by clients and . More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#	false	string	

Name	Description	Required	Schema	Default
generation	A sequence number representing a specific generation of the desired state. Populated by the system. Read-only.	false	integer (int64)	

Name	Description	Required	Schema	Default
creationTimestamp	CreationTimestamp is a timestamp representing the server time when this object was created. It is not guaranteed to be set in happens-before order across separate operations. Clients may not set this value. It is represented in RFC3339 form and is in UTC. Populated by the system. Read-only. Null for lists. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	false	string	

Name	Description	Required	Schema	Default
deletionTimestamp	DeletionTimestamp is RFC 3339 date and time at which this resource will be deleted. This field is set by the server when a graceful deletion is requested by the user, and is not directly settable by a client. The resource is expected to be deleted (no longer visible from resource lists, and not reachable by name) after the time in this field, once the finalizers list is empty. As long as the finalizers list contains items, deletion is blocked. Once the deletion-Timestamp is set, this value may not be unset or be set further into the future, although it may be shortened or the resource may be deleted prior to this time.	false	string	

Name	Description	Required	Schema	Default
deletionGracePeriodSeconds	Number of seconds allowed for this object to gracefully terminate before it will be removed from the system. Only set when deletion-Timestamp is also set. May only be shortened. Read-only.	false	integer (int64)	
labels	Map of string keys and values that can be used to organize and categorize (scope and select) objects. May match selectors of replication controllers and services. More info: http://kubernetes.io/docs/user-guide/labels	false	object	

Name	Description	Required	Schema	Default
annotations	Annotations is an unstructured key value map stored with a resource that may be set by external tools to store and retrieve arbitrary metadata. They are not queryable and should be preserved when modifying objects. More info: http://kubernetes.io/docs/user-guide/annotations	false	object	

Name	Description	Required	Schema	Default
ownerReferences	List of objects depended by this object. If ALL objects in the list have been deleted, this object will be garbage collected. If this object is managed by a controller, then an entry in this list will point to this controller, with the controller field set to true. There cannot be more than one managing controller.	false	v1.OwnerReference array	

Name	Description	Required	Schema	Default
initializers	An initializer is a controller which enforces some system invariant at object creation time. This field is a list of initializers that have not yet acted on this object. If nil or empty, this object has been completely initialized. Otherwise, the object is considered uninitialized and is hidden (in list/watch and get calls) from clients that haven't explicitly asked to observe uninitialized objects. When an object is created, the system will populate this list with the current set of initializers. Only privileged users may set or modify this list. Once it is empty, it may not be modified further by	false	v1.Initializers	

301

Name	Description	Required	Schema	Default
finalizers	Must be empty before the object is deleted from the registry. Each entry is an identifier for the responsible component that will remove the entry from the list. If the deletion-Timestamp of the object is non-nil, entries in this list can only be removed.	false	string array	

Name	Description	Required	Schema	Default
clusterName	The name of the cluster which the object belongs to. This is used to distinguish resources with same name and namespace in different clusters. This field is not set anywhere right now and apiserver is going to ignore it if set in create or update request.	false	string	

v1beta1.ReplicaSetSpec

ReplicaSetSpec is the specification of a ReplicaSet.

Name	Description	Required	Schema	Default
replicas	Replicas is the number of desired replicas. This is a pointer to distinguish between explicit zero and unspecified. Defaults to 1. More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ replicationcontroller/ #what-is-a-replicationcontroller	false	integer (int32)	
minReadySeconds	Minimum number of seconds for which a newly created pod should be ready without any of its container crashing, for it to be considered available. Defaults to 0 (pod will be considered available as soon as it is ready)	false	integer (int32)	

Name	Description	Required	Schema	Default
selector	Selector is a label query over pods that should match the replica count. If the selector is empty, it is defaulted to the labels present on the pod template. Label keys and values that must match in order to be controlled by this replica set. More info: https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/#label-selectors	false	v1.LabelSelector	

Name	Description	Required	Schema	Default
template	Template is the object that describes the pod that will be created if insufficient replicas are detected. More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ replicationcontroller# pod-template	false	v1.PodTemplateSpec	

v1beta1.Deployment

DEPRECATED - This group version of Deployment is deprecated by apps/v1beta2/Deployment. See the release notes for more information. Deployment enables declarative updates for Pods and ReplicaSets.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen-tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard object metadata.	false	v1.ObjectMeta	
spec	Specification of the desired behavior of the Deployment.	false	v1beta1.DeploymentSpec	
status	Most recently observed status of the Deployment.	false	v1beta1.DeploymentStatus	

v1beta1.DaemonSetSpec

DaemonSetSpec is the specification of a daemon set.

Name	Description	Required	Schema	Default
selector	A label query over pods that are managed by the daemon set. Must match in order to be controlled. If empty, defaulted to labels on Pod template. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ labels/ #label- selectors	false	v1.LabelSelector	

Name	Description	Required	Schema	Default
template	An object that describes the pod that will be created. The DaemonSet will create exactly one copy of this pod on every node that matches the template's node selector (or on every node if no node selector is specified). More info: https: //kubernetes. io/docs/ concepts/ workloads/ controllers/ replicationcontroller# pod-template	true	v1.PodTemplateSpec	
updateStrategy	An update strategy to replace existing DaemonSet pods with new pods.	false	v1beta1.DaemonSetUpdateStrategy	

Name	Description	Required	Schema	Default
minReadySeconds	The minimum number of seconds for which a newly created DaemonSet pod should be ready without any of its container crashing, for it to be considered available. Defaults to 0 (pod will be considered available as soon as it is ready).	false	integer (int32)	
templateGeneration	DEPRECATED A sequence number representing a specific generation of the template. Populated by the system. It can be set only during the creation.	false	integer (int64)	

Name	Description	Required	Schema	Default
revisionHistoryLimit	The number of old history to retain to allow rollback. This is a pointer to distinguish between explicit zero and not specified. Defaults to 10.	false	integer (int32)	

types.UID

v1.AzureFileVolumeSource

AzureFile represents an Azure File Service mount on the host and bind mount to the pod.

Name	Description	Required	Schema	Default
secretName	the name of secret that contains Azure Storage Account Name and Key	true	string	
shareName	Share Name	true	string	
readOnly	Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false

v1.ISCSIVolumeSource

Represents an ISCSI disk. ISCSI volumes can only be mounted as read/write once. ISCSI volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
targetPortal	iSCSI Target Portal. The Portal is either an IP or ip_addr:port if the port is other than default (typically TCP ports 860 and 3260).	true	string	
iqn	Target iSCSI Qualified Name.	true	string	
lun	iSCSI Target Lun number.	true	integer (int32)	
iscsiInterface	iSCSI Interface Name that uses an iSCSI transport. Defaults to *default* (tcp).	false	string	

Name	Description	Required	Schema	Default
fsType	Filesystem type of the volume that you want to mount. Tip: Ensure that the filesystem type is supported by the host operating system. Examples: ”ext4”, ”xfs”, ”ntfs”. Implicitly inferred to be ”ext4” if unspecified. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# iscsi	false	string	
readOnly	ReadOnly here will force the ReadOnly setting in VolumeMounts. Defaults to false.	false	boolean	false

Name	Description	Required	Schema	Default
portals	iSCSI Target Portal List. The portal is either an IP or ip_addr:port if the port is other than default (typically TCP ports 860 and 3260).	false	string array	
chapAuthDiscovery	whether support iSCSI Discovery CHAP authentication	false	boolean	false
chapAuthSession	whether support iSCSI Session CHAP authentication	false	boolean	false
secretRef	CHAP Secret for iSCSI target and initiator authentication	false	v1.LocalObjectReference	

Name	Description	Required	Schema	Default
initiatorName	Custom iSCSI Initiator Name. If initiatorName is specified with iscsiInterface simultaneously, new iSCSI interface <target portal>:<volume name> will be created for the connection.	false	string	

v1beta1.IngressList

IngressList is a collection of Ingress.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ListMeta	
items	Items is the list of Ingress.	true	v1beta1.Ingress array	

v1.EmptyDirVolumeSource

Represents an empty directory for a pod. Empty directory volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
medium	What type of storage medium should back this directory. The default is ”” which means to use the node's default medium. Must be an empty string (default) or Memory. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# emptydir	false	string	

Name	Description	Required	Schema	Default
sizeLimit	Total amount of local storage required for this EmptyDir volume. The size limit is also applicable for memory medium. The maximum usage on memory medium EmptyDir would be the minimum value between the SizeLimit specified here and the sum of memory limits of all containers in a pod. The default is nil which means that the limit is undefined. More info: http: //kubernetes. io/docs/user-guide/ volumes# emptydir	false	string	

v1beta1.ScaleSpec

describes the attributes of a scale subresource

Name	Description	Required	Schema	Default
replicas	desired number of instances for the scaled object.	false	integer (int32)	

v1.PodAffinityTerm

Defines a set of pods (namely those matching the labelSelector relative to the given namespace(s)) that this pod should be co-located (affinity) or not co-located (anti-affinity) with, where co-located is defined as running on a node whose value of the label with key <topologyKey> matches that of any node on which a pod of the set of pods is running

Name	Description	Required	Schema	Default
labelSelector	A label query over a set of resources, in this case pods.	false	v1.LabelSelector	
namespaces	namespaces specifies which namespaces the labelSelector applies to (matches against); null or empty list means "this pod's namespace"	false	string array	

Name	Description	Required	Schema	Default
topologyKey	This pod should be co-located (affinity) or not co-located (anti-affinity) with the pods matching the labelSelector in the specified namespaces, where co-located is defined as running on a node whose value of the label with key topologyKey matches that of any node on which any of the selected pods is running. Empty topologyKey is not allowed.	true	string	

v1.EnvFromSource

EnvFromSource represents the source of a set of ConfigMaps

Name	Description	Required	Schema	Default
prefix	An optional identifer to prepend to each key in the ConfigMap. Must be a C_IDENTIFIER.	false	string	
configMapRef	The ConfigMap to select from	false	v1.ConfigMapEnvSource	
secretRef	The Secret to select from	false	v1.SecretEnvSource	

v1.PodAffinity

Pod affinity is a group of inter pod affinity scheduling rules.

Name	Description	Required	Schema	Default
requiredDuringSchedulingIgnoredDuringExecution	If the affinity requirements specified by this field are not met at scheduling time, the pod will not be scheduled onto the node. If the affinity requirements specified by this field cease to be met at some point during pod execution (e.g. due to a pod label update), the system may or may not try to eventually evict the pod from its node. When there are multiple elements, the lists of nodes corresponding to each podAffinityTerm are intersected, i.e. all terms must be satisfied.	false	v1.PodAffinityTerm array	

Name	Description	Required	Schema	Default
preferredDuringSchedulingIgnoredDuringExecution	The scheduler will prefer to schedule pods to nodes that satisfy the affinity expressions specified by this field, but it may choose a node that violates one or more of the expressions. The node that is most preferred is the one with the greatest sum of weights, i.e. for each node that meets all of the scheduling requirements (resource request, requiredDuringScheduling affinity expressions, etc.), compute a sum by iterating through the elements of this field and adding "weight" to the sum if the node has pods which matches the corresponding podAffinityTerm; the node(s) with	false	v1.WeightedPodAffinityTerm array	

Name	Description	Required	Schema	Default

v1.FlockerVolumeSource

Represents a Flocker volume mounted by the Flocker agent. One and only one of datasetName and datasetUUID should be set. Flocker volumes do not support ownership management or SELinux relabeling.

Name	Description	Required	Schema	Default
datasetName	Name of the dataset stored as metadata → name on the dataset for Flocker should be considered as deprecated	false	string	
datasetUUID	UUID of the dataset. This is unique identifier of a Flocker dataset	false	string	

v1.PersistentVolumeClaimVolumeSource

PersistentVolumeClaimVolumeSource references the user's PVC in the same namespace. This volume finds the bound PV and mounts that volume for the pod. A PersistentVolumeClaimVolumeSource is, essentially, a wrapper around another type of volume that is owned by someone else (the system).

Name	Description	Required	Schema	Default
claimName	ClaimName is the name of a PersistentVolumeClaim in the same namespace as the pod using this volume. More info: https://kubernetes.io/docs/concepts/storage/persistent-volumes#persistentvolumeclaims	true	string	
readOnly	Will force the ReadOnly setting in VolumeMounts. Default false.	false	boolean	false

v1.ListMeta

ListMeta describes metadata that synthetic resources must have, including lists and various status objects. A resource may have only one of {ObjectMeta, ListMeta}.

Name	Description	Required	Schema	Default
selfLink	selfLink is a URL representing this object. Populated by the system. Read-only.	false	string	

Name	Description	Required	Schema	Default
resourceVersion	String that identifies the server's internal version of this object that can be used by clients to determine when objects have changed. Value must be treated as opaque by clients and passed unmodified back to the server. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# concurrency-control-and-consistency	false	string	

Name	Description	Required	Schema	Default
continue	continue may be set if the user set a limit on the number of items returned, and indicates that the server has more data available. The value is opaque and may be used to issue another request to the endpoint that served this list to retrieve the next set of available objects. Continuing a list may not be possible if the server configuration has changed or more than a few minutes have passed. The resourceVersion field returned when using this continue value will be identical to the value in the first response.	false	string	

Name	Description	Required	Schema	Default

v1beta1.RollbackConfig

DEPRECATED.

Name	Description	Required	Schema	Default
revision	The revision to rollback to. If set to 0, rollback to the last revision.	false	integer (int64)	

v1.SecretVolumeSource

Adapts a Secret into a volume.

The contents of the target Secret's Data field will be presented in a volume as files using the keys in the Data field as the file names. Secret volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
secretName	Name of the secret in the pod's namespace to use. More info: https://kubernetes.io/docs/concepts/storage/volumes#secret	false	string	

Name	Description	Required	Schema	Default
items	If unspecified, each key-value pair in the Data field of the referenced Secret will be projected into the volume as a file whose name is the key and content is the value. If specified, the listed keys will be projected into the specified paths, and unlisted keys will not be present. If a key is specified which is not present in the Secret, the volume setup will error unless it is marked optional. Paths must be relative and may not contain the .. path or start with ...	false	v1.KeyToPath array	

Name	Description	Required	Schema	Default
defaultMode	Optional: mode bits to use on created files by default. Must be a value between 0 and 0777. Defaults to 0644. Directories within the path are not affected by this setting. This might be in conflict with other options that affect the file mode, like fsGroup, and the result can be other mode bits set.	false	integer (int32)	
optional	Specify whether the Secret or it's keys must be defined	false	boolean	false

v1.FlexVolumeSource

FlexVolume represents a generic volume resource that is provisioned/attached using an exec based plugin.

Name	Description	Required	Schema	Default
driver	Driver is the name of the driver to use for this volume.	true	string	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". The default filesystem depends on FlexVolume script.	false	string	

Name	Description	Required	Schema	Default
secretRef	Optional: SecretRef is reference to the secret object containing sensitive information to pass to the plugin scripts. This may be empty if no secret object is specified. If the secret object contains more than one secret, all secrets are passed to the plugin scripts.	false	v1.LocalObjectReference	
readOnly	Optional: Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false
options	Optional: Extra command options if any.	false	object	

v1.EnvVarSource

EnvVarSource represents a source for the value of an EnvVar.

Name	Description	Required	Schema	Default
fieldRef	Selects a field of the pod: supports metadata.name, metadata.namespace, metadata.labels, metadata.annotations, spec.nodeName, spec.serviceAccountName, status.hostIP, status.podIP.	false	v1.ObjectFieldSelector	
resourceFieldRef	Selects a resource of the container: only resources limits and requests (limits.cpu, limits.memory, limits.ephemeral-storage, requests.cpu, requests.memory and requests.ephemeral-storage) are currently supported.	false	v1.ResourceFieldSelector	
configMapKeyRef	Selects a key of a ConfigMap.	false	v1.ConfigMapKeySelector	

Name	Description	Required	Schema	Default
secretKeyRef	Selects a key of a secret in the pod's namespace	false	v1.SecretKeySelector	

v1.LoadBalancerIngress

LoadBalancerIngress represents the status of a load-balancer ingress point: traffic intended for the service should be sent to an ingress point.

Name	Description	Required	Schema	Default
ip	IP is set for load-balancer ingress points that are IP based (typically GCE or OpenStack load-balancers)	false	string	
hostname	Hostname is set for load-balancer ingress points that are DNS based (typically AWS load-balancers)	false	string	

v1.AzureDiskVolumeSource

AzureDisk represents an Azure Data Disk mount on the host and bind mount to the pod.

Name	Description	Required	Schema	Default
diskName	The Name of the data disk in the blob storage	true	string	
diskURI	The URI the data disk in the blob storage	true	string	
cachingMode	Host Caching mode: None, Read Only, Read Write.	false	v1.AzureDataDiskCachingMode	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified.	false	string	
readOnly	Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false

Name	Description	Required	Schema	Default
kind	Expected values Shared: multiple blob disks per storage account Dedicated: single blob disk per storage account Managed: azure managed data disk (only in managed availability set). defaults to shared	false	v1.AzureDataDiskKind	

v1.KeyToPath

Maps a string key to a path within a volume.

Name	Description	Required	Schema	Default
key	The key to project.	true	string	
path	The relative path of the file to map the key to. May not be an absolute path. May not contain the path element ... May not start with the string ...	true	string	

Name	Description	Required	Schema	Default
mode	Optional: mode bits to use on this file, must be a value between 0 and 0777. If not specified, the volume defaultMode will be used. This might be in conflict with other options that affect the file mode, like fsGroup, and the result can be other mode bits set.	false	integer (int32)	

v1beta1.DaemonSetUpdateStrategy

Name	Description	Required	Schema	Default
type	Type of daemon set update. Can be "RollingUpdate" or "OnDelete". Default is OnDelete.	false	string	
rollingUpdate	Rolling update config params. Present only if type = "RollingUpdate".	false	v1beta1.RollingUpdateDaemonSet	

v1.VsphereVirtualDiskVolumeSource

Represents a vSphere volume resource.

Name	Description	Required	Schema	Default
volumePath	Path that identifies vSphere volume vmdk	true	string	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified.	false	string	
storagePolicyName	Storage Policy Based Management (SPBM) profile name.	false	string	
storagePolicyID	Storage Policy Based Management (SPBM) profile ID associated with the StoragePolicyName.	false	string	

v1.DeleteOptions

DeleteOptions may be provided when deleting an API object.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen- tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md# resources	false	string	

Name	Description	Required	Schema	Default
gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int64)	
preconditions	Must be fulfilled before a deletion is carried out. If not possible, a 409 Conflict status will be returned.	false	v1.Preconditions	

Name	Description	Required	Schema	Default
orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	false

Name	Description	Required	Schema	Default
propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all dependents in the foreground.	false	v1.DeletionPropagation	

v1beta1.DaemonSetList

DaemonSetList is a collection of daemon sets.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen-tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	false	v1.ListMeta	
items	A list of daemon sets.	true	v1beta1.DaemonSet array	

v1.Volume

Volume represents a named volume in a pod that may be accessed by any container in the pod.

Name	Description	Required	Schema	Default
name	Volume's name. Must be a DNS_LABEL and unique within the pod. More info: https://kubernetes.io/docs/concepts/overview/working-with-objects/names/#names	true	string	

Name	Description	Required	Schema	Default
hostPath	HostPath represents a pre-existing file or directory on the host machine that is directly exposed to the container. This is generally used for system agents or other privileged things that are allowed to see the host machine. Most containers will NOT need this. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# hostpath	false	v1.HostPathVolumeSource	

Name	Description	Required	Schema	Default
emptyDir	EmptyDir represents a temporary directory that shares a pod's lifetime. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# emptydir	false	v1.EmptyDirVolumeSource	
gcePersistentDisk	GCEPersistentDisk represents a GCE Disk resource that is attached to a kubelet's host machine and then exposed to the pod. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# gcepersistentdisk	false	v1.GCEPersistentDiskVolumeSource	

Name	Description	Required	Schema	Default
awsElasticBlockStore	AWSElasticBlockStore represents an AWS Disk resource that is attached to a kubelet's host machine and then exposed to the pod. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# awselasticblockstore	false	v1.AWSElasticBlockStoreVolumeSource	
gitRepo	GitRepo represents a git repository at a particular revision.	false	v1.GitRepoVolumeSource	
secret	Secret represents a secret that should populate this volume. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# secret	false	v1.SecretVolumeSource	

Name	Description	Required	Schema	Default
nfs	NFS represents an NFS mount on the host that shares a pod's lifetime More info: https://kubernetes.io/docs/concepts/storage/volumes#nfs	false	v1.NFSVolumeSource	
iscsi	ISCSI represents an ISCSI Disk resource that is attached to a kubelet's host machine and then exposed to the pod. More info: https://releases.k8s.io/HEAD/examples/volumes/iscsi/README.md	false	v1.ISCSIVolumeSource	

Name	Description	Required	Schema	Default
glusterfs	Glusterfs represents a Glusterfs mount on the host that shares a pod's lifetime. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ glusterfs/ README. md	false	v1.GlusterfsVolumeSource	
persistentVolumeClaim	PersistentVolumeClaim represents a reference to a PersistentVolume- Claim in the same namespace. More info: https: //kubernetes. io/docs/ concepts/ storage/ persistent- volumes# persistentvolumeclaims	false	v1.PersistentVolumeClaimVolumeSource	

Name	Description	Required	Schema	Default
rbd	RBD represents a Rados Block Device mount on the host that shares a pod's lifetime. More info: https://releases.k8s.io/HEAD/examples/volumes/rbd/README.md	false	v1.RBDVolumeSource	
flexVolume	FlexVolume represents a generic volume resource that is provisioned/attached using an exec based plugin.	false	v1.FlexVolumeSource	
cinder	Cinder represents a cinder volume attached and mounted on kubelets host machine More info: https://releases.k8s.io/HEAD/examples/mysql-cinder-pd/README.md	false	v1.CinderVolumeSource	

Name	Description	Required	Schema	Default
cephfs	CephFS represents a Ceph FS mount on the host that shares a pod's lifetime	false	v1.CephFSVolumeSource	
flocker	Flocker represents a Flocker volume attached to a kubelet's host machine. This depends on the Flocker control service being running	false	v1.FlockerVolumeSource	
downwardAPI	DownwardAPI represents downward API about the pod that should populate this volume	false	v1.DownwardAPIVolumeSource	
fc	FC represents a Fibre Channel resource that is attached to a kubelet's host machine and then exposed to the pod.	false	v1.FCVolumeSource	

Name	Description	Required	Schema	Default
azureFile	AzureFile represents an Azure File Service mount on the host and bind mount to the pod.	false	v1.AzureFileVolumeSource	
configMap	ConfigMap represents a configMap that should populate this volume	false	v1.ConfigMapVolumeSource	
vsphereVolume	VsphereVolume represents a vSphere volume attached and mounted on kubelets host machine	false	v1.VsphereVirtualDiskVolumeSource	
quobyte	Quobyte represents a Quobyte mount on the host that shares a pod's lifetime	false	v1.QuobyteVolumeSource	
azureDisk	AzureDisk represents an Azure Data Disk mount on the host and bind mount to the pod.	false	v1.AzureDiskVolumeSource	

Name	Description	Required	Schema	Default
photonPersistentDisk	PhotonPersistentDisk represents a PhotonController persistent disk attached and mounted on kubelets host machine	false	v1.PhotonPersistentDiskVolumeSource	
projected	Items for all in one resources secrets, configmaps, and downward API	false	v1.ProjectedVolumeSource	
portworxVolume	PortworxVolume represents a portworx volume attached and mounted on kubelets host machine	false	v1.PortworxVolumeSource	
scaleIO	ScaleIO represents a ScaleIO persistent volume attached and mounted on Kubernetes nodes.	false	v1.ScaleIOVolumeSource	
storageos	StorageOS represents a StorageOS volume attached and mounted on Kubernetes nodes.	false	v1.StorageOSVolumeSource	

v1.ResourceFieldSelector

ResourceFieldSelector represents container resources (cpu, memory) and their output format

Name	Description	Required	Schema	Default
containerName	Container name: required for volumes, optional for env vars	false	string	
resource	Required: resource to select	true	string	
divisor	Specifies the output format of the exposed resources, defaults to "1"	false	string	

v1.VolumeProjection

Projection that may be projected along with other supported volume types

Name	Description	Required	Schema	Default
secret	information about the secret data to project	false	v1.SecretProjection	
downwardAPI	information about the downwardAPI data to project	false	v1.DownwardAPIProjection	
configMap	information about the configMap data to project	false	v1.ConfigMapProjection	

v1.Probe

Probe describes a health check to be performed against a container to determine whether it is alive or ready to receive traffic.

Name	Description	Required	Schema	Default
exec	One and only one of the following should be specified. Exec specifies the action to take.	false	v1.ExecAction	
httpGet	HTTPGet specifies the http request to perform.	false	v1.HTTPGetAction	
tcpSocket	TCPSocket specifies an action involving a TCP port. TCP hooks not yet supported	false	v1.TCPSocketAction	
initialDelaySeconds	Number of seconds after the container has started before liveness probes are initiated. More info: https: //kubernetes. io/docs/ concepts/ workloads/ pods/pod-lifecycle# container-probes	false	integer (int32)	

Name	Description	Required	Schema	Default
timeoutSeconds	Number of seconds after which the probe times out. Defaults to 1 second. Minimum value is 1. More info: https: //kubernetes. io/docs/ concepts/ workloads/ pods/pod-lifecycle# container-probes	false	integer (int32)	
periodSeconds	How often (in seconds) to perform the probe. Default to 10 seconds. Minimum value is 1.	false	integer (int32)	
successThreshold	Minimum consecutive successes for the probe to be considered successful after having failed. Defaults to 1. Must be 1 for liveness. Minimum value is 1.	false	integer (int32)	

Name	Description	Required	Schema	Default
failureThreshold	Minimum consecutive failures for the probe to be considered failed after having succeeded. Defaults to 3. Minimum value is 1.	false	integer (int32)	

v1.WeightedPodAffinityTerm

The weights of all of the matched WeightedPodAffinityTerm fields are added per-node to find the most preferred node(s)

Name	Description	Required	Schema	Default
weight	weight associated with matching the corresponding podAffinityTerm, in the range 1-100.	true	integer (int32)	
podAffinityTerm	Required. A pod affinity term, associated with the corresponding weight.	true	v1.PodAffinityTerm	

v1beta1.DeploymentSpec

DeploymentSpec is the specification of the desired behavior of the Deployment.

Name	Description	Required	Schema	Default
replicas	Number of desired pods. This is a pointer to distinguish between explicit zero and not specified. Defaults to 1.	false	integer (int32)	
selector	Label selector for pods. Existing ReplicaSets whose pods are selected by this will be the ones affected by this deployment.	false	v1.LabelSelector	
template	Template describes the pods that will be created.	true	v1.PodTemplateSpec	
strategy	The deployment strategy to use to replace existing pods with new ones.	false	v1beta1.DeploymentStrategy	

Name	Description	Required	Schema	Default
minReadySeconds	Minimum number of seconds for which a newly created pod should be ready without any of its container crashing, for it to be considered available. Defaults to 0 (pod will be considered available as soon as it is ready)	false	integer (int32)	
revisionHistoryLimit	The number of old ReplicaSets to retain to allow rollback. This is a pointer to distinguish between explicit zero and not specified.	false	integer (int32)	
paused	Indicates that the deployment is paused and will not be processed by the deployment controller.	false	boolean	false

Name	Description	Required	Schema	Default
rollbackTo	DEPRECATED The config this deployment is rolling back to. Will be cleared after rollback is done.	false	v1beta1.RollbackConfig	

Name	Description	Required	Schema	Default
progressDeadlineSeconds	The maximum time in seconds for a deployment to make progress before it is considered to be failed. The deployment controller will continue to process failed deployments and a condition with a ProgressDeadlineExceeded reason will be surfaced in the deployment status. Note that progress will not be estimated during the time a deployment is paused. This is not set by default.	false	integer (int32)	

v1.SecretKeySelector

SecretKeySelector selects a key of a Secret.

365

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/ #names	false	string	
key	The key of the secret to select from. Must be a valid secret key.	true	string	
optional	Specify whether the Secret or it's key must be defined	false	boolean	false

v1.Capability

v1.DownwardAPIVolumeFile

DownwardAPIVolumeFile represents information to create the file containing the pod field

Name	Description	Required	Schema	Default
path	Required: Path is the relative path name of the file to be created. Must not be absolute or contain the .. path. Must be utf-8 encoded. The first item of the relative path must not start with ..	true	string	
fieldRef	Required: Selects a field of the pod: only annotations, labels, name and namespace are supported.	false	v1.ObjectFieldSelector	
resourceFieldRef	Selects a resource of the container: only resources limits and requests (limits.cpu, limits.memory, requests.cpu and requests.memory) are currently supported.	false	v1.ResourceFieldSelector	

Name	Description	Required	Schema	Default
mode	Optional: mode bits to use on this file, must be a value between 0 and 0777. If not specified, the volume defaultMode will be used. This might be in conflict with other options that affect the file mode, like fsGroup, and the result can be other mode bits set.	false	integer (int32)	

v1.PodSpec

PodSpec is a description of a pod.

Name	Description	Required	Schema	Default
volumes	List of volumes that can be mounted by containers belonging to the pod. More info: https://kubernetes.io/docs/concepts/storage/volumes	false	v1.Volume array	

Name	Description	Required	Schema	Default
initContainers	List of initialization containers belonging to the pod. Init containers are executed in order prior to containers being started. If any init container fails, the pod is considered to have failed and is handled according to its restartPolicy. The name for an init container or normal container must be unique among all containers. Init containers may not have Lifecycle actions, Readiness probes, or Liveness probes. The re-sourceRequire-ments of an init container are taken into account during scheduling by finding the highest request/limit for each resource type, and then using the max of of	false	v1.Container array	

Name	Description	Required	Schema	Default
containers	List of containers belonging to the pod. Containers cannot currently be added or removed. There must be at least one container in a Pod. Cannot be updated.	true	v1.Container array	
restartPolicy	Restart policy for all containers within the pod. One of Always, OnFailure, Never. Default to Always. More info: https: //kubernetes. io/docs/ concepts/ workloads/ pods/pod-lifecycle/ #restart-policy	false	string	

Name	Description	Required	Schema	Default
terminationGracePeriodSeconds	Optional duration in seconds the pod needs to terminate gracefully. May be decreased in delete request. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period will be used instead. The grace period is the duration in seconds after the processes running in the pod are sent a termination signal and the time when the processes are forcibly halted with a kill signal. Set this value longer than the expected cleanup time for your process. Defaults to 30 seconds.	false	integer (int64)	

Name	Description	Required	Schema	Default
activeDeadlineSeconds	Optional duration in seconds the pod may be active on the node relative to StartTime before the system will actively try to mark it failed and kill associated containers. Value must be a positive integer.	false	integer (int64)	

Name	Description	Required	Schema	Default
dnsPolicy	Set DNS policy for the pod. Defaults to "ClusterFirst". Valid values are *ClusterFirstWithHostNet*, *ClusterFirst*, *Default* or *None*. DNS parameters given in DNSConfig will be merged with the policy selected with DNSPolicy. To have DNS options set along with hostNetwork, you have to specify DNS policy explicitly to *ClusterFirstWithHostNet*. Note that *None* policy is an alpha feature introduced in v1.9 and CustomPodDNS feature gate must be enabled to use it.	false	string	

Name	Description	Required	Schema	Default
nodeSelector	NodeSelector is a selector which must be true for the pod to fit on a node. Selector which must match a node's labels for the pod to be scheduled on that node. More info: https://kubernetes.io/docs/concepts/configuration/assign-pod-node/	false	object	
serviceAccountName	ServiceAccountName is the name of the ServiceAccount to use to run this pod. More info: https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/	false	string	

Name	Description	Required	Schema	Default
serviceAccount	DeprecatedServiceAccount is a depreciated alias for ServiceAccountName. Deprecated: Use serviceAccountName instead.	false	string	
automountServiceAccountToken	AutomountServiceAccountToken indicates whether a service account token should be automatically mounted.	false	boolean	false
nodeName	NodeName is a request to schedule this pod onto a specific node. If it is non-empty, the scheduler simply schedules this pod onto that node, assuming that it fits resource requirements.	false	string	

Name	Description	Required	Schema	Default
hostNetwork	Host networking requested for this pod. Use the host's network namespace. If this option is set, the ports that will be used must be specified. Default to false.	false	boolean	false
hostPID	Use the host's pid namespace. Optional: Default to false.	false	boolean	false
hostIPC	Use the host's ipc namespace. Optional: Default to false.	false	boolean	false
securityContext	SecurityContext holds pod-level security attributes and common container settings. Optional: Defaults to empty. See type description for default values of each field.	false	v1.PodSecurityContext	

Name	Description	Required	Schema	Default
imagePullSecrets	ImagePullSecrets is an optional list of references to secrets in the same namespace to use for pulling any of the images used by this PodSpec. If specified, these secrets will be passed to individual puller implementations for them to use. For example, in the case of docker, only DockerConfig type secrets are honored. More info: https://kubernetes.io/docs/concepts/containers/images#specifying-imagepullsecrets-on-a-pod	false	v1.LocalObjectReference array	

Name	Description	Required	Schema	Default
hostname	Specifies the hostname of the Pod If not specified, the pod's hostname will be set to a system-defined value.	false	string	
subdomain	If specified, the fully qualified Pod hostname will be "<hostname>.<subdomain>.<pod namespace>.svc.<cluster domain>". If not specified, the pod will not have a domainname at all.	false	string	
affinity	If specified, the pod's scheduling constraints	false	v1.Affinity	
schedulerName	If specified, the pod will be dispatched by specified scheduler. If not specified, the pod will be dispatched by default scheduler.	false	string	
tolerations	If specified, the pod's tolerations.	false	v1.Toleration array	

Name	Description	Required	Schema	Default
hostAliases	HostAliases is an optional list of hosts and IPs that will be injected into the pod's hosts file if specified. This is only valid for non-hostNetwork pods.	false	v1.HostAlias array	
priorityClassName	If specified, indicates the pod's priority. "SYSTEM" is a special keyword which indicates the highest priority. Any other name must be defined by creating a PriorityClass object with that name. If not specified, the pod priority will be default or zero if there is no default.	false	string	

Name	Description	Required	Schema	Default
priority	The priority value. Various system components use this field to find the priority of the pod. When Priority Admission Controller is enabled, it prevents users from setting this field. The admission controller populates this field from PriorityClassName. The higher the value, the higher the priority.	false	integer (int32)	

Name	Description	Required	Schema	Default
dnsConfig	Specifies the DNS parameters of a pod. Parameters specified here will be merged to the generated DNS configuration based on DNSPolicy. This is an alpha feature introduced in v1.9 and CustomPodDNS feature gate must be enabled to use it.	false	v1.PodDNSConfig	

v1.ContainerPort

ContainerPort represents a network port in a single container.

Name	Description	Required	Schema	Default
name	If specified, this must be an IANA_SVC_NAME and unique within the pod. Each named port in a pod must have a unique name. Name for the port that can be referred to by services.	false	string	
hostPort	Number of port to expose on the host. If specified, this must be a valid port number, $0 < x < 65536$. If HostNetwork is specified, this must match ContainerPort. Most containers do not need this.	false	integer (int32)	
containerPort	Number of port to expose on the pod's IP address. This must be a valid port number, $0 < x < 65536$.	true	integer (int32)	

Name	Description	Required	Schema	Default
protocol	Protocol for port. Must be UDP or TCP. Defaults to "TCP".	false	string	
hostIP	What host IP to bind the external port to.	false	string	

v1.Lifecycle

Lifecycle describes actions that the management system should take in response to container lifecycle events. For the PostStart and PreStop lifecycle handlers, management of the container blocks until the action is complete, unless the container process fails, in which case the handler is aborted.

Name	Description	Required	Schema	Default
postStart	PostStart is called immediately after a container is created. If the handler fails, the container is terminated and restarted according to its restart policy. Other management of the container blocks until the hook completes. More info: https: //kubernetes. io/docs/ concepts/ containers/ container- lifecycle- hooks/ #container- hooks	false	v1.Handler	

Name	Description	Required	Schema	Default
preStop	PreStop is called immediately before a container is terminated. The container is terminated after the handler completes. The reason for termination is passed to the handler. Regardless of the outcome of the handler, the container is eventually terminated. Other management of the container blocks until the hook completes. More info: https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#container-hooks	false	v1.Handler	

v1.GlusterfsVolumeSource

Represents a Glusterfs mount that lasts the lifetime of a pod. Glusterfs volumes do not support ownership management or SELinux relabeling.

Name	Description	Required	Schema	Default
endpoints	EndpointsName is the endpoint name that details Glusterfs topology. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ glusterfs/ README. md#create- a-pod	true	string	
path	Path is the Glusterfs volume path. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/ glusterfs/ README. md#create- a-pod	true	string	

Name	Description	Required	Schema	Default
readOnly	ReadOnly here will force the Glusterfs volume to be mounted with read-only permissions. Defaults to false. More info: https://releases.k8s.io/HEAD/examples/volumes/glusterfs/README.md#create-a-pod	false	boolean	false

v1.Handler

Handler defines a specific action that should be taken

Name	Description	Required	Schema	Default
exec	One and only one of the following should be specified. Exec specifies the action to take.	false	v1.ExecAction	
httpGet	HTTPGet specifies the http request to perform.	false	v1.HTTPGetAction	

Name	Description	Required	Schema	Default
tcpSocket	TCPSocket specifies an action involving a TCP port. TCP hooks not yet supported	false	v1.TCPSocketAction	

v1.Toleration

The pod this Toleration is attached to tolerates any taint that matches the triple <key,value,effect> using the matching operator <operator>.

Name	Description	Required	Schema	Default
key	Key is the taint key that the toleration applies to. Empty means match all taint keys. If the key is empty, operator must be Exists; this combination means to match all values and all keys.	false	string	

Name	Description	Required	Schema	Default
operator	Operator represents a key's relationship to the value. Valid operators are Exists and Equal. Defaults to Equal. Exists is equivalent to wildcard for value, so that a pod can tolerate all taints of a particular category.	false	string	
value	Value is the taint value the toleration matches to. If the operator is Exists, the value should be empty, otherwise just a regular string.	false	string	

Name	Description	Required	Schema	Default
effect	Effect indicates the taint effect to match. Empty means match all taint effects. When specified, allowed values are NoSchedule, PreferNoSchedule and NoExecute.	false	string	
tolerationSeconds	TolerationSeconds represents the period of time the toleration (which must be of effect NoExecute, otherwise this field is ignored) tolerates the taint. By default, it is not set, which means tolerate the taint forever (do not evict). Zero and negative values will be treated as 0 (evict immediately) by the system.	false	integer (int64)	

v1beta1.IngressTLS

IngressTLS describes the transport layer security associated with an Ingress.

Name	Description	Required	Schema	Default
hosts	Hosts are a list of hosts included in the TLS certificate. The values in this list must match the name/s used in the tlsSecret. Defaults to the wildcard host setting for the loadbalancer controller fulfilling this Ingress, if left unspecified.	false	string array	

Name	Description	Required	Schema	Default
secretName	SecretName is the name of the secret used to terminate SSL traffic on 443. Field is left optional to allow SSL routing based on SNI hostname alone. If the SNI host in a listener conflicts with the "Host" header field used by an IngressRule, the SNI host is used for termination and value of the Host header is used for routing.	false	string	

v1.StatusCause

StatusCause provides more information about an api.Status failure, including cases when multiple errors are encountered.

Name	Description	Required	Schema	Default
reason	A machine-readable description of the cause of the error. If this value is empty there is no information available.	false	string	
message	A human-readable description of the cause of the error. This field may be presented as-is to a reader.	false	string	

Name	Description	Required	Schema	Default
field	The field of the resource that has caused this error, as named by its JSON serialization. May include dot and postfix notation for nested attributes. Arrays are zero-indexed. Fields may appear more than once in an array of causes due to fields having multiple errors. Optional. Examples: "name" - the field "name" on the current resource "items[0].name" - the field "name" on the first array entry in "items"	false	string	

v1beta1.Scale

represents a scaling request for a resource.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard object metadata; More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata.	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	defines the behavior of the scale. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#spec- and-status.	false	v1beta1.ScaleSpec	
status	current status of the scale. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#spec- and-status. Read-only.	false	v1beta1.ScaleStatus	

v1.RBDVolumeSource

Represents a Rados Block Device mount that lasts the lifetime of a pod. RBD volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
monitors	A collection of Ceph monitors. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/rbd/ README. md#how-to- use-it	true	string array	

Name	Description	Required	Schema	Default
image	The rados image name. More info: https:// releases.k8s. io/HEAD/ examples/ volumes/rbd/ README. md#how-to-use-it	true	string	
fsType	Filesystem type of the volume that you want to mount. Tip: Ensure that the filesystem type is supported by the host operating system. Examples: "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes#rbd	false	string	

Name	Description	Required	Schema	Default
pool	The rados pool name. Default is rbd. More info: https://releases.k8s.io/HEAD/examples/volumes/rbd/README.md#how-to-use-it	false	string	
user	The rados user name. Default is admin. More info: https://releases.k8s.io/HEAD/examples/volumes/rbd/README.md#how-to-use-it	false	string	
keyring	Keyring is the path to key ring for RBDUser. Default is /etc/ceph/keyring. More info: https://releases.k8s.io/HEAD/examples/volumes/rbd/README.md#how-to-use-it	false	string	

Name	Description	Required	Schema	Default
secretRef	SecretRef is name of the authentication secret for RBDUser. If provided overrides keyring. Default is nil. More info: https://releases.k8s.io/HEAD/examples/volumes/rbd/README.md#how-to-use-it	false	v1.LocalObjectReference	
readOnly	ReadOnly here will force the ReadOnly setting in VolumeMounts. Defaults to false. More info: https://releases.k8s.io/HEAD/examples/volumes/rbd/README.md#how-to-use-it	false	boolean	false

v1.ConfigMapProjection

Adapts a ConfigMap into a projected volume.

The contents of the target ConfigMap's Data field will be presented in a projected volume as files using the keys in the Data field as the file names, unless the items element is populated with specific mappings of keys to paths. Note

that this is identical to a configmap volume source without the default mode.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/ #names	false	string	

Name	Description	Required	Schema	Default
items	If unspecified, each key-value pair in the Data field of the referenced ConfigMap will be projected into the volume as a file whose name is the key and content is the value. If specified, the listed keys will be projected into the specified paths, and unlisted keys will not be present. If a key is specified which is not present in the ConfigMap, the volume setup will error unless it is marked optional. Paths must be relative and may not contain the .. path or start with ...	false	v1.KeyToPath array	

Name	Description	Required	Schema	Default
optional	Specify whether the ConfigMap or it's keys must be defined	false	boolean	false

v1.PhotonPersistentDiskVolumeSource

Represents a Photon Controller persistent disk resource.

Name	Description	Required	Schema	Default
pdID	ID that identifies Photon Controller persistent disk	true	string	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified.	false	string	

v1.ScaleIOVolumeSource

ScaleIOVolumeSource represents a persistent ScaleIO volume

Name	Description	Required	Schema	Default
gateway	The host address of the ScaleIO API Gateway.	true	string	
system	The name of the storage system as configured in ScaleIO.	true	string	
secretRef	SecretRef references to the secret for ScaleIO user and other sensitive information. If this is not provided, Login operation will fail.	true	v1.LocalObjectReference	
sslEnabled	Flag to enable/disable SSL communication with Gateway, default false	false	boolean	false
protectionDomain	The name of the ScaleIO Protection Domain for the configured storage.	false	string	
storagePool	The ScaleIO Storage Pool associated with the protection domain.	false	string	

Name	Description	Required	Schema	Default
storageMode	Indicates whether the storage for a volume should be ThickProvisioned or ThinProvisioned.	false	string	
volumeName	The name of a volume already created in the ScaleIO system that is associated with this volume source.	false	string	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified.	false	string	
readOnly	Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false

v1.HostPathType

v1.Initializers

Initializers tracks the progress of initialization.

Name	Description	Required	Schema	Default
pending	Pending is a list of initializers that must execute in order before this object is visible. When the last pending initializer is removed, and no failing result is set, the initializers struct will be set to nil and the object is considered as initialized and visible to all clients.	true	v1.Initializer array	
result	If result is set with the Failure field, the object will be persisted to storage and then deleted, ensuring that other clients can observe the deletion.	false	v1.Status	

v1.Status

Status is a return value for calls that don't return other objects.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
status	Status of the operation. One of: "Success" or "Failure". More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	string	
message	A human-readable description of the status of this operation.	false	string	
reason	A machine-readable description of why this operation is in the "Failure" status. If this value is empty there is no information available. A Reason clarifies an HTTP status code but does not override it.	false	string	

Name	Description	Required	Schema	Default
details	Extended data associated with the reason. Each reason may define its own extended details. This field is optional and the data returned is not guaranteed to conform to any schema except that defined by the reason type.	false	v1.StatusDetails	
code	Suggested HTTP return code for this status, 0 if not set.	false	integer (int32)	

v1.PodDNSConfig

PodDNSConfig defines the DNS parameters of a pod in addition to those generated from DNSPolicy.

Name	Description	Required	Schema	Default
nameservers	A list of DNS name server IP addresses. This will be appended to the base nameservers generated from DNSPolicy. Duplicated nameservers will be removed.	false	string array	
searches	A list of DNS search domains for host-name lookup. This will be appended to the base search paths generated from DNSPolicy. Duplicated search paths will be removed.	false	string array	

Name	Description	Required	Schema	Default
options	A list of DNS resolver options. This will be merged with the base options generated from DNSPolicy. Duplicated entries will be removed. Resolution options given in Options will override those that appear in the base DNSPolicy.	false	v1.PodDNSConfigOption array	

v1beta1.ScaleStatus

represents the current status of a scale subresource.

Name	Description	Required	Schema	Default
replicas	actual number of observed instances of the scaled object.	true	integer (int32)	

Name	Description	Required	Schema	Default
selector	label query over pods that should match the replicas count. More info: http://kubernetes.io/docs/user-guide/labels#label-selectors	false	object	

Name	Description	Required	Schema	Default
targetSelector	label selector for pods that should match the replicas count. This is a serialized version of both map-based and more expressive set-based selectors. This is done to avoid introspection in the clients. The string will be in the same format as the query-param syntax. If the target type only supports map-based selectors, both this field and map-based selector field are populated. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ labels/ #label-selectors	false	string	

Name	Description	Required	Schema	Default

v1.NFSVolumeSource

Represents an NFS mount that lasts the lifetime of a pod. NFS volumes do not support ownership management or SELinux relabeling.

Name	Description	Required	Schema	Default
server	Server is the hostname or IP address of the NFS server. More info: https://kubernetes.io/docs/concepts/storage/volumes#nfs	true	string	
path	Path that is exported by the NFS server. More info: https://kubernetes.io/docs/concepts/storage/volumes#nfs	true	string	

Name	Description	Required	Schema	Default
readOnly	ReadOnly here will force the NFS export to be mounted with read-only permissions. Defaults to false. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes#nfs	false	boolean	false

v1beta1.DeploymentList

DeploymentList is a list of Deployments.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata.	false	v1.ListMeta	
items	Items is the list of Deployments.	true	v1beta1.Deployment array	

v1beta1.DeploymentRollback

DEPRECATED. DeploymentRollback stores the information required to rollback a deployment.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen- tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md# resources	false	string	
name	Required: This must match the Name of a deployment.	true	string	
updatedAnnotations	The annotations to be updated to a deployment	false	object	
rollbackTo	The config of this deployment rollback.	true	v1beta1.RollbackConfig	

v1.HTTPHeader

HTTPHeader describes a custom header to be used in HTTP probes

Name	Description	Required	Schema	Default
name	The header field name	true	string	
value	The header field value	true	string	

v1.FCVolumeSource

Represents a Fibre Channel volume. Fibre Channel volumes can only be mounted as read/write once. Fibre Channel volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
targetWWNs	Optional: FC target worldwide names (WWNs)	false	string array	
lun	Optional: FC target lun number	false	integer (int32)	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified.	false	string	

Name	Description	Required	Schema	Default
readOnly	Optional: Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false
wwids	Optional: FC volume world wide identifiers (wwids) Either wwids or combination of targetWWNs and lun must be set, but not both simultaneously.	false	string array	

v1.PodAntiAffinity

Pod anti affinity is a group of inter pod anti affinity scheduling rules.

Name	Description	Required	Schema	Default
requiredDuringSchedulingIgnoredDuringExecution	If the anti-affinity requirements specified by this field are not met at scheduling time, the pod will not be scheduled onto the node. If the anti-affinity requirements specified by this field cease to be met at some point during pod execution (e.g. due to a pod label update), the system may or may not try to eventually evict the pod from its node. When there are multiple elements, the lists of nodes corresponding to each podAffinityTerm are intersected, i.e. all terms must be satisfied.	false	v1.PodAffinityTerm array	

Name	Description	Required	Schema	Default
preferredDuringSchedulingIgnoredDuringExecution	The scheduler will prefer to schedule pods to nodes that satisfy the anti-affinity expressions specified by this field, but it may choose a node that violates one or more of the expressions. The node that is most preferred is the one with the greatest sum of weights, i.e. for each node that meets all of the scheduling requirements (resource request, requiredDuringScheduling anti-affinity expressions, etc.), compute a sum by iterating through the elements of this field and adding "weight" to the sum if the node has pods which matches the corresponding podAffinityTerm; the	false	v1.WeightedPodAffinityTerm array	

424

Name	Description	Required	Schema	Default

v1.DeletionPropagation

v1beta1.DeploymentStrategy

DeploymentStrategy describes how to replace existing pods with new ones.

Name	Description	Required	Schema	Default
type	Type of deployment. Can be "Recreate" or "RollingUpdate". Default is RollingUpdate.	false	string	
rollingUpdate	Rolling update config params. Present only if DeploymentStrategyType = RollingUpdate.	false	v1beta1.RollingUpdateDeployment	

v1.TCPSocketAction

TCPSocketAction describes an action based on opening a socket

Name	Description	Required	Schema	Default
port	Number or name of the port to access on the container. Number must be in the range 1 to 65535. Name must be an IANA_SVC_NAME.	true	string	
host	Optional: Host name to connect to, defaults to the pod IP.	false	string	

v1beta1.IngressRule

IngressRule represents the rules mapping the paths under a specified host to the related backend services. Incoming requests are first evaluated for a host match, then routed to the backend associated with the matching IngressRuleValue.

Name	Description	Required	Schema	Default
host	Host is the fully qualified domain name of a network host, as defined by RFC 3986. Note the following deviations from the "host" part of the URI as defined in the RFC: 1. IPs are not allowed. Currently an IngressRule-Value can only apply to the IP in the Spec of the parent Ingress. 2. The : delimiter is not respected because ports are not allowed. Currently the port of an Ingress is implicitly :80 for http and :443 for https. Both these may change in the future. Incoming requests are matched against the host before the Ingress-RuleValue. If the host is unspecified, the Ingress routes all	false	string	

Name	Description	Required	Schema	Default
http		false	v1beta1.HTTPIngressRuleValue	

v1.HTTPGetAction

HTTPGetAction describes an action based on HTTP Get requests.

Name	Description	Required	Schema	Default
path	Path to access on the HTTP server.	false	string	
port	Name or number of the port to access on the container. Number must be in the range 1 to 65535. Name must be an IANA_SVC_NAME.	true	string	
host	Host name to connect to, defaults to the pod IP. You probably want to set "Host" in httpHeaders instead.	false	string	
scheme	Scheme to use for connecting to the host. Defaults to HTTP.	false	string	

Name	Description	Required	Schema	Default
httpHeaders	Custom headers to set in the request. HTTP allows repeated headers.	false	v1.HTTPHeader array	

v1.StatusDetails

StatusDetails is a set of additional properties that MAY be set by the server to provide additional information about a response. The Reason field of a Status object defines what attributes will be set. Clients must ignore fields that do not match the defined type of each attribute, and should assume that any attribute may be empty, invalid, or under defined.

Name	Description	Required	Schema	Default
name	The name attribute of the resource associated with the status StatusReason (when there is a single name which can be described).	false	string	
group	The group attribute of the resource associated with the status StatusReason.	false	string	

Name	Description	Required	Schema	Default
kind	The kind attribute of the resource associated with the status StatusReason. On some operations may differ from the requested resource Kind. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	
uid	UID of the resource. (when there is a single resource which can be described). More info: http: //kubernetes. io/docs/user-guide/ identifiers# uids	false	string	

Name	Description	Required	Schema	Default
causes	The Causes array includes more details associated with the StatusReason failure. Not all Status-Reasons may provide detailed causes.	false	v1.StatusCause array	
retryAfterSeconds	If specified, the time in seconds before the operation should be retried. Some errors may indicate the client must take an alternate action - for those errors this field may indicate how long to wait before taking the alternate action.	false	integer (int32)	

v1.LoadBalancerStatus

LoadBalancerStatus represents the status of a load-balancer.

Name	Description	Required	Schema	Default
ingress	Ingress is a list containing ingress points for the load-balancer. Traffic intended for the service should be sent to these ingress points.	false	v1.LoadBalancerIngress array	

v1.Container

A single application container that you want to run within a pod.

Name	Description	Required	Schema	Default
name	Name of the container specified as a DNS_LABEL. Each container in a pod must have a unique name (DNS_LABEL). Cannot be updated.	true	string	

Name	Description	Required	Schema	Default
image	Docker image name. More info: https: //kubernetes. io/docs/ concepts/ containers/ images This field is optional to allow higher level config management to default or override container images in workload controllers like Deployments and StatefulSets.	false	string	

Name	Description	Required	Schema	Default
command	Entrypoint array. Not executed within a shell. The docker image's ENTRYPOINT is used if this is not provided. Variable references $(VAR_NAME) are expanded using the container's environment. If a variable cannot be resolved, the reference in the input string will be unchanged. The $(VAR_NAME) syntax can be escaped with a double $$, ie: $$(VAR_NAME). Escaped references will never be expanded, regardless of whether the variable exists or not. Cannot be updated. More info: https: //kubernetes. io/docs/ tasks/inject- data- application/ define- command- argument- container/ #running-a- command-in-	false	string array	

434

Name	Description	Required	Schema	Default
args	Arguments to the entrypoint. The docker image's CMD is used if this is not provided. Variable references $(VAR_NAME) are expanded using the container's environment. If a variable cannot be resolved, the reference in the input string will be unchanged. The $(VAR_NAME) syntax can be escaped with a double $$, ie: $$(VAR_NAME). Escaped references will never be expanded, regardless of whether the variable exists or not. Cannot be updated. More info: https://kubernetes.io/docs/tasks/inject-data-application/define-command-argument-container/#running-a-command-in-a-shell	false	string array	

Name	Description	Required	Schema	Default
workingDir	Container's working directory. If not specified, the container runtime's default will be used, which might be configured in the container image. Cannot be updated.	false	string	

Name	Description	Required	Schema	Default
ports	List of ports to expose from the container. Exposing a port here gives the system additional information about the network connections a container uses, but is primarily informational. Not specifying a port here DOES NOT prevent that port from being exposed. Any port which is listening on the default "0.0.0.0" address inside a container will be accessible from the network. Cannot be updated.	false	v1.ContainerPort array	

Name	Description	Required	Schema	Default
envFrom	List of sources to populate environment variables in the container. The keys defined within a source must be a C_IDENTIFIER. All invalid keys will be reported as an event when the container is starting. When a key exists in multiple sources, the value associated with the last source will take precedence. Values defined by an Env with a duplicate key will take precedence. Cannot be updated.	false	v1.EnvFromSource array	
env	List of environment variables to set in the container. Cannot be updated.	false	v1.EnvVar array	

Name	Description	Required	Schema	Default
resources	Compute Resources required by this container. Cannot be updated. More info: https: //kubernetes. io/docs/ concepts/ storage/ persistent-volumes# resources	false	v1.ResourceRequirements	
volumeMounts	Pod volumes to mount into the container's filesystem. Cannot be updated.	false	v1.VolumeMount array	
volumeDevices	volumeDevices is the list of block devices to be used by the container. This is an alpha feature and may change in the future.	false	v1.VolumeDevice array	

Name	Description	Required	Schema	Default
livenessProbe	Periodic probe of container liveness. Container will be restarted if the probe fails. Cannot be updated. More info: https: //kubernetes. io/docs/ concepts/ workloads/ pods/pod- lifecycle# container- probes	false	v1.Probe	
readinessProbe	Periodic probe of container service readiness. Container will be removed from service endpoints if the probe fails. Cannot be updated. More info: https: //kubernetes. io/docs/ concepts/ workloads/ pods/pod- lifecycle# container- probes	false	v1.Probe	

Name	Description	Required	Schema	Default
lifecycle	Actions that the management system should take in response to container lifecycle events. Cannot be updated.	false	v1.Lifecycle	

Name	Description	Required	Schema	Default
terminationMessagePath	Optional: Path at which the file to which the container's termination message will be written is mounted into the container's filesystem. Message written is intended to be brief final status, such as an assertion failure message. Will be truncated by the node if greater than 4096 bytes. The total message length across all containers will be limited to 12kb. Defaults to /dev/termination-log. Cannot be updated.	false	string	

Name	Description	Required	Schema	Default
terminationMessagePolicy	Indicate how the termination message should be populated. File will use the contents of termination-MessagePath to populate the container status message on both success and failure. Fallback-ToLogsOn-Error will use the last chunk of container log output if the termination message file is empty and the container exited with an error. The log output is limited to 2048 bytes or 80 lines, whichever is smaller. Defaults to File. Cannot be updated.	false	string	

Name	Description	Required	Schema	Default
imagePullPolicy	Image pull policy. One of Always, Never, IfNotPresent. Defaults to Always if :latest tag is specified, or IfNotPresent otherwise. Cannot be updated. More info: https: //kubernetes. io/docs/ concepts/ containers/ images# updating- images	false	string	
securityContext	Security options the pod should run with. More info: https: //kubernetes. io/docs/ concepts/ policy/ security- context/ More info: https: //kubernetes. io/docs/ tasks/ configure- pod- container/ security- context/	false	v1.SecurityContext	

Name	Description	Required	Schema	Default
stdin	Whether this container should allocate a buffer for stdin in the container runtime. If this is not set, reads from stdin in the container will always result in EOF. Default is false.	false	boolean	false

Name	Description	Required	Schema	Default
stdinOnce	Whether the container runtime should close the stdin channel after it has been opened by a single attach. When stdin is true the stdin stream will remain open across multiple attach sessions. If stdinOnce is set to true, stdin is opened on container start, is empty until the first client attaches to stdin, and then remains open and accepts data until the client disconnects, at which time stdin is closed and remains closed until the container is restarted. If this flag is false, a container processes that reads from stdin will never receive an EOF. Default is false	false	boolean	false

Name	Description	Required	Schema	Default
tty	Whether this container should allocate a TTY for itself, also requires *stdin* to be true. Default is false.	false	boolean	false

v1.PodSecurityContext

PodSecurityContext holds pod-level security attributes and common container settings. Some fields are also present in container.securityContext. Field values of container.securityContext take precedence over field values of PodSecurity-Context.

Name	Description	Required	Schema	Default
seLinuxOptions	The SELinux context to be applied to all containers. If unspecified, the container runtime will allocate a random SELinux context for each container. May also be set in SecurityContext. If set in both SecurityContext and PodSecurityContext, the value specified in SecurityContext takes precedence for that container.	false	v1.SELinuxOptions	

Name	Description	Required	Schema	Default
runAsUser	The UID to run the entrypoint of the container process. Defaults to user specified in image metadata if unspecified. May also be set in SecurityContext. If set in both SecurityContext and PodSecurityContext, the value specified in SecurityContext takes precedence for that container.	false	integer (int64)	

Name	Description	Required	Schema	Default
runAsNonRoot	Indicates that the container must run as a non-root user. If true, the Kubelet will validate the image at runtime to ensure that it does not run as UID 0 (root) and fail to start the container if it does. If unset or false, no such validation will be performed. May also be set in SecurityContext. If set in both SecurityContext and PodSecurityContext, the value specified in SecurityContext takes precedence.	false	boolean	false

Name	Description	Required	Schema	Default
supplementalGroups	A list of groups applied to the first process run in each container, in addition to the container's primary GID. If unspecified, no groups will be added to any container.	false	integer (int32) array	

Name	Description	Required	Schema	Default
fsGroup	A special supplemental group that applies to all containers in a pod. Some volume types allow the Kubelet to change the ownership of that volume to be owned by the pod: 1. The owning GID will be the FSGroup 2. The setgid bit is set (new files created in the volume will be owned by FSGroup) 3. The permission bits are OR'd with rw-rw	false	integer (int64)	

v1.OwnerReference

OwnerReference contains enough information to let you identify an owning object. Currently, an owning object must be in the same namespace, so there is no namespace field.

Name	Description	Required	Schema	Default
apiVersion	API version of the referent.	true	string	

Name	Description	Required	Schema	Default
kind	Kind of the referent. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	true	string	
name	Name of the referent. More info: http: //kubernetes. io/docs/user- guide/ identifiers# names	true	string	
uid	UID of the referent. More info: http: //kubernetes. io/docs/user- guide/ identifiers# uids	true	string	
controller	If true, this reference points to the managing controller.	false	boolean	false

Name	Description	Required	Schema	Default
blockOwnerDeletion	If true, AND if the owner has the "foreground-Deletion" finalizer, then the owner cannot be deleted from the key-value store until this reference is removed. Defaults to false. To set this field, a user needs "delete" permission of the owner, otherwise 422 (Unprocessable Entity) will be returned.	false	boolean	false

v1beta1.ReplicaSetStatus

ReplicaSetStatus represents the current status of a ReplicaSet.

Name	Description	Required	Schema	Default
replicas	Replicas is the most recently oberved number of replicas. More info: https://kubernetes.io/docs/concepts/workloads/controllers/replicationcontroller/#what-is-a-replicationcontroller	true	integer (int32)	
fullyLabeledReplicas	The number of pods that have labels matching the labels of the pod template of the replicaset.	false	integer (int32)	
readyReplicas	The number of ready replicas for this replica set.	false	integer (int32)	
availableReplicas	The number of available replicas (ready for at least min-ReadySeconds) for this replica set.	false	integer (int32)	
observedGeneration	ObservedGeneration reflects the generation of the most recently observed ReplicaSet.	false	integer (int64)	

Name	Description	Required	Schema	Default
conditions	Represents the latest available observations of a replica set's current state.	false	v1beta1.ReplicaSetCondition array	

v1.APIResource

APIResource specifies the name of a resource and whether it is namespaced.

Name	Description	Required	Schema	Default
name	name is the plural name of the resource.	true	string	
singularName	singularName is the singular name of the resource. This allows clients to handle plural and singular opaquely. The singularName is more correct for reporting status on a single item and both singular and plural are allowed from the kubectl CLI interface.	true	string	

Name	Description	Required	Schema	Default
namespaced	namespaced indicates if a resource is namespaced or not.	true	boolean	false
group	group is the preferred group of the resource. Empty implies the group of the containing resource list. For subresources, this may have a different value, for example: Scale".	false	string	
version	version is the preferred version of the resource. Empty implies the version of the containing resource list For subresources, this may have a different value, for example: v1 (while inside a v1beta1 version of the core resource's group)".	false	string	

Name	Description	Required	Schema	Default
kind	kind is the kind for the resource (e.g. *Foo* is the kind for a resource *foo*)	true	string	
verbs	verbs is a list of supported kube verbs (this includes get, list, watch, create, update, patch, delete, deletecollection, and proxy)	true	string array	
shortNames	shortNames is a list of suggested short names of the resource.	false	string array	
categories	categories is a list of the grouped resources this resource belongs to (e.g. *all*)	false	string array	

v1.VolumeDevice

volumeDevice describes a mapping of a raw block device within a container.

Name	Description	Required	Schema	Default
name	name must match the name of a persistentVolumeClaim in the pod	true	string	

Name	Description	Required	Schema	Default
devicePath	devicePath is the path inside of the container that the device will be mapped to.	true	string	

v1.NodeSelectorRequirement

A node selector requirement is a selector that contains values, a key, and an operator that relates the key and values.

Name	Description	Required	Schema	Default
key	The label key that the selector applies to.	true	string	
operator	Represents a key's relationship to a set of values. Valid operators are In, NotIn, Exists, DoesNotExist. Gt, and Lt.	true	string	

Name	Description	Required	Schema	Default
values	An array of string values. If the operator is In or NotIn, the values array must be non-empty. If the operator is Exists or DoesNotExist, the values array must be empty. If the operator is Gt or Lt, the values array must have a single element, which will be interpreted as an integer. This array is replaced during a strategic merge patch.	false	string array	

v1beta1.ReplicaSet

DEPRECATED - This group version of ReplicaSet is deprecated by apps/v1beta2/ReplicaSet. See the release notes for more information. ReplicaSet ensures that a specified number of pod replicas are running at any given time.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	

Name	Description	Required	Schema	Default
metadata	If the Labels of a ReplicaSet are empty, they are defaulted to be the same as the Pod(s) that the ReplicaSet manages. Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	
spec	Spec defines the specification of the desired behavior of the ReplicaSet. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#spec-and-status	false	v1beta1.ReplicaSetSpec	

Name	Description	Required	Schema	Default
status	Status is the most recently observed status of the ReplicaSet. This data may be out of date by some window of time. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1beta1.ReplicaSetStatus	

v1.HostPathVolumeSource

Represents a host path mapped into a pod. Host path volumes do not support ownership management or SELinux relabeling.

Name	Description	Required	Schema	Default
path	Path of the directory on the host. If the path is a symlink, it will follow the link to the real path. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# hostpath	true	string	
type	Type for HostPath Volume Defaults to "" More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# hostpath	false	v1.HostPathType	

v1.SecretProjection

Adapts a secret into a projected volume.

The contents of the target Secret's Data field will be presented in a projected volume as files using the keys in the Data field as the file names. Note that this is identical to a secret volume source without the default mode.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working-with-objects/ names/ #names	false	string	

Name	Description	Required	Schema	Default
items	If unspecified, each key-value pair in the Data field of the referenced Secret will be projected into the volume as a file whose name is the key and content is the value. If specified, the listed keys will be projected into the specified paths, and unlisted keys will not be present. If a key is specified which is not present in the Secret, the volume setup will error unless it is marked optional. Paths must be relative and may not contain the .. path or start with ...	false	v1.KeyToPath array	

Name	Description	Required	Schema	Default
optional	Specify whether the Secret or its key must be defined	false	boolean	false

v1.PodDNSConfigOption

PodDNSConfigOption defines DNS resolver options of a pod.

Name	Description	Required	Schema	Default
name	Required.	false	string	
value		false	string	

v1beta1.DaemonSet

DEPRECATED - This group version of DaemonSet is deprecated by apps/v1beta2/DaemonSet. See the release notes for more information. DaemonSet represents the configuration of a daemon set.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard object's metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	The desired behavior of this daemon set. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1beta1.DaemonSetSpec	
status	The current status of this daemon set. This data may be out of date by some window of time. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1beta1.DaemonSetStatus	

v1.CinderVolumeSource

Represents a cinder volume resource in Openstack. A Cinder volume must exist before mounting to a container. The volume must also be in the same region as the kubelet. Cinder volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
volumeID	volume id used to identify the volume in cinder More info: https://releases.k8s.io/HEAD/examples/mysql-cinder-pd/README.md	true	string	
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Examples: "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified. More info: https://releases.k8s.io/HEAD/examples/mysql-cinder-pd/README.md	false	string	

Name	Description	Required	Schema	Default
readOnly	Optional: Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts. More info: https:// releases.k8s. io/HEAD/ examples/ mysql-cinder-pd/ README. md	false	boolean	false

v1.SecurityContext

SecurityContext holds security configuration that will be applied to a container. Some fields are present in both SecurityContext and PodSecurityContext. When both are set, the values in SecurityContext take precedence.

Name	Description	Required	Schema	Default
capabilities	The capabilities to add/drop when running containers. Defaults to the default set of capabilities granted by the container runtime.	false	v1.Capabilities	

473

Name	Description	Required	Schema	Default
privileged	Run container in privileged mode. Processes in privileged containers are essentially equivalent to root on the host. Defaults to false.	false	boolean	false
seLinuxOptions	The SELinux context to be applied to the container. If unspecified, the container runtime will allocate a random SELinux context for each container. May also be set in PodSecurity-Context. If set in both SecurityContext and PodSecurity-Context, the value specified in SecurityContext takes precedence.	false	v1.SELinuxOptions	

Name	Description	Required	Schema	Default
runAsUser	The UID to run the entrypoint of the container process. Defaults to user specified in image metadata if unspecified. May also be set in PodSecurity-Context. If set in both SecurityContext and PodSecurity-Context, the value specified in SecurityContext takes precedence.	false	integer (int64)	

Name	Description	Required	Schema	Default
runAsNonRoot	Indicates that the container must run as a non-root user. If true, the Kubelet will validate the image at runtime to ensure that it does not run as UID 0 (root) and fail to start the container if it does. If unset or false, no such validation will be performed. May also be set in PodSecurity-Context. If set in both SecurityCon-text and PodSecurity-Context, the value specified in SecurityCon-text takes precedence.	false	boolean	false
readOnlyRootFilesystem	Whether this container has a read-only root filesystem. Default is false.	false	boolean	false

Name	Description	Required	Schema	Default
allowPrivilegeEscalation	AllowPrivilegeEscalation controls whether a process can gain more privileges than its parent process. This bool directly controls if the no_new_privs flag will be set on the container process. AllowPrivilegeEscalation is true always when the container is: 1) run as Privileged 2) has CAP_SYS_ADMIN	false	boolean	false

v1.AWSElasticBlockStoreVolumeSource

Represents a Persistent Disk resource in AWS.

An AWS EBS disk must exist before mounting to a container. The disk must also be in the same AWS zone as the kubelet. An AWS EBS disk can only be mounted as read/write once. AWS EBS volumes support ownership management and SELinux relabeling.

Name	Description	Required	Schema	Default
volumeID	Unique ID of the persistent disk resource in AWS (Amazon EBS volume). More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# awselasticblockstore	true	string	
fsType	Filesystem type of the volume that you want to mount. Tip: Ensure that the filesystem type is supported by the host operating system. Examples: "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified. More info: https: //kubernetes. io/docs/ concepts/ storage/ volumes# awselasticblockstore	false	string	

Name	Description	Required	Schema	Default
partition	The partition in the volume that you want to mount. If omitted, the default is to mount by volume name. Examples: For volume /dev/sda1, you specify the partition as "1". Similarly, the volume partition for /dev/sda is "0" (or you can leave the property empty).	false	integer (int32)	
readOnly	Specify "true" to force and set the ReadOnly property in VolumeMounts to "true". If omitted, the default is "false". More info: https://kubernetes.io/docs/concepts/storage/volumes#awselasticblockstore	false	boolean	false

v1.QuobyteVolumeSource

Represents a Quobyte mount that lasts the lifetime of a pod. Quobyte volumes do not support ownership management or SELinux relabeling.

Name	Description	Required	Schema	Default
registry	Registry represents a single or multiple Quobyte Registry services specified as a string as host:port pair (multiple entries are separated with commas) which acts as the central registry for volumes	true	string	
volume	Volume is a string that references an already created Quobyte volume by name.	true	string	
readOnly	ReadOnly here will force the Quobyte volume to be mounted with read-only permissions. Defaults to false.	false	boolean	false

Name	Description	Required	Schema	Default
user	User to map volume access to Defaults to serivceaccount user	false	string	
group	Group to map volume access to Default is no group	false	string	

v1.WatchEvent

Name	Description	Required	Schema	Default
type		true	string	
object		true	string	

v1.LabelSelectorRequirement

A label selector requirement is a selector that contains values, a key, and an operator that relates the key and values.

Name	Description	Required	Schema	Default
key	key is the label key that the selector applies to.	true	string	
operator	operator represents a key's relationship to a set of values. Valid operators are In, NotIn, Exists and DoesNotExist.	true	string	

Name	Description	Required	Schema	Default
values	values is an array of string values. If the operator is In or NotIn, the values array must be non-empty. If the operator is Exists or DoesNotExist, the values array must be empty. This array is replaced during a strategic merge patch.	false	string array	

v1.EnvVar

EnvVar represents an environment variable present in a Container.

Name	Description	Required	Schema	Default
name	Name of the environment variable. Must be a C_IDENTIFIER.	true	string	

Name	Description	Required	Schema	Default
value	Variable references $(VAR_NAME) are expanded using the previous defined environment variables in the container and any service environment variables. If a variable cannot be resolved, the reference in the input string will be unchanged. The $(VAR_NAME) syntax can be escaped with a double $$, ie: $$(VAR_NAME). Escaped references will never be expanded, regardless of whether the variable exists or not. Defaults to "".	false	string	

Name	Description	Required	Schema	Default
valueFrom	Source for the environment variable's value. Cannot be used if value is not empty.	false	v1.EnvVarSource	

v1.ResourceRequirements

ResourceRequirements describes the compute resource requirements.

Name	Description	Required	Schema	Default
limits	Limits describes the maximum amount of compute resources allowed. More info: https://kubernetes.io/docs/concepts/configuration/manage-compute-resources-container/	false	object	

484

Name	Description	Required	Schema	Default
requests	Requests describes the minimum amount of compute resources required. If Requests is omitted for a container, it defaults to Limits if that is explicitly specified, otherwise to an implementation-defined value. More info: https: //kubernetes. io/docs/ concepts/ configuration/ manage-compute-resources-container/	false	object	

v1.HostAlias

HostAlias holds the mapping between IP and hostnames that will be injected as an entry in the pod's hosts file.

Name	Description	Required	Schema	Default
ip	IP address of the host file entry.	false	string	
hostnames	Hostnames for the above IP address.	false	string array	

v1.PodTemplateSpec

PodTemplateSpec describes the data a pod should have when created from a template

Name	Description	Required	Schema	Default
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	
spec	Specification of the desired behavior of the pod. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#spec-and-status	false	v1.PodSpec	

v1.NodeSelector

A node selector represents the union of the results of one or more label queries over a set of nodes; that is, it represents the OR of the selectors represented by the node selector terms.

Name	Description	Required	Schema	Default
nodeSelectorTerms	Required. A list of node selector terms. The terms are ORed.	true	v1.NodeSelectorTerm array	

v1.Patch

Patch is provided to give a concrete name and type to the Kubernetes PATCH request body.

v1beta1.DeploymentCondition

DeploymentCondition describes the state of a deployment at a certain point.

Name	Description	Required	Schema	Default
type	Type of deployment condition.	true	string	
status	Status of the condition, one of True, False, Unknown.	true	string	
lastUpdateTime	The last time this condition was updated.	false	string	
lastTransitionTime	Last time the condition transitioned from one status to another.	false	string	
reason	The reason for the condition's last transition.	false	string	

Name	Description	Required	Schema	Default
message	A human readable message indicating details about the transition.	false	string	

v1.ConfigMapEnvSource

ConfigMapEnvSource selects a ConfigMap to populate the environment variables with.

The contents of the target ConfigMap's Data field will represent the key-value pairs as environment variables.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https://kubernetes.io/docs/concepts/overview/working-with-objects/names/#names	false	string	
optional	Specify whether the ConfigMap must be defined	false	boolean	false

v1.StorageOSVolumeSource

Represents a StorageOS persistent volume resource.

Name	Description	Required	Schema	Default
volumeName	VolumeName is the human-readable name of the StorageOS volume. Volume names are only unique within a namespace.	false	string	

Name	Description	Required	Schema	Default
volumeNamespace	VolumeNamespace specifies the scope of the volume within StorageOS. If no namespace is specified then the Pod's namespace will be used. This allows the Kubernetes name scoping to be mirrored within StorageOS for tighter integration. Set VolumeName to any name to override the default behaviour. Set to "default" if you are not using namespaces within StorageOS. Namespaces that do not pre-exist within StorageOS will be created.	false	string	

Name	Description	Required	Schema	Default
fsType	Filesystem type to mount. Must be a filesystem type supported by the host operating system. Ex. "ext4", "xfs", "ntfs". Implicitly inferred to be "ext4" if unspecified.	false	string	
readOnly	Defaults to false (read/write). ReadOnly here will force the ReadOnly setting in VolumeMounts.	false	boolean	false
secretRef	SecretRef specifies the secret to use for obtaining the StorageOS API credentials. If not specified, default values will be attempted.	false	v1.LocalObjectReference	

v1.NodeAffinity

Node affinity is a group of node affinity scheduling rules.

Name	Description	Required	Schema	Default
requiredDuringSchedulingIgnoredDuringExecution	If the affinity requirements specified by this field are not met at scheduling time, the pod will not be scheduled onto the node. If the affinity requirements specified by this field cease to be met at some point during pod execution (e.g. due to an update), the system may or may not try to eventually evict the pod from its node.	false	v1.NodeSelector	

Name	Description	Required	Schema	Default
preferredDuringSchedulingIgnoredDuringExecution	The scheduler will prefer to schedule pods to nodes that satisfy the affinity expressions specified by this field, but it may choose a node that violates one or more of the expressions. The node that is most preferred is the one with the greatest sum of weights, i.e. for each node that meets all of the scheduling requirements (resource request, requiredDuringScheduling affinity expressions, etc.), compute a sum by iterating through the elements of this field and adding "weight" to the sum if the node matches the corresponding matchExpressions; the node(s) with the highest	false	v1.PreferredSchedulingTerm array	

493

Name	Description	Required	Schema	Default

v1.AzureDataDiskKind

v1.PreferredSchedulingTerm

An empty preferred scheduling term matches all objects with implicit weight 0 (i.e. it's a no-op). A null preferred scheduling term matches no objects (i.e. is also a no-op).

Name	Description	Required	Schema	Default
weight	Weight associated with matching the corresponding nodeSelectorTerm, in the range 1-100.	true	integer (int32)	
preference	A node selector term, associated with the corresponding weight.	true	v1.NodeSelectorTerm	

v1beta1.DaemonSetCondition

DaemonSetCondition describes the state of a DaemonSet at a certain point.

Name	Description	Required	Schema	Default
type	Type of DaemonSet condition.	true	string	
status	Status of the condition, one of True, False, Unknown.	true	string	

Name	Description	Required	Schema	Default
lastTransitionTime	Last time the condition transitioned from one status to another.	false	string	
reason	The reason for the condition's last transition.	false	string	
message	A human readable message indicating details about the transition.	false	string	

v1.ConfigMapKeySelector

Selects a key from a ConfigMap.

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/ #names	false	string	
key	The key to select.	true	string	

Name	Description	Required	Schema	Default
optional	Specify whether the ConfigMap or it's key must be defined	false	boolean	false

v1beta1.HTTPIngressPath

HTTPIngressPath associates a path regex with a backend. Incoming urls matching the path are forwarded to the backend.

Name	Description	Required	Schema	Default
path	Path is an extended POSIX regex as defined by IEEE Std 1003.1, (i.e this follows the egrep/unix syntax, not the perl syntax) matched against the path of an incoming request. Currently it can contain characters disallowed from the conventional "path" part of a URL as defined by RFC 3986. Paths must begin with a /. If unspecified, the path defaults to a catch all sending traffic to the backend.	false	string	

Name	Description	Required	Schema	Default
backend	Backend defines the referenced service endpoint to which the traffic will be forwarded to.	true	v1beta1.IngressBackend	

v1beta1.Ingress

Ingress is a collection of rules that allow inbound connections to reach the endpoints defined by a backend. An Ingress can be configured to give services externally-reachable urls, load balance traffic, terminate SSL, offer name based virtual hosting etc.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	Spec is the desired state of the Ingress. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#spec-and-status	false	v1beta1.IngressSpec	
status	Status is the current state of the Ingress. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#spec-and-status	false	v1beta1.IngressStatus	

v1.AzureDataDiskCachingMode

any

Represents an untyped JSON map - see the description of the field for more info about the structure of this object.

Edit This Page

Operations

Operations

get available resources

GET /apis/extensions/v1beta1

Responses

HTTP Code	Description	Schema
default	success	v1.APIResourceList

Consumes

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

list or watch objects of kind DaemonSet

GET /apis/extensions/v1beta1/daemonsets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

506

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSetList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

list or watch objects of kind Deployment

GET /apis/extensions/v1beta1/deployments

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DeploymentList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

list or watch objects of kind Ingress

`GET /apis/extensions/v1beta1/ingresses`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1beta1.IngressList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

list or watch objects of kind DaemonSet

`GET /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

527

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

528

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSetList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

delete collection of DaemonSet

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

create a DaemonSet

POST /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.DaemonSet	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1beta1.DaemonSet
200	success	v1beta1.DaemonSet
201	Created	v1beta1.DaemonSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read the specified DaemonSet

GET /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace.*	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSet

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace the specified DaemonSet

PUT /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.DaemonSet	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSet
201	Created	v1beta1.DaemonSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

delete a DaemonSet

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

543

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update the specified DaemonSet

PATCH /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSet

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read status of the specified DaemonSet

`GET /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace status of the specified DaemonSet

```
PUT /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}/status
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.DaemonSet	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSet
201	Created	v1beta1.DaemonSet

Consumes

- /

Produces

- application/json
- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update status of the specified DaemonSet

`PATCH /apis/extensions/v1beta1/namespaces/{namespace}/daemonsets/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DaemonSet

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

list or watch objects of kind Deployment

GET /apis/extensions/v1beta1/namespaces/{namespace}/deployments

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the **continue** field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.DeploymentList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

delete collection of Deployment

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/deployments

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

561

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

create a Deployment

POST /apis/extensions/v1beta1/namespaces/{namespace}/deployments

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Deployment	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1beta1.Deployment
200	success	v1beta1.Deployment
201	Created	v1beta1.Deployment

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read the specified Deployment

GET /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace*.	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Deployment

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace the specified Deployment

PUT /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Deployment	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Deployment
201	Created	v1beta1.Deployment

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

delete a Deployment

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

569

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update the specified Deployment

PATCH /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Deployment

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

create rollback of a Deployment

`POST /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/rollback`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.DeploymentRollback	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DeploymentRollback	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1beta1.DeploymentRollback
200	success	v1beta1.DeploymentRollback
201	Created	v1beta1.DeploymentRollback

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read scale of the specified Deployment

GET /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/scale

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Scale	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Scale

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace scale of the specified Deployment

PUT /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/scale

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Scale	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Scale	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Scale
201	Created	v1beta1.Scale

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update scale of the specified Deployment

`PATCH /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/scale`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Scale	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Scale

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read status of the specified Deployment

```
GET /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/status
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Deployment

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace status of the specified Deployment

PUT /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/status

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Deployment	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Deployment
201	Created	v1beta1.Deployment

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update status of the specified Deployment

`PATCH /apis/extensions/v1beta1/namespaces/{namespace}/deployments/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Type	Name	Description	Required	Schema	Default
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Deployment

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

list or watch objects of kind Ingress

`GET /apis/extensions/v1beta1/namespaces/{namespace}/ingresses`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the **continue** field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

584

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

585

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.IngressList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

delete collection of Ingress

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/ingresses

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

591

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

592

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

create an Ingress

POST /apis/extensions/v1beta1/namespaces/{namespace}/ingresses

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Ingress	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1beta1.Ingress
200	success	v1beta1.Ingress
201	Created	v1beta1.Ingress

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read the specified Ingress

GET /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}

594

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace.*	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Ingress

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace the specified Ingress

PUT /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Ingress	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Ingress
201	Created	v1beta1.Ingress

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

delete an Ingress

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update the specified Ingress

PATCH /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Ingress

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read status of the specified Ingress

`GET /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Ingress

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace status of the specified Ingress

`PUT /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Ingress	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Ingress
201	Created	v1beta1.Ingress

Consumes

- /

Produces

- application/json
- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update status of the specified Ingress

`PATCH /apis/extensions/v1beta1/namespaces/{namespace}/ingresses/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Ingress

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

list or watch objects of kind ReplicaSet

GET /apis/extensions/v1beta1/namespaces/{namespace}/replicasets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSetList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

delete collection of ReplicaSet

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/replicasets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

617

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

create a ReplicaSet

POST /apis/extensions/v1beta1/namespaces/{namespace}/replicasets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.ReplicaSet	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1beta1.ReplicaSet
200	success	v1beta1.ReplicaSet
201	Created	v1beta1.ReplicaSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read the specified ReplicaSet

GET /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace*.	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace the specified ReplicaSet

PUT /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.ReplicaSet	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSet
201	Created	v1beta1.ReplicaSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

delete a ReplicaSet

DELETE /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update the specified ReplicaSet

PATCH /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSet

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read scale of the specified ReplicaSet

```
GET /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}/scale
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Scale	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Scale

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace scale of the specified ReplicaSet

PUT /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}/scale

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.Scale	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Scale	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Scale
201	Created	v1beta1.Scale

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update scale of the specified ReplicaSet

PATCH /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}/scale

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Scale	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.Scale

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

read status of the specified ReplicaSet

GET /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}/status

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

replace status of the specified ReplicaSet

`PUT /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1beta1.ReplicaSet	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSet
201	Created	v1beta1.ReplicaSet

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

partially update status of the specified ReplicaSet

PATCH /apis/extensions/v1beta1/namespaces/{namespace}/replicasets/{name}/status

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSet

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apisextensionsv1beta1

list or watch objects of kind ReplicaSet

GET /apis/extensions/v1beta1/replicasets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	

635

Type	Name	Description	Required	Schema	Default
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

639

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1beta1.ReplicaSetList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of DaemonSet

`GET /apis/extensions/v1beta1/watch/daemonsets`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

646

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of Deployment

GET /apis/extensions/v1beta1/watch/deployments

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

653

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of Ingress

`GET /apis/extensions/v1beta1/watch/ingresses`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of DaemonSet

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/daemonsets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

668

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch changes to an object of kind DaemonSet

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/daemonsets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the DaemonSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of Deployment

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/deployments

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

680

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch changes to an object of kind Deployment

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/deployments/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

689

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Deployment	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of Ingress

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/ingresses

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

697

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch changes to an object of kind Ingress

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/ingresses/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Ingress	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of ReplicaSet

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/replicasets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

713

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch changes to an object of kind ReplicaSet

GET /apis/extensions/v1beta1/watch/namespaces/{namespace}/replicasets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ReplicaSet	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

watch individual changes to a list of ReplicaSet

GET /apis/extensions/v1beta1/watch/replicasets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

725

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

727

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apisextensionsv1beta1

Edit This Page

Top Level API Objects

Top Level API Objects

- v1.Service
- v1.ServiceList
- v1.Event
- v1.EventList
- v1.Namespace
- v1.NamespaceList
- v1.Secret
- v1.SecretList

- v1.ConfigMap
- v1.ConfigMapList

Definitions

v1.APIResourceList

APIResourceList is a list of APIResource, it is used to expose the name of the resources supported in a specific group and version, and if the resource is namespaced.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
groupVersion	groupVersion is the group and version this APIResourceList is for.	true	string	
resources	resources contains the name of the resources and if they are namespaced.	true	v1.APIResource array	

v1.NamespaceList

NamespaceList is a list of Namespaces.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard list metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
items	Items is the list of Namespace objects in the list. More info: https://kubernetes.io/docs/concepts/overview/working-with-objects/namespaces/	true	v1.Namespace array	

v1.ListMeta

ListMeta describes metadata that synthetic resources must have, including lists and various status objects. A resource may have only one of {ObjectMeta, ListMeta}.

Name	Description	Required	Schema	Default
selfLink	selfLink is a URL representing this object. Populated by the system. Read-only.	false	string	

Name	Description	Required	Schema	Default
resourceVersion	String that identifies the server's internal version of this object that can be used by clients to determine when objects have changed. Value must be treated as opaque by clients and passed unmodified back to the server. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# concurrency-control-and-consistency	false	string	

Name	Description	Required	Schema	Default
continue	continue may be set if the user set a limit on the number of items returned, and indicates that the server has more data available. The value is opaque and may be used to issue another request to the endpoint that served this list to retrieve the next set of available objects. Continuing a list may not be possible if the server configuration has changed or more than a few minutes have passed. The resourceVersion field returned when using this continue value will be identical to the value in the first response.	false	string	

Name	Description	Required	Schema	Default

v1.Namespace

Namespace provides a scope for Names. Use of multiple namespaces is optional.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	Spec defines the behavior of the Namespace. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#spec-and-status	false	v1.NamespaceSpec	
status	Status describes the current status of a Namespace. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#spec-and-status	false	v1.NamespaceStatus	

v1.Initializers

Initializers tracks the progress of initialization.

Name	Description	Required	Schema	Default
pending	Pending is a list of initializers that must execute in order before this object is visible. When the last pending initializer is removed, and no failing result is set, the initializers struct will be set to nil and the object is considered as initialized and visible to all clients.	true	v1.Initializer array	
result	If result is set with the Failure field, the object will be persisted to storage and then deleted, ensuring that other clients can observe the deletion.	false	v1.Status	

v1.Preconditions

Preconditions must be fulfilled before an operation (update, delete, etc.) is carried out.

Name	Description	Required	Schema	Default
uid	Specifies the target UID.	false	types.UID	

v1.Status

Status is a return value for calls that don't return other objects.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard list metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
status	Status of the operation. One of: "Success" or "Failure". More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	string	
message	A human-readable description of the status of this operation.	false	string	
reason	A machine-readable description of why this operation is in the "Failure" status. If this value is empty there is no information available. A Reason clarifies an HTTP status code but does not override it.	false	string	

Name	Description	Required	Schema	Default
details	Extended data associated with the reason. Each reason may define its own extended details. This field is optional and the data returned is not guaranteed to conform to any schema except that defined by the reason type.	false	v1.StatusDetails	
code	Suggested HTTP return code for this status, 0 if not set.	false	integer (int32)	

v1.ServiceStatus

ServiceStatus represents the current status of a service.

Name	Description	Required	Schema	Default
loadBalancer	LoadBalancer contains the current status of the load-balancer, if one is present.	false	v1.LoadBalancerStatus	

v1.Secret

Secret holds secret data of a certain type. The total bytes of the values in the Data field must be less than MaxSecretSize bytes.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard object's metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
data	Data contains the secret data. Each key must consist of alphanumeric characters, -, _ or .. The serialized form of the secret data is a base64 encoded string, representing the arbitrary (possibly non-string) data value here. Described in https://tools.ietf.org/html/rfc4648#section-4	false	object	

Name	Description	Required	Schema	Default
stringData	stringData allows specifying non-binary secret data in string form. It is provided as a write-only convenience method. All keys and values are merged into the data field on write, overwriting any existing values. It is never output when reading from the API.	false	object	
type	Used to facilitate programmatic handling of secret data.	false	string	

v1.WatchEvent

Name	Description	Required	Schema	Default
type		true	string	
object		true	string	

v1.Event

Event is a report of an event somewhere in the cluster.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen-tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard object's metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	true	v1.ObjectMeta	
involvedObject	The object that this event is about.	true	v1.ObjectReference	

Name	Description	Required	Schema	Default
reason	This should be a short, machine understandable string that gives the reason for the transition into the object's current status.	false	string	
message	A human-readable description of the status of this operation.	false	string	
source	The component reporting this event. Should be a short machine understandable string.	false	v1.EventSource	
firstTimestamp	The time at which the event was first recorded. (Time of server receipt is in TypeMeta.)	false	string	
lastTimestamp	The time at which the most recent occurrence of this event was recorded.	false	string	

Name	Description	Required	Schema	Default
count	The number of times this event has occurred.	false	integer (int32)	
type	Type of this event (Normal, Warning), new types could be added in the future	false	string	
eventTime	Time when this Event was first observed.	false	string	
series	Data about the Event series this event represents or nil if it's a singleton Event.	false	v1.EventSeries	
action	What action was taken/failed regarding to the Regarding object.	false	string	
related	Optional secondary object for more complex actions.	false	v1.ObjectReference	
reportingComponent	Name of the controller that emitted this Event, e.g. `kubernetes.io/kubelet`.	true	string	

Name	Description	Required	Schema	Default
reportingInstance	ID of the controller instance, e.g. `kubelet-xyzf`.	true	string	

v1.LoadBalancerIngress

LoadBalancerIngress represents the status of a load-balancer ingress point: traffic intended for the service should be sent to an ingress point.

Name	Description	Required	Schema	Default
ip	IP is set for load-balancer ingress points that are IP based (typically GCE or OpenStack load-balancers)	false	string	
hostname	Hostname is set for load-balancer ingress points that are DNS based (typically AWS load-balancers)	false	string	

v1.DeletionPropagation

v1.NamespaceStatus

NamespaceStatus is information about the current status of a Namespace.

Name	Description	Required	Schema	Default
phase	Phase is the current lifecycle phase of the namespace. More info: https: //kubernetes. io/docs/ tasks/ administer- cluster/ namespaces/	false	string	

v1.ServiceList

ServiceList holds a list of services.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	v1.ListMeta	
items	List of services	true	v1.Service array	

v1.NamespaceSpec

NamespaceSpec describes the attributes on a Namespace.

756

Name	Description	Required	Schema	Default
finalizers	Finalizers is an opaque list of values that must be empty to permanently remove object from storage. More info: https: //kubernetes. io/docs/ tasks/ administer- cluster/ namespaces/	false	v1.FinalizerName array	

v1.Service

Service is a named abstraction of software service (for example, mysql) consisting of local port (for example 3306) that the proxy listens on, and the selector that determines which pods will answer requests sent through the proxy.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
spec	Spec defines the behavior of a service. https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1.ServiceSpec	
status	Most recently observed status of the service. Populated by the system. Read-only. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#spec-and-status	false	v1.ServiceStatus	

v1.Patch

Patch is provided to give a concrete name and type to the Kubernetes PATCH request body.

v1.ConfigMapList

ConfigMapList is a resource containing a list of ConfigMap objects.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ListMeta	
items	Items is the list of ConfigMaps.	true	v1.ConfigMap array	

v1.DeleteOptions

DeleteOptions may be provided when deleting an API object.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	

Name	Description	Required	Schema	Default
gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int64)	
preconditions	Must be fulfilled before a deletion is carried out. If not possible, a 409 Conflict status will be returned.	false	v1.Preconditions	

Name	Description	Required	Schema	Default
orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	false

Name	Description	Required	Schema	Default
propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all dependents in the foreground.	false	v1.DeletionPropagation	

v1.EventSeries

EventSeries contain information on series of events, i.e. thing that was/is happening continously for some time.

Name	Description	Required	Schema	Default
count	Number of occurrences in this series up to the last heartbeat time	false	integer (int32)	
lastObservedTime	Time of the last occurence observed	false	string	
state	State of this Series: Ongoing or Finished	false	string	

v1.StatusDetails

StatusDetails is a set of additional properties that MAY be set by the server to provide additional information about a response. The Reason field of a Status object defines what attributes will be set. Clients must ignore fields that do not match the defined type of each attribute, and should assume that any attribute may be empty, invalid, or under defined.

Name	Description	Required	Schema	Default
name	The name attribute of the resource associated with the status StatusReason (when there is a single name which can be described).	false	string	

Name	Description	Required	Schema	Default
group	The group attribute of the resource associated with the status StatusReason.	false	string	
kind	The kind attribute of the resource associated with the status StatusReason. On some operations may differ from the requested resource Kind. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	
uid	UID of the resource. (when there is a single resource which can be described). More info: http://kubernetes.io/docs/user-guide/identifiers#uids	false	string	

Name	Description	Required	Schema	Default
causes	The Causes array includes more details associated with the StatusReason failure. Not all StatusReasons may provide detailed causes.	false	v1.StatusCause array	
retryAfterSeconds	If specified, the time in seconds before the operation should be retried. Some errors may indicate the client must take an alternate action - for those errors this field may indicate how long to wait before taking the alternate action.	false	integer (int32)	

v1.ConfigMap

ConfigMap holds configuration data for pods to consume.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard object's metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#metadata	false	v1.ObjectMeta	

Name	Description	Required	Schema	Default
data	Data contains the configuration data. Each key must consist of alphanumeric characters, -, _ or .. Values with non-UTF-8 byte sequences must use the BinaryData field. The keys stored in Data must not overlap with the keys in the BinaryData field, this is enforced during validation process.	false	object	

Name	Description	Required	Schema	Default
binaryData	BinaryData contains the binary data. Each key must consist of alphanumeric characters, -, _ or .. BinaryData can contain byte sequences that are not in the UTF-8 range. The keys stored in BinaryData must not overlap with the ones in the Data field, this is enforced during validation process. Using this field will require 1.10+ apiserver and kubelet.	false	object	

v1.Initializer

Initializer is information about an initializer that has not yet completed.

Name	Description	Required	Schema	Default
name	name of the process that is responsible for initializing this object.	true	string	

v1.ObjectReference

ObjectReference contains enough information to let you inspect or modify the referred object.

Name	Description	Required	Schema	Default
kind	Kind of the referent. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	false	string	
namespace	Namespace of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ namespaces/	false	string	

Name	Description	Required	Schema	Default
name	Name of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/ #names	false	string	
uid	UID of the referent. More info: https: //kubernetes. io/docs/ concepts/ overview/ working- with-objects/ names/#uids	false	string	
apiVersion	API version of the referent.	false	string	
resourceVersion	Specific resourceVer- sion to which this reference is made, if any. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md# concurrency- control-and- consistency	false	string	

Name	Description	Required	Schema	Default
fieldPath	If referring to a piece of an object instead of an entire object, this string should contain a valid JSON/Go field access statement, such as desiredState.manifest.containers[2]. For example, if the object reference is to a container within a pod, this would take on a value like: "spec.containers{name}" (where "name" refers to the name of the container that triggered the event) or if no container name is specified "spec.containers[2]" (container with index 2 in this pod). This syntax is chosen only to have some well-defined way of referencing a part of an object.	false	string	

Name	Description	Required	Schema	Default

v1.LoadBalancerStatus

LoadBalancerStatus represents the status of a load-balancer.

Name	Description	Required	Schema	Default
ingress	Ingress is a list containing ingress points for the load-balancer. Traffic intended for the service should be sent to these ingress points.	false	v1.LoadBalancerIngress array	

v1.SecretList

SecretList is a list of Secret.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this represen- tation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md# resources	false	string	
metadata	Standard list metadata. More info: https: //git.k8s.io/ community/ contributors/ devel/api- conventions. md#types- kinds	false	v1.ListMeta	

Name	Description	Required	Schema	Default
items	Items is a list of secret objects. More info: https: //kubernetes. io/docs/ concepts/ configuration/ secret	true	v1.Secret array	

v1.FinalizerName

v1.ServicePort

ServicePort contains information on service's port.

Name	Description	Required	Schema	Default
name	The name of this port within the service. This must be a DNS_LABEL. All ports within a ServiceSpec must have unique names. This maps to the *Name* field in Endpoint- Port objects. Optional if only one ServicePort is defined on this service.	false	string	

Name	Description	Required	Schema	Default
protocol	The IP protocol for this port. Supports "TCP" and "UDP". Default is TCP.	false	string	
port	The port that will be exposed by this service.	true	integer (int32)	

Name	Description	Required	Schema	Default
targetPort	Number or name of the port to access on the pods targeted by the service. Number must be in the range 1 to 65535. Name must be an IANA_SVC_NAME. If this is a string, it will be looked up as a named port in the target Pod's container ports. If this is not specified, the value of the *port* field is used (an identity map). This field is ignored for services with clusterIP=None, and should be omitted or set equal to the *port* field. More info: https://kubernetes.io/docs/concepts/services-networking/service/#defining-a-service	false	string	

Name	Description	Required	Schema	Default
nodePort	The port on each node on which this service is exposed when type=NodePort or LoadBalancer. Usually assigned by the system. If specified, it will be allocated to the service if unused or else creation of the service will fail. Default is to auto-allocate a port if the ServiceType of this Service requires one. More info: https: //kubernetes. io/docs/ concepts/ services-networking/ service/ #nodeport	false	integer (int32)	

v1.OwnerReference

OwnerReference contains enough information to let you identify an owning object. Currently, an owning object must be in the same namespace, so there is no namespace field.

Name	Description	Required	Schema	Default
apiVersion	API version of the referent.	true	string	
kind	Kind of the referent. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	true	string	
name	Name of the referent. More info: http: //kubernetes. io/docs/user-guide/ identifiers# names	true	string	
uid	UID of the referent. More info: http: //kubernetes. io/docs/user-guide/ identifiers# uids	true	string	
controller	If true, this reference points to the managing controller.	false	boolean	false

Name	Description	Required	Schema	Default
blockOwnerDeletion	If true, AND if the owner has the "foreground-Deletion" finalizer, then the owner cannot be deleted from the key-value store until this reference is removed. Defaults to false. To set this field, a user needs "delete" permission of the owner, otherwise 422 (Unprocessable Entity) will be returned.	false	boolean	false

v1.ObjectMeta

ObjectMeta is metadata that all persisted resources must have, which includes all objects users must create.

Name	Description	Required	Schema	Default
name	Name must be unique within a namespace. Is required when creating resources, although some resources may allow a client to request the generation of an appropriate name automatically. Name is primarily intended for creation idempotence and configuration definition. Cannot be updated. More info: http://kubernetes.io/docs/user-guide/identifiers# names	false	string	

Name	Description	Required	Schema	Default
generateName	GenerateName is an optional prefix, used by the server, to generate a unique name ONLY IF the Name field has not been provided. If this field is used, the name returned to the client will be different than the name passed. This value will also be combined with a unique suffix. The provided value has the same validation rules as the Name field, and may be truncated by the length of the suffix required to make the value unique on the server. If this field is specified and the generated name exists, the server will NOT return a 409 - instead, it will either return 201 Created or 500 with	false	string	

Name	Description	Required	Schema	Default
namespace	Namespace defines the space within each name must be unique. An empty namespace is equivalent to the "default" namespace, but "default" is the canonical representation. Not all objects are required to be scoped to a namespace - the value of this field for those objects will be empty. Must be a DNS_LABEL. Cannot be updated. More info: http://kubernetes.io/docs/user-guide/namespaces	false	string	
selfLink	SelfLink is a URL representing this object. Populated by the system. Read-only.	false	string	

Name	Description	Required	Schema	Default
uid	UID is the unique in time and space value for this object. It is typically generated by the server on successful creation of a resource and is not allowed to change on PUT operations. Populated by the system. Read-only. More info: http://kubernetes.io/docs/user-guide/identifiers#uids	false	string	

Name	Description	Required	Schema	Default
resourceVersion	An opaque value that represents the internal version of this object that can be used by clients to determine when objects have changed. May be used for optimistic concurrency, change detection, and the watch operation on a resource or set of resources. Clients must treat these values as opaque and passed unmodified back to the server. They may only be valid for a particular resource or set of resources. Populated by the system. Read-only. Value must be treated as opaque by clients and . More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#	false	string	

Name	Description	Required	Schema	Default
generation	A sequence number representing a specific generation of the desired state. Populated by the system. Read-only.	false	integer (int64)	

Name	Description	Required	Schema	Default
creationTimestamp	CreationTimestamp is a timestamp representing the server time when this object was created. It is not guaranteed to be set in happens-before order across separate operations. Clients may not set this value. It is represented in RFC3339 form and is in UTC. Populated by the system. Read-only. Null for lists. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md# metadata	false	string	

Name	Description	Required	Schema	Default
deletionTimestamp	DeletionTimestamp is RFC 3339 date and time at which this resource will be deleted. This field is set by the server when a graceful deletion is requested by the user, and is not directly settable by a client. The resource is expected to be deleted (no longer visible from resource lists, and not reachable by name) after the time in this field, once the finalizers list is empty. As long as the finalizers list contains items, deletion is blocked. Once the deletion-Timestamp is set, this value may not be unset or be set further into the future, although it may be shortened or the resource may be deleted prior to this time.	false	string	

Name	Description	Required	Schema	Default
deletionGracePeriodSeconds	Number of seconds allowed for this object to gracefully terminate before it will be removed from the system. Only set when deletion-Timestamp is also set. May only be shortened. Read-only.	false	integer (int64)	
labels	Map of string keys and values that can be used to organize and categorize (scope and select) objects. May match selectors of replication controllers and services. More info: http: //kubernetes. io/docs/user-guide/labels	false	object	

Name	Description	Required	Schema	Default
annotations	Annotations is an unstructured key value map stored with a resource that may be set by external tools to store and retrieve arbitrary metadata. They are not queryable and should be preserved when modifying objects. More info: http://kubernetes.io/docs/user-guide/annotations	false	object	

Name	Description	Required	Schema	Default
ownerReferences	List of objects depended by this object. If ALL objects in the list have been deleted, this object will be garbage collected. If this object is managed by a controller, then an entry in this list will point to this controller, with the controller field set to true. There cannot be more than one managing controller.	false	v1.OwnerReference array	

Name	Description	Required	Schema	Default
initializers	An initializer is a controller which enforces some system invariant at object creation time. This field is a list of initializers that have not yet acted on this object. If nil or empty, this object has been completely initialized. Otherwise, the object is considered uninitialized and is hidden (in list/watch and get calls) from clients that haven't explicitly asked to observe uninitialized objects. When an object is created, the system will populate this list with the current set of initializers. Only privileged users may set or modify this list. Once it is empty, it may not be modified further by	false	v1.Initializers	

Name	Description	Required	Schema	Default
finalizers	Must be empty before the object is deleted from the registry. Each entry is an identifier for the responsible component that will remove the entry from the list. If the deletion-Timestamp of the object is non-nil, entries in this list can only be removed.	false	string array	

Name	Description	Required	Schema	Default
clusterName	The name of the cluster which the object belongs to. This is used to distinguish resources with same name and namespace in different clusters. This field is not set anywhere right now and apiserver is going to ignore it if set in create or update request.	false	string	

v1.EventList

EventList is a list of events.

Name	Description	Required	Schema	Default
kind	Kind is a string value representing the REST resource this object represents. Servers may infer this from the endpoint the client submits requests to. Cannot be updated. In CamelCase. More info: https: //git.k8s.io/ community/ contributors/ devel/api-conventions. md#types-kinds	false	string	

Name	Description	Required	Schema	Default
apiVersion	APIVersion defines the versioned schema of this representation of an object. Servers should convert recognized schemas to the latest internal value, and may reject unrecognized values. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#resources	false	string	
metadata	Standard list metadata. More info: https://git.k8s.io/community/contributors/devel/api-conventions.md#types-kinds	false	v1.ListMeta	
items	List of events	true	v1.Event array	

v1.ClientIPConfig

ClientIPConfig represents the configurations of Client IP based session affinity.

Name	Description	Required	Schema	Default
timeoutSeconds	timeoutSeconds specifies the seconds of ClientIP type session sticky time. The value must be >0 && 86400(for 1 day) if ServiceAffinity == "ClientIP". Default value is 10800(for 3 hours).	false	integer (int32)	

v1.APIResource

APIResource specifies the name of a resource and whether it is namespaced.

Name	Description	Required	Schema	Default
name	name is the plural name of the resource.	true	string	

Name	Description	Required	Schema	Default
singularName	singularName is the singular name of the resource. This allows clients to handle plural and singular opaquely. The singular-Name is more correct for reporting status on a single item and both singular and plural are allowed from the kubectl CLI interface.	true	string	
namespaced	namespaced indicates if a resource is namespaced or not.	true	boolean	false

Name	Description	Required	Schema	Default
group	group is the preferred group of the resource. Empty implies the group of the containing resource list. For subresources, this may have a different value, for example: Scale".	false	string	
version	version is the preferred version of the resource. Empty implies the version of the containing resource list For subresources, this may have a different value, for example: v1 (while inside a v1beta1 version of the core resource's group)".	false	string	

Name	Description	Required	Schema	Default
kind	kind is the kind for the resource (e.g. *Foo* is the kind for a resource *foo*)	true	string	
verbs	verbs is a list of supported kube verbs (this includes get, list, watch, create, update, patch, delete, deletecollection, and proxy)	true	string array	
shortNames	shortNames is a list of suggested short names of the resource.	false	string array	
categories	categories is a list of the grouped resources this resource belongs to (e.g. *all*)	false	string array	

v1.ServiceSpec

ServiceSpec describes the attributes that a user creates on a service.

Name	Description	Required	Schema	Default
ports	The list of ports that are exposed by this service. More info: https://kubernetes.io/docs/concepts/services-networking/service/#virtual-ips-and-service-proxies	false	v1.ServicePort array	

Name	Description	Required	Schema	Default
selector	Route service traffic to pods with label keys and values matching this selector. If empty or not present, the service is assumed to have an external process managing its endpoints, which Kubernetes will not modify. Only applies to types ClusterIP, NodePort, and LoadBalancer. Ignored if type is ExternalName. More info: https: //kubernetes. io/docs/ concepts/ services-networking/ service/	false	object	

Name	Description	Required	Schema	Default
clusterIP	clusterIP is the IP address of the service and is usually assigned randomly by the master. If an address is specified manually and is not in use by others, it will be allocated to the service; otherwise, creation of the service will fail. This field can not be changed through updates. Valid values are "None", empty string (""), or a valid IP address. "None" can be specified for headless services when proxying is not required. Only applies to types ClusterIP, NodePort, and LoadBalancer. Ignored if type is ExternalName. More info: https: //kubernetes. io/docs/ concepts/ services- networking/	false	string	

Name	Description	Required	Schema	Default
type	type determines how the Service is exposed. Defaults to ClusterIP. Valid options are External-Name, ClusterIP, NodePort, and LoadBalancer. "External-Name" maps to the specified externalName. "ClusterIP" allocates a cluster-internal IP address for load-balancing to endpoints. Endpoints are determined by the selector or if that is not specified, by manual construction of an Endpoints object. If clusterIP is "None", no virtual IP is allocated and the endpoints are published as a set of endpoints rather than a stable IP. "NodePort" builds on ClusterIP and allocates	false	string	

Name	Description	Required	Schema	Default
externalIPs	externalIPs is a list of IP addresses for which nodes in the cluster will also accept traffic for this service. These IPs are not managed by Kubernetes. The user is responsible for ensuring that traffic arrives at a node with this IP. A common example is external load-balancers that are not part of the Kubernetes system.	false	string array	

Name	Description	Required	Schema	Default
sessionAffinity	Supports "ClientIP" and "None". Used to maintain session affinity. Enable client IP based session affinity. Must be ClientIP or None. Defaults to None. More info: https://kubernetes.io/docs/concepts/services-networking/service/#virtual-ips-and-service-proxies	false	string	

Name	Description	Required	Schema	Default
loadBalancerIP	Only applies to Service Type: LoadBalancer will get created with the IP specified in this field. This feature depends on whether the underlying cloud-provider supports specifying the loadBalancerIP when a load balancer is created. This field will be ignored if the cloud-provider does not support the feature.	false	string	

Name	Description	Required	Schema	Default
loadBalancerSourceRanges	If specified and supported by the platform, this will restrict traffic through the cloud-provider load-balancer will be restricted to the specified client IPs. This field will be ignored if the cloud-provider does not support the feature." More info: https://kubernetes.io/docs/tasks/access-application-cluster/configure-cloud-provider-firewall/	false	string array	

Name	Description	Required	Schema	Default
externalName	externalName is the external reference that kubedns or equivalent will return as a CNAME record for this service. No proxying will be involved. Must be a valid RFC-1123 hostname (https: //tools.ietf. org/html/ rfc1123) and requires Type to be ExternalName.	false	string	

Name	Description	Required	Schema	Default
externalTrafficPolicy	externalTrafficPolicy denotes if this Service desires to route external traffic to node-local or cluster-wide endpoints. "Local" preserves the client source IP and avoids a second hop for LoadBalancer and Nodeport type services, but risks potentially imbalanced traffic spreading. "Cluster" obscures the client source IP and may cause a second hop to another node, but should have good overall load-spreading.	false	string	

Name	Description	Required	Schema	Default
healthCheckNodePort	healthCheckNodePort specifies the healthcheck nodePort for the service. If not specified, HealthCheckNodePort is created by the service api backend with the allocated nodePort. Will use user-specified nodePort value if specified by the client. Only effects when Type is set to LoadBalancer and ExternalTrafficPolicy is set to Local.	false	integer (int32)	

817

Name	Description	Required	Schema	Default
publishNotReadyAddresses	publishNotReadyAddresses, when set to true, indicates that DNS implementations must publish the notReadyAddresses of subsets for the Endpoints associated with the Service. The default value is false. The primary use case for setting this field is to use a StatefulSet's Headless Service to propagate SRV records for its Pods without respect to their readiness for purpose of peer discovery. This field will replace the service.alpha.kubernetes.io/tolerate-unready-endpoints when that annotation is deprecated and all clients have been converted to use this field.	false	boolean	false

Name	Description	Required	Schema	Default
sessionAffinityConfig	sessionAffinityConfig contains the configurations of session affinity.	false	v1.SessionAffinityConfig	

v1.EventSource

EventSource contains information for an event.

Name	Description	Required	Schema	Default
component	Component from which the event is generated.	false	string	
host	Node name on which the event is generated.	false	string	

types.UID

v1.StatusCause

StatusCause provides more information about an api.Status failure, including cases when multiple errors are encountered.

Name	Description	Required	Schema	Default
reason	A machine-readable description of the cause of the error. If this value is empty there is no information available.	false	string	

Name	Description	Required	Schema	Default
message	A human-readable description of the cause of the error. This field may be presented as-is to a reader.	false	string	

Name	Description	Required	Schema	Default
field	The field of the resource that has caused this error, as named by its JSON serialization. May include dot and postfix notation for nested attributes. Arrays are zero-indexed. Fields may appear more than once in an array of causes due to fields having multiple errors. Optional. Examples: "name" - the field "name" on the current resource "items[0].name" - the field "name" on the first array entry in "items"	false	string	

v1.SessionAffinityConfig

SessionAffinityConfig represents the configurations of session affinity.

Name	Description	Required	Schema	Default
clientIP	clientIP contains the configurations of Client IP based session affinity.	false	v1.ClientIPConfig	

any

Represents an untyped JSON map - see the description of the field for more info about the structure of this object.

Edit This Page

Operations

Operations

get available resources

`GET /api/v1`

Responses

HTTP Code	Description	Schema
default	success	v1.APIResourceList

Consumes

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apiv1

list or watch objects of kind ConfigMap

GET /api/v1/configmaps

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.ConfigMapList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

list or watch objects of kind Event

GET /api/v1/events

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use 834 the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.EventList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

list or watch objects of kind Namespace

`GET /api/v1/namespaces`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.NamespaceList

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

create a Namespace

`POST /api/v1/namespaces`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Namespace	

843

Responses

HTTP Code	Description	Schema
202	Accepted	v1.Namespace
200	success	v1.Namespace
201	Created	v1.Namespace

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

list or watch objects of kind ConfigMap

GET /api/v1/namespaces/{namespace}/configmaps

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.ConfigMapList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

delete collection of ConfigMap

DELETE /api/v1/namespaces/{namespace}/configmaps

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

857

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apiv1

create a ConfigMap

POST /api/v1/namespaces/{namespace}/configmaps

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.ConfigMap	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1.ConfigMap
200	success	v1.ConfigMap
201	Created	v1.ConfigMap

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

read the specified ConfigMap

```
GET /api/v1/namespaces/{namespace}/configmaps/{name}
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace*.	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ConfigMap	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.ConfigMap

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace the specified ConfigMap

`PUT /api/v1/namespaces/{namespace}/configmaps/{name}`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.ConfigMap	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ConfigMap	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.ConfigMap
201	Created	v1.ConfigMap

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

delete a ConfigMap

DELETE /api/v1/namespaces/{namespace}/configmaps/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

865

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ConfigMap	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update the specified ConfigMap

PATCH /api/v1/namespaces/{namespace}/configmaps/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ConfigMap	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.ConfigMap

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

list or watch objects of kind Event

`GET /api/v1/namespaces/{namespace}/events`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

872

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.EventList

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

delete collection of Event

DELETE /api/v1/namespaces/{namespace}/events

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

create an Event

POST /api/v1/namespaces/{namespace}/events

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Event	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1.Event
200	success	v1.Event
201	Created	v1.Event

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

read the specified Event

GET /api/v1/namespaces/{namespace}/events/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace.*	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Event	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Event

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace the specified Event

`PUT /api/v1/namespaces/{namespace}/events/{name}`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Event	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Event	true	string	

884

Responses

HTTP Code	Description	Schema
200	success	v1.Event
201	Created	v1.Event

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

delete an Event

DELETE /api/v1/namespaces/{namespace}/events/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Event	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update the specified Event

PATCH /api/v1/namespaces/{namespace}/events/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Event	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Event

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apiv1

list or watch objects of kind Secret

`GET /api/v1/namespaces/{namespace}/secrets`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use 895 the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.SecretList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

delete collection of Secret

DELETE /api/v1/namespaces/{namespace}/secrets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

902

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

create a Secret

POST /api/v1/namespaces/{namespace}/secrets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Secret	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1.Secret
200	success	v1.Secret
201	Created	v1.Secret

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

read the specified Secret

GET /api/v1/namespaces/{namespace}/secrets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace*.	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Secret	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Secret

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace the specified Secret

`PUT /api/v1/namespaces/{namespace}/secrets/{name}`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Secret	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Secret	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Secret
201	Created	v1.Secret

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

delete a Secret

DELETE /api/v1/namespaces/{namespace}/secrets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

911

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Secret	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update the specified Secret

PATCH /api/v1/namespaces/{namespace}/secrets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Secret	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Secret

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

list or watch objects of kind Service

GET /api/v1/namespaces/{namespace}/services

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

918

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

919

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.ServiceList

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

delete collection of Service

DELETE /api/v1/namespaces/{namespace}/services

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

925

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

create a Service

POST /api/v1/namespaces/{namespace}/services

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Service	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
202	Accepted	v1.Service
200	success	v1.Service
201	Created	v1.Service

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

read the specified Service

GET /api/v1/namespaces/{namespace}/services/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace*.	false	boolean	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Service

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace the specified Service

```
PUT /api/v1/namespaces/{namespace}/services/{name}
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Service	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Service
201	Created	v1.Service

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

delete a Service

DELETE /api/v1/namespaces/{namespace}/services/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	

Type	Name	Description	Required	Schema	Default
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

934

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update the specified Service

PATCH /api/v1/namespaces/{namespace}/services/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Service

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apiv1

read status of the specified Service

```
GET /api/v1/namespaces/{namespace}/services/{name}/status
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Service

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace status of the specified Service

`PUT /api/v1/namespaces/{namespace}/services/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Service	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Service
201	Created	v1.Service

Consumes

- /

Produces

- application/json
- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update status of the specified Service

`PATCH /api/v1/namespaces/{namespace}/services/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Service

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

read the specified Namespace

`GET /api/v1/namespaces/{name}`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	export	Should this value be exported. Export strips fields that a user can not specify.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	exact	Should the export be exact. Exact export maintains cluster-specific fields like *Namespace.*	false	boolean	
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace the specified Namespace

PUT /api/v1/namespaces/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Namespace	
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace
201	Created	v1.Namespace

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

delete a Namespace

DELETE /api/v1/namespaces/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.DeleteOptions	
QueryParameter	gracePeriodSeconds	The duration in seconds before the object should be deleted. Value must be non-negative integer. The value zero indicates delete immediately. If this value is nil, the default grace period for the specified type will be used. Defaults to a per object value if not specified. zero means delete immediately.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	orphanDependents	Deprecated: please use the PropagationPolicy, this field will be deprecated in 1.7. Should the dependent objects be orphaned. If true/false, the "orphan" finalizer will be added to/removed from the object's finalizers list. Either this field or PropagationPolicy may be set, but not both.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	propagationPolicy	Whether and how garbage collection will be performed. Either this field or OrphanDependents may be set, but not both. The default policy is decided by the existing finalizer set in the metadata.finalizers and the resource-specific default policy. Acceptable values are: *Orphan* - orphan the dependents; *Background* - allow the garbage collector to delete the dependents in the background; *Foreground* - a cascading policy that deletes all depen-	false	string	

945

Type	Name	Description	Required	Schema	Default
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Status

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update the specified Namespace

```
PATCH /api/v1/namespaces/{name}
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	name	name of the Namespace	true	string	

946

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace

Consumes

- application/json-patch+json
- application/merge-patch+json
- application/strategic-merge-patch+json

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace finalize of the specified Namespace

PUT /api/v1/namespaces/{name}/finalize

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Namespace	
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace
201	Created	v1.Namespace

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

read status of the specified Namespace

```
GET /api/v1/namespaces/{name}/status
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

replace status of the specified Namespace

`PUT /api/v1/namespaces/{name}/status`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Namespace	
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace
201	Created	v1.Namespace

Consumes

- /

949

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

partially update status of the specified Namespace

```
PATCH /api/v1/namespaces/{name}/status
```

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
BodyParameter	body		true	v1.Patch	
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.Namespace

Consumes

- application/json-patch+json

- application/merge-patch+json

- application/strategic-merge-patch+json

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

Tags

- apiv1

list or watch objects of kind Secret

`GET /api/v1/secrets`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifica-tions. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.SecretList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

list or watch objects of kind Service

GET /api/v1/services

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

957

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.ServiceList

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of ConfigMap

`GET /api/v1/watch/configmaps`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Event

`GET /api/v1/watch/events`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

976

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Namespace

`GET /api/v1/watch/namespaces`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of ConfigMap

GET /api/v1/watch/namespaces/{namespace}/configmaps

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

990

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch changes to an object of kind ConfigMap

GET /api/v1/watch/namespaces/{namespace}/configmaps/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

997

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the ConfigMap	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Event

GET /api/v1/watch/namespaces/{namespace}/events

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

1005

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch changes to an object of kind Event

GET /api/v1/watch/namespaces/{namespace}/events/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

1012

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Event	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Secret

GET /api/v1/watch/namespaces/{namespace}/secrets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

1019

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch changes to an object of kind Secret

GET /api/v1/watch/namespaces/{namespace}/secrets/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Secret	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Service

GET /api/v1/watch/namespaces/{namespace}/services

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

1033

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

1034

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch changes to an object of kind Service

GET /api/v1/watch/namespaces/{namespace}/services/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameters	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default
PathParameter	namespace	object name and auth scope, such as for teams and projects	true	string	
PathParameter	name	name of the Service	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch changes to an object of kind Namespace

GET /api/v1/watch/namespaces/{name}

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

1049

Type	Name	Description	Required	Schema	Default
PathParameter	name	name of the Namespace	true	string	

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Secret

GET /api/v1/watch/secrets

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

1055

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json
- application/yaml
- application/vnd.kubernetes.protobuf
- application/json;stream=watch
- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

watch individual changes to a list of Service

`GET /api/v1/watch/services`

Parameters

Type	Name	Description	Required	Schema	Default
QueryParameter	pretty	If *true*, then the output is pretty printed.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	labelSelector	A selector to restrict the list of returned objects by their labels. Defaults to everything.	false	string	
QueryParameter	fieldSelector	A selector to restrict the list of returned objects by their fields. Defaults to everything.	false	string	
QueryParameter	includeUninitialized	If true, partially initialized resources are included in the response.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	watch	Watch for changes to the described resources and return them as a stream of add, update, and remove notifications. Specify resourceVersion.	false	boolean	

Type	Name	Description	Required	Schema	Default
QueryParameter	resourceVersion	When specified with a watch call, shows changes that occur after that particular version of a resource. Defaults to changes from the beginning of history. When specified for list: - if unset, then the result is returned from remote storage based on quorum-read flag; - if it's 0, then we simply return what we currently have in cache, no guarantee; - if set to non zero, then the result is at least as fresh as given rv.	false	string	

Type	Name	Description	Required	Schema	Default
QueryParameter	timeoutSeconds	Timeout for the list/watch call.	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	limit	limit is a maximum number of responses to return for a list call. If more items exist, the server will set the `continue` field on the list metadata to a value that can be used with the same initial query to retrieve the next set of results. Setting a limit may return fewer than the requested amount of items (up to zero items) in the event all requested objects are filtered out and clients should only use the presence of the continue field to determine whether	false	integer (int32)	

Type	Name	Description	Required	Schema	Default
QueryParameter	continue	The continue option should be set when retrieving more results from the server. Since this value is server defined, clients may only use the continue value from a previous query result with identical query parameters (except for the value of continue) and the server may reject a continue value it does not recognize. If the specified continue value is no longer valid whether due to expiration (generally five to fifteen minutes) or a configuration	false	string	

Type	Name	Description	Required	Schema	Default

Responses

HTTP Code	Description	Schema
200	success	v1.WatchEvent

Consumes

- /

Produces

- application/json

- application/yaml

- application/vnd.kubernetes.protobuf

- application/json;stream=watch

- application/vnd.kubernetes.protobuf;stream=watch

Tags

- apiv1

Edit This Page

kubeadm version

This command prints the version of kubeadm.

Print the version of kubeadm

Synopsis

Print the version of kubeadm

```
kubeadm version [flags]
```

Options

-h, --help

help for version

-o, --output string

Output format; available options are 'yaml', 'json' and 'short'

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Edit This Page

kubeadm alpha

- – kubeadm alpha phase preflight
  – kubeadm alpha phase certs
  – kubeadm alpha phase certs renew
  – kubeadm alpha phase kubeconfig
  – kubeadm alpha phase kubelet
  – kubeadm alpha phase controlplane
  – kubeadm alpha phase etcd
  – kubeadm alpha phase mark-master
  – kubeadm alpha phase bootstrap-token
  – kubeadm alpha phase upload-config
  – kubeadm alpha phase addon
  – kubeadm alpha phase self-hosting
  – What's next

  Caution: `kubeadm alpha` provides a preview of a set of features made available for gathering feedback from the community. Please try it out and give us feedback!

In v1.8.0, kubeadm introduced the `kubeadm alpha phase` command with the aim of making kubeadm more modular. This modularity enables you to invoke atomic sub-steps of the bootstrap process; you can let kubeadm do some parts and fill in yourself where you need customizations.

`kubeadm alpha phase` is consistent with kubeadm init workflow, and behind the scene both use the same code.

kubeadm alpha phase preflight

You can execute preflight checks both for the master node, like in `kubeadm init`, or for the worker node like in `kubeadm join`.

- master
- node

Run master pre-flight checks

Synopsis

Run master pre-flight checks, functionally equivalent to what implemented by kubeadm init.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase preflight master [flags]
```

Examples

```
  # Run master pre-flight checks.
  kubeadm alpha phase preflight master
```

Options

-h, --help

help for master

Options inherited from parent commands

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilegedUser,Swap'. Value 'all' ignores errors from all checks.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Run node pre-flight checks

Synopsis

Run node pre-flight checks, functionally equivalent to what implemented by kubeadm join.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase preflight node [flags]
```

Examples

```
  # Run node pre-flight checks.
  kubeadm alpha phase preflight node
```

Options

-h, --help

help for node

Options inherited from parent commands

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilegedUser,Swap'. Value 'all' ignores errors from all checks.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase certs

You can create all required certificates with the `all` subcommand or selectively create certificates.

- all
- ca
- apiserver
- apiserver-kubelet-client
- sa
- front-proxy-ca

1067

- front-proxy-client

Generates all PKI assets necessary to establish the control plane

Synopsis

Generates a self-signed CA to provision identities for each component in the cluster (including nodes) and client certificates to be used by various components.

If a given certificate and private key pair both exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs all [flags]
```

Examples

```
  # Creates all PKI assets necessary to establish the control plane,
  # functionally equivalent to what generated by kubeadm init.
  kubeadm alpha phase certs all

  # Creates all PKI assets using options read from a configuration file.
  kubeadm alpha phase certs all --config masterconfiguration.yaml
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on, to use for the API server serving cert

--apiserver-cert-extra-sans stringSlice

Optional extra altnames to use for the API server serving cert. Can be both IP addresses and DNS names

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for all

1068

--service-cidr string   Default: "10.96.0.0/12"

Alternative range of IP address for service VIPs, from which derives the internal API server VIP that will be added to the API Server serving cert

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services, to use for the API server serving cert

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the self-signed kubernetes CA to provision identities for other kuberenets components

Synopsis

Generates the self-signed kubernetes CA to provision identities for other kuberenets components, and saves them into ca.cert and ca.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs ca [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for ca

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the certificate for serving the kubernetes API

Synopsis

Generates the certificate for serving the kubernetes API, and saves them into apiserver.cert and apiserver.key files.

Default SANs are kubernetes, kubernetes.default, kubernetes.default.svc, kubernetes.default.svc.cluster.local, 10.96.0.1, 127.0.0.1

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs apiserver [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on, to use for the API server serving cert

--apiserver-cert-extra-sans stringSlice

Optional extra altnames to use for the API server serving cert. Can be both IP addresses and DNS names

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver

--service-cidr string   Default: "10.96.0.0/12"

Alternative range of IP address for service VIPs, from which derives the internal API server VIP that will be added to the API Server serving cert

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services, to use for the API server serving cert

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the Client certificate for the API server to connect to kubelet

Synopsis

Generates the Client certificate for the API server to connect to kubelet, and saves them into apiserver-kubelet-client.cert and apiserver-kubelet-client.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs apiserver-kubelet-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver-kubelet-client

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a private key for signing service account tokens along with its public key

Synopsis

Generates the private key for signing service account tokens along with its public key, and saves them into sa.key and sa.pub files. If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs sa [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for sa

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the self-signed CA to provision identities for front proxy

Synopsis

Generates the self-signed CA to provision identities for front proxy, and saves them into front-proxy-ca.cert and front-proxy-ca.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs front-proxy-ca [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for front-proxy-ca

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client for the front proxy

Synopsis

Generates the client for the front proxy, and saves them into front-proxy-client.cert and front-proxy-client.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs front-proxy-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for front-proxy-client

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase certs renew

You can renew all Kubernetes certificates using the `all` subcommand or renew them selectively.

- all
- apiserver-etcd-client
- apiserver-kubelet-client
- apiserver
- etcd-healthcheck-client
- etcd-peer
- etcd-server
- front-proxy-client

renew all available certificates

Synopsis

Renews all known certificates necessary to run the control plan. Renewals are run unconditionally, regardless of expiration date. Renewals can also be run individually for more control.

```
kubeadm alpha phase certs renew all [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for all

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client apiserver uses to access etcd

Synopsis

Renews the client apiserver uses to access etcd, and saves them into apiserver-etcd-client.cert and apiserver-etcd-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew apiserver-etcd-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver-etcd-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the Client certificate for the API server to connect to kubelet

Synopsis

Renews the Client certificate for the API server to connect to kubelet, and saves them into apiserver-kubelet-client.cert and apiserver-kubelet-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew apiserver-kubelet-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver-kubelet-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the certificate for serving the kubernetes API

Synopsis

Renews the certificate for serving the kubernetes API, and saves them into apiserver.cert and apiserver.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew apiserver [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client certificate for liveness probes to healtcheck etcd

Synopsis

Renews the client certificate for liveness probes to healtcheck etcd, and saves them into etcd/healthcheck-client.cert and etcd/healthcheck-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew etcd-healthcheck-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for etcd-healthcheck-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the credentials for etcd nodes to communicate with each other

Synopsis

Renews the credentials for etcd nodes to communicate with each other, and saves them into etcd/peer.cert and etcd/peer.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew etcd-peer [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for etcd-peer

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the certificate for serving etcd

Synopsis

Renews the certificate for serving etcd, and saves them into etcd/server.cert and etcd/server.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew etcd-server [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for etcd-server

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client for the front proxy

Synopsis

Renews the client for the front proxy, and saves them into front-proxy-client.cert and front-proxy-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew front-proxy-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for front-proxy-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase kubeconfig

You can create all required kubeconfig files with the `all` subcommand, or selectively create the files. Additionally, the `user` subcommand supports the creation of kubeconfig files for additional users.

- all
- admin
- kubelet
- controller-manager
- scheduler
- user

Generates all kubeconfig files necessary to establish the control plane and the admin kubeconfig file

Synopsis

Generates all kubeconfig files necessary to establish the control plane and the admin kubeconfig file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig all [flags]
```

Examples

```
  # Generates all kubeconfig files, functionally equivalent to what generated
  # by kubeadm init.
  kubeadm alpha phase kubeconfig all

  # Generates all kubeconfig files using options read from a configuration file.
  kubeadm alpha phase kubeconfig all --config masterconfiguration.yaml
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for all

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

--node-name string

The node name that should be used for the kubelet client certificate

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the admin to use and for kubeadm itself

Synopsis

Generates the kubeconfig file for the admin and for kubeadm itself, and saves it to admin.conf file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig admin [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for admin

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the kubelet to use. Please note that this should be used *only* for bootstrapping purposes

Synopsis

Generates the kubeconfig file for the kubelet to use and saves it to /etc/kubernetes/kubelet.conf file.

Please note that this should only be used for bootstrapping purposes. After your control plane is up, you should request all kubelet credentials from the CSR API.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig kubelet [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for kubelet

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

--node-name string

The node name that should be used for the kubelet client certificate

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the controller manager to use

Synopsis

Generates the kubeconfig file for the controller manager to use and saves it to /etc/kubernetes/controller-manager.conf file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig controller-manager [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for controller-manager

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the scheduler to use

Synopsis

Generates the kubeconfig file for the scheduler to use and saves it to /etc/kubernetes/scheduler.conf file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig scheduler [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for scheduler

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

1085

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Outputs a kubeconfig file for an additional user

Synopsis

Outputs a kubeconfig file for an additional user.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig user [flags]
```

Examples

```
  # Outputs a kubeconfig file for an additional user named foo
  kubeadm alpha phase kubeconfig user --client-name=foo
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--client-name string

The name of user. It will be used as the CN if client certificates are created

-h, --help

help for user

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

--org stringSlice

The orgnizations of the client certificate. It will be used as the O if client certificates are created

--token string

The token that should be used as the authentication mechanism for this kube-config, instead of client certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase kubelet

Use the following commands to manage the kubelet phase.

- config annotate-cri
- config download
- config enable-dynamic
- config upload
- config write-to-disk
- write-env-file

annotates the node with the given crisocket

Synopsis

Adds an annotation to the current node with the CRI socket specified in the kubeadm InitConfiguration object.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config annotate-cri [flags]
```

Examples

```
  kubeadm alpha phase kubelet config annotate-cri --config kubeadm.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for annotate-cri

--kubeconfig string   Default: ”/etc/kubernetes/admin.conf”

The KubeConfig file to use when talking to the cluster. If the flag is not set, a
set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Downloads the kubelet configuration from the cluster ConfigMap kubelet-config-
1.X, where X is the minor version of the kubelet.

Synopsis

Downloads the kubelet configuration from a ConfigMap of the form "kubelet-
config-1.X" in the cluster, where X is the minor version of the kubelet. Either
kubeadm autodetects the kubelet version by exec-ing "kubelet –version" or re-
spects the –kubelet-version parameter.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config download [flags]
```

Examples

```
  # Downloads the kubelet configuration from the ConfigMap in the cluster. Autodetects the k
  kubeadm alpha phase kubelet config download

  # Downloads the kubelet configuration from the ConfigMap in the cluster. Uses a specific c
  kubeadm alpha phase kubelet config download --kubelet-version v1.12.0
```

Options

-h, --help

help for download

--kubeconfig string   Default: ”/etc/kubernetes/kubelet.conf”

The KubeConfig file to use when talking to the cluster. If the flag is not set, a
set of standard locations are searched for an existing KubeConfig file.

--kubelet-version string

The desired version for the kubelet. Defaults to being autodetected from 'kubelet --version'.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

EXPERIMENTAL: Enables or updates dynamic kubelet configuration for a Node

Synopsis

Enables or updates dynamic kubelet configuration for a Node, against the kubelet-config-1.X ConfigMap in the cluster, where X is the minor version of the desired kubelet version.

WARNING: This feature is still experimental, and disabled by default. Enable only if you know what you are doing, as it may have surprising side-effects at this stage.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config enable-dynamic [flags]
```

Examples

```
  # Enables dynamic kubelet configuration for a Node.
  kubeadm alpha phase kubelet enable-dynamic-config --node-name node-1 --kubelet-version v1.

  WARNING: This feature is still experimental, and disabled by default. Enable only if you k
  may have surprising side-effects at this stage.
```

Options

-h, --help

help for enable-dynamic

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubelet-version string

The desired version for the kubelet

--node-name string

Name of the node that should enable the dynamic kubelet configuration

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Uploads kubelet configuration to a ConfigMap based on a kubeadm InitConfiguration file.

Synopsis

Uploads kubelet configuration extracted from the kubeadm InitConfiguration object to a ConfigMap of the form kubelet-config-1.X in the cluster, where X is the minor version of the current (API Server) Kubernetes version.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config upload [flags]
```

Examples

```
  # Uploads the kubelet configuration from the kubeadm Config file to a ConfigMap in the cl
  kubeadm alpha phase kubelet config upload --config kubeadm.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for upload

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Writes kubelet configuration to disk, either based on the –config argument.

Synopsis

Writes kubelet configuration to disk, based on the kubeadm configuration passed via "–config".

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config write-to-disk [flags]
```

Examples

```
  # Extracts the kubelet configuration from a kubeadm configuration file
  kubeadm alpha phase kubelet config write-to-disk --config kubeadm.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for write-to-disk

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Writes an environment file with runtime flags for the kubelet.

Synopsis

Writes an environment file with flags that should be passed to the kubelet executing on the master or node. This –config flag can either consume a InitConfiguration object or a JoinConfiguration one, as this function is used for both "kubeadm init" and "kubeadm join".

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet write-env-file [flags]
```

Examples

```
  # Writes a dynamic environment file with kubelet flags from a InitConfiguration file.
  kubeadm alpha phase kubelet write-env-file --config masterconfig.yaml

  # Writes a dynamic environment file with kubelet flags from a JoinConfiguration file.
  kubeadm alpha phase kubelet write-env-file --config nodeconfig.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for write-env-file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase controlplane

You can create all required static Pod files for the control plane components with the `all` subcommand, or selectively create the files.

- all
- apiserver
- controller-manager
- scheduler

Generates all static Pod manifest files necessary to establish the control plane

Synopsis

Generates all static Pod manifest files necessary to establish the control plane.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane all [flags]
```

Examples

```
# Generates all static Pod manifest files for control plane components,
# functionally equivalent to what generated by kubeadm init.
kubeadm alpha phase controlplane all

# Generates all static Pod manifest files using options read from a configuration file.
kubeadm alpha phase controlplane --config masterconfiguration.yaml
```

Options

--apiserver-advertise-address string

The IP address of the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--apiserver-extra-args mapStringString

A set of extra flags to pass to the API Server or override default ones in form of <flagname>=<value>

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--controller-manager-extra-args mapStringString

A set of extra flags to pass to the Controller Manager or override default ones in form of <flagname>=<value>

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for all

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

--scheduler-extra-args mapStringString

A set of extra flags to pass to the Scheduler or override default ones in form of <flagname>=<value>

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the API server static Pod manifest

Synopsis

Generates the static Pod manifest file for the API server and saves it into /etc/kubernetes/manifests/kube-apiserver.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane apiserver [flags]
```

Options

--apiserver-advertise-address string

The IP address of the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--apiserver-extra-args mapStringString

A set of extra flags to pass to the API Server or override default ones in form of <flagname>=<value>

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for apiserver

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the controller-manager static Pod manifest

Synopsis

Generates the static Pod manifest file for the controller-manager and saves it into /etc/kubernetes/manifests/kube-controller-manager.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane controller-manager [flags]
```


Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--controller-manager-extra-args mapStringString

A set of extra flags to pass to the Controller Manager or override default ones in form of <flagname>=<value>

-h, --help

help for controller-manager

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the scheduler static Pod manifest

Synopsis

Generates the static Pod manifest file for the scheduler and saves it into /etc/kubernetes/manifests/kube-scheduler.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane scheduler [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for scheduler

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--scheduler-extra-args mapStringString

A set of extra flags to pass to the Scheduler or override default ones in form of <flagname>=<value>

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase etcd

Use the following command to create a self-hosted, local etcd instance based on a static Pod file.

- etcd local

Generates the static Pod manifest file for a local, single-node etcd instance

Synopsis

Generates the static Pod manifest file for a local, single-node etcd instance and saves it to /etc/kubernetes/manifests/etcd.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase etcd local [flags]
```

Examples

```
  # Generates the static Pod manifest file for etcd, functionally
  # equivalent to what generated by kubeadm init.
  kubeadm alpha phase etcd local

  #  Generates the static Pod manifest file for etcd.
  kubeadm alpha phase etcd local --config masterconfiguration.yaml
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for local

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase mark-master

Use the following command to label and taint the node with the `node-role.kubernetes.io/master=""` key-value pair.

- mark-master

Mark a node as master

Synopsis

Applies a label that specifies that a node is a master and a taint that forces workloads to be deployed accordingly.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase mark-master [flags]
```

Examples

```
  # Applies master label and taint to the current node, functionally equivalent to what exe
  kubeadm alpha phase mark-master

  # Applies master label and taint to a specific node
  kubeadm alpha phase mark-master --node-name myNode
```

Options

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for mark-master

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--node-name string

The node name to which label and taints should apply

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase bootstrap-token

Use the following actions to fully configure bootstrap tokens. You can fully configure bootstrap tokens with the `all` subcommand, or selectively configure single elements.

- all
- create
- cluster-info
- node allow-auto-approve
- node allow-post-csrs

Makes all the bootstrap token configurations and creates an initial token

Synopsis

Bootstrap tokens are used for establishing bidirectional trust between a node joining the cluster and a the master node.

This command makes all the configurations required to make bootstrap tokens works and then creates an initial token.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token all [flags]
```

Examples

```
  # Makes all the bootstrap token configurations and creates an initial token, functionally
  # equivalent to what generated by kubeadm init.
  kubeadm alpha phase bootstrap-token all
```

Options

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--description string

A human friendly description of how this token is used.

--groups stringSlice   Default: [system:bootstrappers:kubeadm:default-node-token]

Extra groups that this token will authenticate as when used for authentication. Must match "\\Asystem:bootstrappers:[a-z0-9:-]{0,255}[a-z0-9]\\z"

-h, --help

help for all

--skip-token-print

Skip printing of the bootstrap token

--token string

The token to use for establishing bidirectional trust between nodes and masters. The format is [a-z0-9]{6}\.[a-z0-9]{16} - e.g. abcdef.0123456789abcdef

--token-ttl duration   Default: 24h0m0s

The duration before the token is automatically deleted (e.g. 1s, 2m, 3h). If set to '0', the token will never expire

--usages stringSlice   Default: [signing,authentication]

Describes the ways in which this token can be used. You can pass --usages multiple times or provide a comma separated list of options. Valid options: [signing,authentication]

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Creates a bootstrap token to be used for node joining

Synopsis

Creates a bootstrap token. If no token value is given, kubeadm will generate a random token instead.

Alternatively, you can use kubeadm token.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token create [flags]
```

Options

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--description string

A human friendly description of how this token is used.

--groups stringSlice   Default: [system:bootstrappers:kubeadm:default-node-token]

Extra groups that this token will authenticate as when used for authentication. Must match "\\Asystem:bootstrappers:[a-z0-9:-]{0,255}[a-z0-9]\\z"

-h, --help

help for create

--skip-token-print

Skip printing of the bootstrap token

--token string

The token to use for establishing bidirectional trust between nodes and masters. The format is [a-z0-9]{6}\.[a-z0-9]{16} - e.g. abcdef.0123456789abcdef

--token-ttl duration   Default: 24h0m0s

The duration before the token is automatically deleted (e.g. 1s, 2m, 3h). If set to '0', the token will never expire

--usages stringSlice   Default: [signing,authentication]

Describes the ways in which this token can be used. You can pass --usages multiple times or provide a comma separated list of options. Valid options: [signing,authentication]

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Uploads the cluster-info ConfigMap from the given kubeconfig file

Synopsis

Uploads the "cluster-info" ConfigMap in the "kube-public" namespace, populating it with cluster information extracted from the given kubeconfig file. The ConfigMap is used for the node bootstrap process in its initial phases, before the client trusts the API server.

See online documentation about Authenticating with Bootstrap Tokens for more details.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token cluster-info [flags]
```

Options

-h, --help

help for cluster-info

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Configures RBAC rules to allow the csrapprover controller automatically approve CSRs from a node bootstrap token

Synopsis

Configures RBAC rules to allow the csrapprover controller to automatically approve certificate signing requests generated by nodes joining the cluster. It configures also RBAC rules for certificates rotation (with auto approval of new certificates).

See online documentation about TLS bootstrapping for more details.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token node allow-auto-approve [flags]
```

Options

-h, --help

help for allow-auto-approve

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Configures RBAC to allow node bootstrap tokens to post CSRs in order for nodes to get long term certificate credentials

Synopsis

Configures RBAC rules to allow node bootstrap tokens to post a certificate signing request, thus enabling nodes joining the cluster to request long term certificate credentials.

See online documentation about TLS bootstrapping for more details.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token node allow-post-csrs [flags]
```

Options

-h, --help

help for allow-post-csrs

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase upload-config

You can use this command to upload the kubeadm configuration to your cluster. Alternatively, you can use kubeadm config.

- mark-master

Uploads the currently used configuration for kubeadm to a ConfigMap

Synopsis

Uploads the kubeadm init configuration of your cluster to a ConfigMap called kubeadm-config in the kube-system namespace. This enables correct configuration of system components and a seamless user experience when upgrading.

Alternatively, you can use kubeadm config.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase upload-config [flags]
```

Examples

```
  # uploads the configuration of your cluster
  kubeadm alpha phase upload-config --config=myConfig.yaml
```

Options

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for upload-config

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase addon

You can install all the available addons with the `all` subcommand, or install them selectively.

> **Note:** If `kubeadm` is invoked with `--feature-gates=CoreDNS=false`, kube-dns is installed.

- all
- kube-proxy
- coredns

Installs all addons to a Kubernetes cluster

Synopsis

Installs the CoreDNS and the kube-proxy addons components via the API server. Please note that although the DNS server is deployed, it will not be scheduled until CNI is installed.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase addon all [flags]
```

Examples

```
# Installs the CoreDNS and the kube-proxy addons components via the API server,
# functionally equivalent to what installed by kubeadm init.

kubeadm alpha phase selfhosting from-staticpods
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for all

--image-repository string   Default: "k8s.gcr.io"

Choose a container registry to pull control plane images from

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Installs the kube-proxy addon to a Kubernetes cluster

Synopsis

Installs the kube-proxy addon components via the API server.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase addon kube-proxy [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for kube-proxy

--image-repository string   Default: "k8s.gcr.io"

Choose a container registry to pull control plane images from

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Installs the CoreDNS addon to a Kubernetes cluster

Synopsis

Installs the CoreDNS addon components via the API server. Please note that although the DNS server is deployed, it will not be scheduled until CNI is installed.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase addon coredns [flags]
```

Options

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for coredns

--image-repository string   Default: "k8s.gcr.io"

Choose a container registry to pull control plane images from

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase self-hosting

> **Caution:** Self-hosting is an alpha feature. See kubeadm init documentation for self-hosting limitations.

- self-hosting

Converts a static Pod-hosted control plane into a self-hosted one

Synopsis

Converts static Pod files for control plane components into self-hosted DaemonSets configured via the Kubernetes API.

See the documentation for self-hosting limitations.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase selfhosting convert-from-staticpods [flags]
```

Examples

```
# Converts a static Pod-hosted control plane into a self-hosted one,
# functionally equivalent to what generated by kubeadm init executed
# with --feature-gates=SelfHosting=true.

kubeadm alpha phase selfhosting convert-from-staticpods
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for convert-from-staticpods

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

What's next

- kubeadm init to bootstrap a Kubernetes master node
- kubeadm join to connect a node to the cluster
- kubeadm reset to revert any changes made to this host by `kubeadm init` or `kubeadm join`

Edit This Page

Overview of kubeadm

- – What's next

Kubeadm is a tool built to provide `kubeadm init` and `kubeadm join` as best-practice "fast paths" for creating Kubernetes clusters.

kubeadm performs the actions necessary to get a minimum viable cluster up and running. By design, it cares only about bootstrapping, not about provisioning machines. Likewise, installing various nice-to-have addons, like the Kubernetes Dashboard, monitoring solutions, and cloud-specific addons, is not in scope.

Instead, we expect higher-level and more tailored tooling to be built on top of kubeadm, and ideally, using kubeadm as the basis of all deployments will make it easier to create conformant clusters.

What's next

- kubeadm init to bootstrap a Kubernetes master node
- kubeadm join to bootstrap a Kubernetes worker node and join it to the cluster
- kubeadm upgrade to upgrade a Kubernetes cluster to a newer version
- kubeadm config if you initialized your cluster using kubeadm v1.7.x or lower, to configure your cluster for `kubeadm upgrade`
- kubeadm token to manage tokens for `kubeadm join`
- kubeadm reset to revert any changes made to this host by `kubeadm init` or `kubeadm join`
- kubeadm version to print the kubeadm version
- kubeadm alpha to preview a set of features made available for gathering feedback from the community

Edit This Page

kubeadm init

This command initializes a Kubernetes master node.

- What's next

Run this command in order to set up the Kubernetes master.

Synopsis

Run this command in order to set up the Kubernetes master.

```
kubeadm init [flags]
```

Options

--apiserver-advertise-address string

The IP address the API Server will advertise it's listening on. Specify '0.0.0.0' to use the address of the default network interface.

--apiserver-bind-port int32   Default: 6443

Port for the API Server to bind to.

--apiserver-cert-extra-sans stringSlice

Optional extra Subject Alternative Names (SANs) to use for the API Server serving certificate. Can be both IP addresses and DNS names.

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save and store the certificates.

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental.

--cri-socket string   Default: "/var/run/dockershim.sock"

Specify the CRI socket to connect to.

--dry-run

Don't apply any changes; just output what would be done.

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for init

1112

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilege-dUser,Swap'. Value 'all' ignores errors from all checks.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane.

--node-name string

Specify the node name.

--pod-network-cidr string

Specify range of IP addresses for the pod network. If set, the control plane will automatically allocate CIDRs for every node.

--service-cidr string   Default: "10.96.0.0/12"

Use alternative range of IP address for service VIPs.

--service-dns-domain string   Default: "cluster.local"

Use alternative domain for services, e.g. "myorg.internal".

--skip-token-print

Skip printing of the default bootstrap token generated by 'kubeadm init'.

--token string

The token to use for establishing bidirectional trust between nodes and masters. The format is [a-z0-9]{6}\.[a-z0-9]{16} - e.g. abcdef.0123456789abcdef

--token-ttl duration   Default: 24h0m0s

The duration before the token is automatically deleted (e.g. 1s, 2m, 3h). If set to '0', the token will never expire

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Init workflow

kubeadm init bootstraps a Kubernetes master node by executing the following steps:

1. Runs a series of pre-flight checks to validate the system state before making changes. Some checks only trigger warnings, others are considered errors and will exit kubeadm until the problem is corrected or the user specifies `--ignore-preflight-errors=<list-of-errors>`.

2. Generates a self-signed CA (or using an existing one if provided) to set up identities for each component in the cluster. If the user has provided their own CA cert and/or key by dropping it in the cert directory configured via `--cert-dir` (`/etc/kubernetes/pki` by default) this step is skipped as described in the Using custom certificates document. The APIServer certs will have additional SAN entries for any `--apiserver-cert-extra-sans` arguments, lowercased if necessary.

3. Writes kubeconfig files in `/etc/kubernetes/` for the kubelet, the controller-manager and the scheduler to use to connect to the API server, each with its own identity, as well as an additional kubeconfig file for administration named `admin.conf`.

4. If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig` enabled, it writes the kubelet init configuration into the `/var/lib/kubelet/config/init/kubelet` file. See Set Kubelet parameters via a config file and Reconfigure a Node's Kubelet in a Live Cluster for more information about Dynamic Kubelet Configuration. This functionality is now by default disabled as it is behind a feature gate, but is expected to be a default in future versions.

5. Generates static Pod manifests for the API server, controller manager and scheduler. In case an external etcd is not provided, an additional static Pod manifest are generated for etcd.

Static Pod manifests are written to `/etc/kubernetes/manifests`; the kubelet watches this directory for Pods to create on startup.

Once control plane Pods are up and running, the `kubeadm init` sequence can continue.

1. If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig` enabled, it completes the kubelet dynamic configuration by creating a ConfigMap and some RBAC rules that enable kubelets to access to it, and updates the node by pointing `Node.spec.configSource` to the newly-created ConfigMap. This functionality is now by default disabled as it is behind a feature gate, but is expected to be a default in future versions.

2. Apply labels and taints to the master node so that no additional workloads will run there.

3. Generates the token that additional nodes can use to register themselves with the master in the future. Optionally, the user can provide a token via `--token`, as described in the kubeadm token docs.

4. Makes all the necessary configurations for allowing node joining with the Bootstrap Tokens and TLS Bootstrap mechanism:

1114

- Write a ConfigMap for making available all the information required for joining, and set up related RBAC access rules.

- Let Bootstrap Tokens access the CSR signing API.

- Configure auto-approval for new CSR requests.

See kubeadm join for additional info.

1. Installs a DNS server (CoreDNS) and the kube-proxy addon components via the API server. In Kubernetes version 1.11 and later CoreDNS is the default DNS server. To install kube-dns instead of CoreDNS, kubeadm must be invoked with `--feature-gates=CoreDNS=false`. Please note that although the DNS server is deployed, it will not be scheduled until CNI is installed.

2. If `kubeadm init` is invoked with the alpha self-hosting feature enabled, (`--feature-gates=SelfHosting=true`), the static Pod based control plane is transformed into a self-hosted control plane.

Using kubeadm init with a configuration file

> **Caution:** The config file is still considered alpha and may change in future versions.

It's possible to configure `kubeadm init` with a configuration file instead of command line flags, and some more advanced features may only be available as configuration file options. This file is passed in the `--config` option.

In Kubernetes 1.11 and later, the default configuration can be printed out using the kubeadm config print-default command. It is **recommended** that you migrate your old `v1alpha2` configuration to `v1alpha3` using the kubeadm config migrate command, because `v1alpha2` will be removed in Kubernetes 1.13.

For more details on each field in the `v1alpha3` configuration you can navigate to our API reference pages.

Adding kube-proxy parameters

For information about kube-proxy parameters in the kubeadm configuration see: - kube-proxy

For information about enabling IPVS mode with kubeadm see: - IPVS

Passing custom flags to control plane components

For information about passing flags to control plane components see: - control-plane-flags

Using custom images

By default, kubeadm pulls images from `k8s.gcr.io`, unless the requested Kubernetes version is a CI version. In this case, `gcr.io/kubernetes-ci-images` is used.

You can override this behavior by using kubeadm with a configuration file. Allowed customization are:

- To provide an alternative `imageRepository` to be used instead of `k8s.gcr.io`.
- To provide a `unifiedControlPlaneImage` to be used instead of different images for control plane components.
- To provide a specific `etcd.image` to be used instead of the image available at`k8s.gcr.io`.

Please note that the configuration field `kubernetesVersion` or the command line flag `--kubernetes-version` affect the version of the images.

Using custom certificates

By default, kubeadm generates all the certificates needed for a cluster to run. You can override this behavior by providing your own certificates.

To do so, you must place them in whatever directory is specified by the `--cert-dir` flag or `CertificatesDir` configuration file key. By default this is `/etc/kubernetes/pki`.

If a given certificate and private key pair exists, kubeadm skips the generation step and existing files are used for the prescribed use case. This means you can, for example, copy an existing CA into `/etc/kubernetes/pki/ca.crt` and `/etc/kubernetes/pki/ca.key`, and kubeadm will use this CA for signing the rest of the certs.

External CA mode

It is also possible to provide just the `ca.crt` file and not the `ca.key` file (this is only available for the root CA file, not other cert pairs). If all other certificates and kubeconfig files are in place, kubeadm recognizes this condition and activates the "External CA" mode. kubeadm will proceed without the CA key on disk.

Instead, run the controller-manager standalone with `--controllers=csrsigner` and point to the CA certificate and key.

Managing the kubeadm drop-in file for the kubelet

The kubeadm package ships with configuration for how the kubelet should be run. Note that the `kubeadm` CLI command never touches this drop-in file. This drop-in file belongs to the kubeadm deb/rpm package.

This is what it looks like:

```
[Service]
Environment="KUBELET_KUBECONFIG_ARGS=--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubele
Environment="KUBELET_SYSTEM_PODS_ARGS=--pod-manifest-path=/etc/kubernetes/manifests --allow-
Environment="KUBELET_NETWORK_ARGS=--network-plugin=cni --cni-conf-dir=/etc/cni/net.d --cni-b
Environment="KUBELET_DNS_ARGS=--cluster-dns=10.96.0.10 --cluster-domain=cluster.local"
Environment="KUBELET_AUTHZ_ARGS=--authorization-mode=Webhook --client-ca-file=/etc/kubernete
Environment="KUBELET_CADVISOR_ARGS="
Environment="KUBELET_CERTIFICATE_ARGS=--rotate-certificates=true --cert-dir=/var/lib/kubelet
ExecStart=/usr/bin/kubelet $KUBELET_KUBECONFIG_ARGS $KUBELET_SYSTEM_PODS_ARGS $KUBELET_NETWO
```

Here's a breakdown of what/why:

- `--bootstrap-kubeconfig=/etc/kubernetes/bootstrap-kubelet.conf` path to a kubeconfig file that is used to get client certificates for kubelet during node join. On success, a kubeconfig file is written to the path specified by `--kubeconfig`.
- `--kubeconfig=/etc/kubernetes/kubelet.conf` points to the kubeconfig file that tells the kubelet where the API server is. This file also has the kubelet's credentials.
- `--pod-manifest-path=/etc/kubernetes/manifests` specifies from where to read static Pod manifests used for starting the control plane.
- `--allow-privileged=true` allows this kubelet to run privileged Pods.
- `--network-plugin=cni` uses CNI networking.
- `--cni-conf-dir=/etc/cni/net.d` specifies where to look for the CNI spec file(s).
- `--cni-bin-dir=/opt/cni/bin` specifies where to look for the actual CNI binaries.
- `--cluster-dns=10.96.0.10` use this cluster-internal DNS server for `nameserver` entries in Pods' `/etc/resolv.conf`.
- `--cluster-domain=cluster.local` uses this cluster-internal DNS domain for `search` entries in Pods' `/etc/resolv.conf`.
- `--client-ca-file=/etc/kubernetes/pki/ca.crt` authenticates requests to the Kubelet API using this CA certificate.
- `--authorization-mode=Webhook` authorizes requests to the Kubelet API by `POST`-ing a `SubjectAccessReview` to the API server.
- `--rotate-certificates` auto rotate the kubelet client certificates by requesting new certificates from the `kube-apiserver` when the certificate expiration approaches.
- `--cert-dir` the directory where the TLS certs are located.

1117

Use kubeadm with CRI runtimes

Since v1.6.0, Kubernetes has enabled the use of CRI, Container Runtime Interface, by default. The container runtime used by default is Docker, which is enabled through the built-in `dockershim` CRI implementation inside of the `kubelet`.

Other CRI-based runtimes include:

- cri-containerd
- cri-o
- frakti
- rkt

Refer to the CRI installation instructions for more information.

After you have successfully installed `kubeadm` and `kubelet`, execute these two additional steps:

1. Install the runtime shim on every node, following the installation document in the runtime shim project listing above.

2. Configure kubelet to use the remote CRI runtime. Please remember to change `RUNTIME_ENDPOINT` to your own value like `/var/run/{your_runtime}.sock`:

```
cat > /etc/systemd/system/kubelet.service.d/20-cri.conf <<EOF
[Service]
Environment="KUBELET_EXTRA_ARGS=--container-runtime=remote --container-runtime-endpoint=$RUN
EOF
systemctl daemon-reload
```

Now `kubelet` is ready to use the specified CRI runtime, and you can continue with the `kubeadm init` and `kubeadm join` workflow to deploy Kubernetes cluster.

You may also want to set `--cri-socket` to `kubeadm init` and `kubeadm reset` when using an external CRI implementation.

Using internal IPs in your cluster

In order to set up a cluster where the master and worker nodes communicate with internal IP addresses (instead of public ones), execute following steps.

1. When running init, you must make sure you specify an internal IP for the API server's bind address, like so:

```
kubeadm init --apiserver-advertise-address=<private-master-ip>
```

1. When a master or worker node has been provisioned, add a flag to `/etc/systemd/system/kubelet.service.d/10-kubeadm.conf`   that specifies the private IP of the worker node:

```
--node-ip=<private-node-ip>
```

1. Finally, when you run `kubeadm join`, make sure you provide the private IP of the API server addressed as defined in step 1.

Setting the node name

By default, `kubeadm` assigns a node name based on a machine's host address. You can override this setting with the `--node-name`flag. The flag passes the appropriate `--hostname-override` to the kubelet.

Be aware that overriding the hostname can interfere with cloud providers.

Self-hosting the Kubernetes control plane

As of 1.8, you can experimentally create a *self-hosted* Kubernetes control plane. This means that key components such as the API server, controller manager, and scheduler run as DaemonSet pods configured via the Kubernetes API instead of static pods configured in the kubelet via static files.

To create a self-hosted cluster, pass the flag `--feature-gates=SelfHosting=true` to `kubeadm init`.

> **Caution:** `SelfHosting` is an alpha feature. It is deprecated in 1.12 and will be removed in 1.13.

Caveats

Self-hosting in 1.8 has some important limitations. In particular, a self-hosted cluster *cannot recover from a reboot of the master node* without manual intervention. This and other limitations are expected to be resolved before self-hosting graduates from alpha.

By default, self-hosted control plane Pods rely on credentials loaded from `hostPath` volumes. Except for initial creation, these credentials are not managed by kubeadm. You can use `--feature-gates=StoreCertsInSecrets=true` to enable an experimental mode where control plane credentials are loaded from Secrets instead. This requires very careful control over the authentication and authorization configuration for your cluster, and may not be appropriate for your environment.

> **Caution:** `StoreCertsInSecrets` is an alpha feature. It is deprecated in 1.12 and will be removed in 1.13.

In kubeadm 1.8, the self-hosted portion of the control plane does not include etcd, which still runs as a static Pod.

Process

The self-hosting bootstrap process is documented in the kubeadm design document.

In summary, `kubeadm init --feature-gates=SelfHosting=true` works as follows:

1. Waits for this bootstrap static control plane to be running and healthy. This is identical to the `kubeadm init` process without self-hosting.

2. Uses the static control plane Pod manifests to construct a set of DaemonSet manifests that will run the self-hosted control plane. It also modifies these manifests where necessary, for example adding new volumes for secrets.

3. Creates DaemonSets in the `kube-system` namespace and waits for the resulting Pods to be running.

4. Once self-hosted Pods are operational, their associated static Pods are deleted and kubeadm moves on to install the next component. This triggers kubelet to stop those static Pods.

5. When the original static control plane stops, the new self-hosted control plane is able to bind to listening ports and become active.

This process (steps 3-6) can also be triggered with `kubeadm phase selfhosting convert-from-staticpods`.

Running kubeadm without an internet connection

For running kubeadm without an internet connection you have to pre-pull the required master images for the version of choice:

Image Name	v1.10 release branch version
k8s.gcr.io/kube-apiserver-${ARCH}	v1.10.x
k8s.gcr.io/kube-controller-manager-${ARCH}	v1.10.x
k8s.gcr.io/kube-scheduler-${ARCH}	v1.10.x
k8s.gcr.io/kube-proxy-${ARCH}	v1.10.x
k8s.gcr.io/etcd-${ARCH}	3.1.12
k8s.gcr.io/pause-${ARCH}	3.1
k8s.gcr.io/k8s-dns-sidecar-${ARCH}	1.14.8
k8s.gcr.io/k8s-dns-kube-dns-${ARCH}	1.14.8
k8s.gcr.io/k8s-dns-dnsmasq-nanny-${ARCH}	1.14.8
coredns/coredns	1.0.6

Here `v1.10.x` means the "latest patch release of the v1.10 branch".

`${ARCH}` can be one of: `amd64`, `arm`, `arm64`, `ppc64le` or `s390x`.

If you run Kubernetes version 1.10 or earlier, and if you set `--feature-gates=CoreDNS=true`, you must also use the `coredns/coredns` image, instead of the three `k8s-dns-*` images.

In Kubernetes 1.11 and later, you can list and pull the images using the `kubeadm config images` sub-command:

```
kubeadm config images list
kubeadm config images pull
```

Starting with Kubernetes 1.12, the `k8s.gcr.io/kube-*`, `k8s.gcr.io/etcd` and `k8s.gcr.io/pause` images don't require an `-${ARCH}` suffix.

Automating kubeadm

Rather than copying the token you obtained from `kubeadm init` to each node, as in the basic kubeadm tutorial, you can parallelize the token distribution for easier automation. To implement this automation, you must know the IP address that the master will have after it is started.

1. Generate a token. This token must have the form `<6 character string>.<16 character string>`. More formally, it must match the regex: `[a-z0-9]{6}\.[a-z0-9]{16}`.

   kubeadm can generate a token for you:

   ```
   kubeadm token generate
   ```

2. Start both the master node and the worker nodes concurrently with this token. As they come up they should find each other and form the cluster. The same `--token` argument can be used on both `kubeadm init` and `kubeadm join`.

Once the cluster is up, you can grab the admin credentials from the master node at `/etc/kubernetes/admin.conf` and use that to talk to the cluster.

Note that this style of bootstrap has some relaxed security guarantees because it does not allow the root CA hash to be validated with `--discovery-token-ca-cert-hash` (since it's not generated when the nodes are provisioned). For details, see the kubeadm join.

What's next

- kubeadm join to bootstrap a Kubernetes worker node and join it to the cluster

- kubeadm upgrade to upgrade a Kubernetes cluster to a newer version
- kubeadm reset to revert any changes made to this host by `kubeadm init` or `kubeadm join`

Edit This Page

kubeadm join

This command initializes a Kubernetes worker node and joins it to the cluster.

- What's next

Run this on any machine you wish to join an existing cluster

Synopsis

When joining a kubeadm initialized cluster, we need to establish bidirectional trust. This is split into discovery (having the Node trust the Kubernetes Master) and TLS bootstrap (having the Kubernetes Master trust the Node).

There are 2 main schemes for discovery. The first is to use a shared token along with the IP address of the API server. The second is to provide a file - a subset of the standard kubeconfig file. This file can be a local file or downloaded via an HTTPS URL. The forms are kubeadm join –discovery-token abcdef.1234567890abcdef 1.2.3.4:6443, kubeadm join –discovery-file path/to/file.conf, or kubeadm join –discovery-file `https://url/file.conf`. Only one form can be used. If the discovery information is loaded from a URL, HTTPS must be used. Also, in that case the host installed CA bundle is used to verify the connection.

If you use a shared token for discovery, you should also pass the –discovery-token-ca-cert-hash flag to validate the public key of the root certificate authority (CA) presented by the Kubernetes Master. The value of this flag is specified as ":", where the supported hash type is "sha256". The hash is calculated over the bytes of the Subject Public Key Info (SPKI) object (as in RFC7469). This value is available in the output of "kubeadm init" or can be calculated using standard tools. The –discovery-token-ca-cert-hash flag may be repeated multiple times to allow more than one public key.

If you cannot know the CA public key hash ahead of time, you can pass the –discovery-token-unsafe-skip-ca-verification flag to disable this verification. This weakens the kubeadm security model since other nodes can potentially impersonate the Kubernetes Master.

The TLS bootstrap mechanism is also driven via a shared token. This is used to temporarily authenticate with the Kubernetes Master to submit a certificate signing request (CSR) for a locally created key pair. By default, kubeadm will

set up the Kubernetes Master to automatically approve these signing requests. This token is passed in with the –tls-bootstrap-token abcdef.1234567890abcdef flag.

Often times the same token is used for both parts. In this case, the –token flag can be used instead of specifying each token individually.

```
kubeadm join [flags]
```

Options

--apiserver-advertise-address string

If the node should host a new control plane instance, the IP address the API Server will advertise it's listening on.

--apiserver-bind-port int32   Default: 6443

If the node should host a new control plane instance, the port for the API Server to bind to.

--config string

Path to kubeadm config file.

--cri-socket string   Default: "/var/run/dockershim.sock"

Specify the CRI socket to connect to.

--discovery-file string

A file or url from which to load cluster information.

--discovery-token string

A token used to validate cluster information fetched from the api server.

--discovery-token-ca-cert-hash stringSlice

For token-based discovery, validate that the root CA public key matches this hash (format: "<type>:<value>").

--discovery-token-unsafe-skip-ca-verification

For token-based discovery, allow joining without --discovery-token-ca-cert-hash pinning.

--experimental-control-plane

Create a new control plane instance on this node

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:

1123

Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for join

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilege-dUser,Swap'. Value 'all' ignores errors from all checks.

--node-name string

Specify the node name.

--tls-bootstrap-token string

A token used for TLS bootstrapping.

--token string

Use this token for both discovery-token and tls-bootstrap-token.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

The joining workflow

`kubeadm join` bootstraps a Kubernetes worker node and joins it to the cluster. This action consists of the following steps:

1. kubeadm downloads necessary cluster information from the API server. By default, it uses the bootstrap token and the CA key hash to verify the authenticity of that data. The root CA can also be discovered directly via a file or URL.

2. If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig` enabled, it first retrieves the kubelet init configuration from the master and writes it to the disk. When kubelet starts up, kubeadm updates the node `Node.spec.configSource` property of the node. See Set Kubelet parameters via a config file and Reconfigure a Node's Kubelet in a Live Cluster for more information about Dynamic Kubelet Configuration.

3. Once the cluster information is known, kubelet can start the TLS boot-strapping process.

The TLS bootstrap uses the shared token to temporarily authenticate with the Kubernetes API server to submit a certificate signing request (CSR); by default the control plane signs this CSR request automatically.

1. Finally, kubeadm configures the local kubelet to connect to the API server with the definitive identity assigned to the node.

Discovering what cluster CA to trust

The kubeadm discovery has several options, each with security tradeoffs. The right method for your environment depends on how you provision nodes and the security expectations you have about your network and node lifecycles.

Token-based discovery with CA pinning

This is the default mode in Kubernetes 1.8 and above. In this mode, kubeadm downloads the cluster configuration (including root CA) and validates it using the token as well as validating that the root CA public key matches the provided hash and that the API server certificate is valid under the root CA.

The CA key hash has the format `sha256:<hex_encoded_hash>`. By default, the hash value is returned in the `kubeadm join` command printed at the end of `kubeadm init` or in the output of `kubeadm token create --print-join-command`. It is in a standard format (see RFC7469) and can also be calculated by 3rd party tools or provisioning systems. For example, using the OpenSSL CLI:

```
openssl x509 -pubkey -in /etc/kubernetes/pki/ca.crt | openssl rsa -pubin -outform der 2>/dev
```

Example `kubeadm join` command:

```
kubeadm join --discovery-token abcdef.1234567890abcdef --discovery-token-ca-cert-hash sha256
```

Advantages:

- Allows bootstrapping nodes to securely discover a root of trust for the master even if other worker nodes or the network are compromised.

- Convenient to execute manually since all of the information required fits into a single `kubeadm join` command that is easy to copy and paste.

Disadvantages:

- The CA hash is not normally known until the master has been provisioned, which can make it more difficult to build automated provisioning tools that use kubeadm. By generating your CA in beforehand, you may workaround this limitation though.

1125

Token-based discovery without CA pinning

This was the default in Kubernetes 1.7 and earlier, but comes with some important caveats. This mode relies only on the symmetric token to sign (HMAC-SHA256) the discovery information that establishes the root of trust for the master. It's still possible in Kubernetes 1.8 and above using the `--discovery-token-unsafe-skip-ca-verification` flag, but you should consider using one of the other modes if possible.

Example `kubeadm join` command:

```
kubeadm join --token abcdef.1234567890abcdef --discovery-token-unsafe-skip-ca-verification 1
```

Advantages:

- Still protects against many network-level attacks.

- The token can be generated ahead of time and shared with the master and worker nodes, which can then bootstrap in parallel without coordination. This allows it to be used in many provisioning scenarios.

Disadvantages:

- If an attacker is able to steal a bootstrap token via some vulnerability, they can use that token (along with network-level access) to impersonate the master to other bootstrapping nodes. This may or may not be an appropriate tradeoff in your environment.

File or HTTPS-based discovery

This provides an out-of-band way to establish a root of trust between the master and bootstrapping nodes. Consider using this mode if you are building automated provisioning using kubeadm.

Example `kubeadm join` commands:

- `kubeadm join --discovery-file path/to/file.conf` (local file)

- `kubeadm join --discovery-file https://url/file.conf` (remote HTTPS URL)

Advantages:

- Allows bootstrapping nodes to securely discover a root of trust for the master even if the network or other worker nodes are compromised.

Disadvantages:

- Requires that you have some way to carry the discovery information from the master to the bootstrapping nodes. This might be possible, for example, via your cloud provider or provisioning tool. The information in this file is not secret, but HTTPS or equivalent is required to ensure its integrity.

1126

Securing your installation even more

The defaults for kubeadm may not work for everyone. This section documents how to tighten up a kubeadm installation at the cost of some usability.

Turning off auto-approval of node client certificates

By default, there is a CSR auto-approver enabled that basically approves any client certificate request for a kubelet when a Bootstrap Token was used when authenticating. If you don't want the cluster to automatically approve kubelet client certs, you can turn it off by executing this command:

```
$ kubectl delete clusterrole kubeadm:node-autoapprove-bootstrap
```

After that, `kubeadm join` will block until the admin has manually approved the CSR in flight:

```
$ kubectl get csr
NAME                                                        AGE       REQUESTOR              C
node-csr-c69HXe7aYcqkS1bKmH4faEnHAWxn6i2bHZ2mDO4jZyQ   18s       system:bootstrap:878f07   F

$ kubectl certificate approve node-csr-c69HXe7aYcqkS1bKmH4faEnHAWxn6i2bHZ2mDO4jZyQ
certificatesigningrequest "node-csr-c69HXe7aYcqkS1bKmH4faEnHAWxn6i2bHZ2mDO4jZyQ" approved

$ kubectl get csr
NAME                                                        AGE       REQUESTOR              C
node-csr-c69HXe7aYcqkS1bKmH4faEnHAWxn6i2bHZ2mDO4jZyQ   1m        system:bootstrap:878f07   A
```

Only after `kubectl certificate approve` has been run, `kubeadm join` can proceed.

Turning off public access to the cluster-info ConfigMap

In order to achieve the joining flow using the token as the only piece of validation information, a ConfigMap with some data needed for validation of the master's identity is exposed publicly by default. While there is no private data in this ConfigMap, some users might wish to turn it off regardless. Doing so will disable the ability to use the `--discovery-token` flag of the `kubeadm join` flow. Here are the steps to do so:

- Fetch the `cluster-info` file from the API Server:

```
$ kubectl -n kube-public get cm cluster-info -o yaml | grep "kubeconfig:" -A11 | grep "apiVe
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <ca-cert>
    server: https://<ip>:<port>
```

1127

```
  name: ""
contexts: []
current-context: ""
kind: Config
preferences: {}
users: []
```

- Use the `cluster-info.yaml` file as an argument to `kubeadm join --discovery-file`.

- Turn off public access to the `cluster-info` ConfigMap:

```
$ kubectl -n kube-public delete rolebinding kubeadm:bootstrap-signer-clusterinfo
```

These commands should be run after `kubeadm init` but before `kubeadm join`.

Using kubeadm join with a configuration file

> **Caution:** The config file is still considered alpha and may change in future versions.

It's possible to configure `kubeadm join` with a configuration file instead of command line flags, and some more advanced features may only be available as configuration file options. This file is passed using the `--config` flag and it must contain a `JoinConfiguration` structure.

To print the default values of `JoinConfiguration` run the following command:

```
kubeadm config print-default --api-objects=JoinConfiguration
```

For details on individual fields in `JoinConfiguration` see the godoc.

What's next

- kubeadm init to bootstrap a Kubernetes master node
- kubeadm token to manage tokens for `kubeadm join`
- kubeadm reset to revert any changes made to this host by `kubeadm init` or `kubeadm join`

Edit This Page

kubeadm upgrade

`kubeadm upgrade` is a user-friendly command that wraps complex upgrading logic behind one command, with support for both planning an upgrade and actually performing it. `kubeadm upgrade` can also be used for downgrading cluster if necessary.

1128

- kubeadm upgrade guidance
- kubeadm upgrade plan
- kubeadm upgrade apply
- kubeadm upgrade diff
- kubeadm upgrade node config
- kubeadm upgrade node experimental-control-plane
- What's next

kubeadm upgrade guidance

Every upgrade process might be a bit different, so we've documented each minor upgrade process individually. For more version-specific upgrade guidance, see the following resources:

- 1.10 to 1.11 upgrades
- 1.11 to 1.12 upgrades

For older versions, please refer to older documentation sets on the Kubernetes website.

In Kubernetes v1.11.0 and later, you can use `kubeadm upgrade diff` to see the changes that would be applied to static pod manifests.

kubeadm upgrade plan

Check which versions are available to upgrade to and validate whether your current cluster is upgradeable. To skip the internet check, pass in the optional [version] parameter.

Synopsis

Check which versions are available to upgrade to and validate whether your current cluster is upgradeable. To skip the internet check, pass in the optional [version] parameter.

```
kubeadm upgrade plan [version] [flags]
```

Options

--allow-experimental-upgrades

Show unstable versions of Kubernetes as an upgrade alternative and allow upgrading to an alpha/beta/release candidate versions of Kubernetes.

--allow-release-candidate-upgrades

1129

Show release candidate versions of Kubernetes as an upgrade alternative and allow upgrading to a release candidate versions of Kubernetes.

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for plan

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilegedUser,Swap'. Value 'all' ignores errors from all checks.

--kubeconfig string   Default: "/Users/zarnold/.kube/config"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--print-config

Specifies whether the configuration file that will be used in the upgrade should be printed or not.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm upgrade apply

Upgrade your Kubernetes cluster to the specified version.

Synopsis

Upgrade your Kubernetes cluster to the specified version.

```
kubeadm upgrade apply [version]
```

1130

Options

--allow-experimental-upgrades

Show unstable versions of Kubernetes as an upgrade alternative and allow upgrading to an alpha/beta/release candidate versions of Kubernetes.

--allow-release-candidate-upgrades

Show release candidate versions of Kubernetes as an upgrade alternative and allow upgrading to a release candidate versions of Kubernetes.

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--cri-socket string   Default: ”/var/run/dockershim.sock”

Specify the CRI socket to connect to.

--dry-run

Do not change any state, just output what actions would be performed.

--etcd-upgrade   Default: true

Perform the upgrade of etcd.

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-f, --force

Force upgrading although some requirements might not be met. This also implies non-interactive mode.

-h, --help

help for apply

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: ’IsPrivilegedUser,Swap’. Value ’all’ ignores errors from all checks.

--image-pull-timeout duration   Default: 15m0s

The maximum amount of time to wait for the control plane pods to be downloaded.

--kubeconfig string   Default: "/Users/zarnold/.kube/config"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--print-config

Specifies whether the configuration file that will be used in the upgrade should be printed or not.

-y, --yes

Perform the upgrade and do not prompt for confirmation (non-interactive mode).

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm upgrade diff

Show what differences would be applied to existing static pod manifests. See also: kubeadm upgrade apply –dry-run

Synopsis

Show what differences would be applied to existing static pod manifests. See also: kubeadm upgrade apply –dry-run

```
kubeadm upgrade diff [version] [flags]
```

Options

--api-server-manifest string   Default: "/etc/kubernetes/manifests/kube-apiserver.yaml"

path to API server manifest

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-c, --context-lines int   Default: 3

How many lines of context in the diff

--controller-manager-manifest string   Default: "/etc/kubernetes/manifests/kube-controller-manager.yaml"

path to controller manifest

-h, --help

help for diff

--scheduler-manifest string   Default: "/etc/kubernetes/manifests/kube-scheduler.yaml"

path to scheduler manifest

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm upgrade node config

Downloads the kubelet configuration from the cluster ConfigMap kubelet-config-1.X, where X is the minor version of the kubelet.

Synopsis

Downloads the kubelet configuration from a ConfigMap of the form "kubelet-config-1.X" in the cluster, where X is the minor version of the kubelet. kubeadm uses the –kubelet-version parameter to determine what the desired kubelet version is. Give

```
kubeadm upgrade node config [flags]
```

Examples

```
  # Downloads the kubelet configuration from the ConfigMap in the cluster. Uses a specific c
  kubeadm upgrade node config --kubelet-version v1.12.0

  # Simulates the downloading of the kubelet configuration from the ConfigMap in the cluster
  # version. Does not change any state locally on the node.
  kubeadm upgrade node config --kubelet-version v1.12.0 --dry-run
```

Options

--dry-run

Do not change any state, just output the actions that would be performed.

-h, --help

help for config

--kubeconfig string   Default: "/etc/kubernetes/kubelet.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubelet-version string

The *desired* version for the kubelet after the upgrade.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm upgrade node experimental-control-plane

Upgrades the control plane instance deployed on this node. IMPORTANT. This command should be executed after executing `kubeadm upgrade apply` on another control plane instance

Synopsis

Downloads the kubelet configuration from a ConfigMap of the form "kubelet-config-1.X" in the cluster, where X is the minor version of the kubelet. kubeadm uses the –kubelet-version parameter to determine what the desired kubelet version is. Give

```
kubeadm upgrade node experimental-control-plane [flags]
```

Examples

```
  # Downloads the kubelet configuration from the ConfigMap in the cluster. Uses a specific c
  kubeadm upgrade node config --kubelet-version v1.12.0

  # Simulates the downloading of the kubelet configuration from the ConfigMap in the cluster
  # version. Does not change any state locally on the node.
```

```
kubeadm upgrade node config --kubelet-version v1.12.0 --dry-run
```

Options

--dry-run

Do not change any state, just output the actions that would be performed.

-h, --help

help for experimental-control-plane

--kubeconfig string   Default: "/etc/kubernetes/kubelet.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

What's next

- kubeadm config if you initialized your cluster using kubeadm v1.7.x or lower, to configure your cluster for `kubeadm upgrade`

Edit This Page

kubeadm config

Beginning with v1.8.0, kubeadm uploads the configuration of your cluster to a ConfigMap called `kubeadm-config` in the `kube-system` namespace, and later reads the ConfigMap when upgrading. This enables correct configuration of system components, and provides a seamless user experience.

You can execute `kubeadm config view` to view the ConfigMap. If you initialized your cluster using kubeadm v1.7.x or lower, you must use `kubeadm config upload` to create the ConfigMap before you may use `kubeadm upgrade`.

In Kubernetes v1.11.0, some new commands were added. You can use `kubeadm config print-default` to print the default configuration and `kubeadm config migrate` to convert your old configuration files to a newer version. `kubeadm config images list` and `kubeadm config images pull` can be used to list and pull the images that kubeadm requires.

- kubeadm config upload from-file
- kubeadm config upload from-flags
- kubeadm config view
- kubeadm config print-default
- kubeadm config migrate
- kubeadm config images list
- kubeadm config images pull
- What's next

kubeadm config upload from-file

Upload a configuration file to the in-cluster ConfigMap for kubeadm configuration.

Synopsis

Using this command, you can upload configuration to the ConfigMap in the cluster using the same config file you gave to 'kubeadm init'. If you initialized your cluster using a v1.7.x or lower kubeadm client and used the –config option, you need to run this command with the same config file before upgrading to v1.8 using 'kubeadm upgrade'.

The configuration is located in the "kube-system" namespace in the "kubeadm-config" ConfigMap.

```
kubeadm config upload from-file [flags]
```

Options

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental.

-h, --help

help for from-file

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm config upload from-flags

Create the in-cluster configuration file for the first time from using flags.

Synopsis

Using this command, you can upload configuration to the ConfigMap in the cluster using the same flags you gave to 'kubeadm init'. If you initialized your cluster using a v1.7.x or lower kubeadm client and set certain flags, you need to run this command with the same flags before upgrading to v1.8 using 'kubeadm upgrade'.

The configuration is located in the "kube-system" namespace in the "kubeadm-config" ConfigMap.

```
kubeadm config upload from-flags [flags]
```

Options

--apiserver-advertise-address string

The IP address the API Server will advertise it's listening on. Specify '0.0.0.0' to use the address of the default network interface.

--apiserver-bind-port int32   Default: 6443

Port for the API Server to bind to.

--apiserver-cert-extra-sans stringSlice

Optional extra Subject Alternative Names (SANs) to use for the API Server serving certificate. Can be both IP addresses and DNS names.

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save and store the certificates.

--cri-socket string   Default: "/var/run/dockershim.sock"

Specify the CRI socket to connect to.

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for from-flags

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane.

--node-name string

Specify the node name.

--pod-network-cidr string

Specify range of IP addresses for the pod network. If set, the control plane will automatically allocate CIDRs for every node.

--service-cidr string   Default: "10.96.0.0/12"

Use alternative range of IP address for service VIPs.

--service-dns-domain string   Default: "cluster.local"

Use alternative domain for services, e.g. "myorg.internal".

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm config view

View the kubeadm configuration stored inside the cluster.

Synopsis

Using this command, you can view the ConfigMap in the cluster where the configuration for kubeadm is located.

The configuration is located in the "kube-system" namespace in the "kubeadm-config" ConfigMap.

```
kubeadm config view [flags]
```

Options

-h, --help

help for view

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm config print-default

Print the default values for a kubeadm configuration object.

Synopsis

This command prints the default InitConfiguration object that is used for 'kubeadm init' and 'kubeadm upgrade', and the default JoinConfiguration object that is used for 'kubeadm join'.

Note that sensitive values like the Bootstrap Token fields are replaced with silly values like {"abcdef.0123456789abcdef" "" "nil" [] []} in order to pass validation but not perform the real computation for creating a token.

```
kubeadm config print-default [flags]
```

Options

--api-objects stringSlice

A comma-separated list for API objects to print the default values for. Available values: [InitConfiguration ClusterConfiguration JoinConfiguration KubeProxyConfiguration KubeletConfiguration MasterConfiguration]. This flag unset means 'print all known objects'

-h, --help

help for print-default

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm config migrate

Read an older version of the kubeadm configuration API types from a file, and output the similar config object for the newer version.

Synopsis

This command lets you convert configuration objects of older versions to the latest supported version, locally in the CLI tool without ever touching anything in the cluster. In this version of kubeadm, the following API versions are supported: - kubeadm.k8s.io/v1alpha2 - kubeadm.k8s.io/v1alpha3

Further, kubeadm can only write out config of version "kubeadm.k8s.io/v1alpha3", but read both types. So regardless of what version you pass to the –old-config parameter here, the API object will be read, deserialized, defaulted, converted, validated, and re-serialized when written to stdout or –new-config if specified.

In other words, the output of this command is what kubeadm actually would read internally if you submitted this file to "kubeadm init"

```
kubeadm config migrate [flags]
```

Options

-h, --help

help for migrate

--new-config string

Path to the resulting equivalent kubeadm config file using the new API version. Optional, if not specified output will be sent to STDOUT.

--old-config string

Path to the kubeadm config file that is using an old API version and should be converted. This flag is mandatory.

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm config images list

Print a list of images kubeadm will use. The configuration file is used in case any images or image repositories are customized.

Synopsis

Print a list of images kubeadm will use. The configuration file is used in case any images or image repositories are customized.

```
kubeadm config images list [flags]
```

Options

--config string

Path to kubeadm config file.

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for list

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane.

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm config images pull

Pull images used by kubeadm.

Synopsis

Pull images used by kubeadm.

```
kubeadm config images pull [flags]
```

Options

--config string

Path to kubeadm config file.

--cri-socket string   Default: "/var/run/dockershim.sock"

Specify the CRI socket to connect to.

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for pull

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane.

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

What's next

- kubeadm upgrade to upgrade a Kubernetes cluster to a newer version

Edit This Page

kubeadm reset

This command reverts any changes made by `kubeadm init` or `kubeadm join`.

- What's next

Run this to revert any changes made to this host by 'kubeadm init' or 'kubeadm join'.

Synopsis

Run this to revert any changes made to this host by 'kubeadm init' or 'kubeadm join'.

```
kubeadm reset [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path to the directory where the certificates are stored. If specified, clean this directory.

--cri-socket string   Default: "/var/run/dockershim.sock"

The path to the CRI socket to use with crictl when cleaning up containers.

-f, --force

Reset the node without prompting for confirmation.

-h, --help

help for reset

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilege-dUser,Swap'. Value 'all' ignores errors from all checks.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

External etcd clean up!

`kubeadm reset` will not delete any etcd data if external etcd is used. This means that if you run `kubeadm init` again using the same etcd endpoints, you will see state from previous clusters.

To wipe etcd data it is recommended you use a client like etcdctl, such as:

```
etcdctl del "" --prefix
```

See the etcd documentation for more information.

What's next

- kubeadm init to bootstrap a Kubernetes master node
- kubeadm join to bootstrap a Kubernetes worker node and join it to the cluster

Edit This Page

kubeadm token

Bootstrap tokens are used for establishing bidirectional trust between a node joining the cluster and a master node, as described in authenticating with bootstrap tokens.

`kubeadm init` creates an initial token with a 24-hour TTL. The following commands allow you to manage such a token and also to create and manage new ones.

- kubeadm token create
- kubeadm token delete

1144

- kubeadm token generate
- kubeadm token list
- What's next

kubeadm token create

Create bootstrap tokens on the server.

Synopsis

This command will create a bootstrap token for you. You can specify the usages for this token, the "time to live" and an optional human friendly description.

The [token] is the actual token to write. This should be a securely generated random token of the form "[a-z0-9]{6}.[a-z0-9]{16}". If no [token] is given, kubeadm will generate a random token instead.

```
kubeadm token create [token]
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--description string

A human friendly description of how this token is used.

--groups stringSlice   Default: [system:bootstrappers:kubeadm:default-node-token]

Extra groups that this token will authenticate as when used for authentication. Must match "\\Asystem:bootstrappers:[a-z0-9:-]{0,255}[a-z0-9]\\z"

-h, --help

help for create

--print-join-command

Instead of printing only the token, print the full 'kubeadm join' flag needed to join the cluster using the token.

--ttl duration   Default: 24h0m0s

The duration before the token is automatically deleted (e.g. 1s, 2m, 3h). If set to '0', the token will never expire

1145

--usages stringSlice   Default: [signing,authentication]

Describes the ways in which this token can be used. You can pass --usages multiple times or provide a comma separated list of options. Valid options: [signing,authentication]

Options inherited from parent commands

--dry-run

Whether to enable dry-run mode or not

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm token delete

Delete bootstrap tokens on the server.

Synopsis

This command will delete a given bootstrap token for you.

The [token-value] is the full Token of the form "[a-z0-9]{6}.[a-z0-9]{16}" or the Token ID of the form "[a-z0-9]{6}" to delete.

```
kubeadm token delete [token-value]
```

Options

-h, --help

help for delete

Options inherited from parent commands

--dry-run

Whether to enable dry-run mode or not

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm token generate

Generate and print a bootstrap token, but do not create it on the server.

Synopsis

This command will print out a randomly-generated bootstrap token that can be used with the "init" and "join" commands.

You don't have to use this command in order to generate a token. You can do so yourself as long as it is in the format "[a-z0-9]{6}.[a-z0-9]{16}". This command is provided for convenience to generate tokens in the given format.

You can also use "kubeadm init" without specifying a token and it will generate and print one for you.

```
kubeadm token generate [flags]
```

Options

-h, --help

help for generate

Options inherited from parent commands

--dry-run

Whether to enable dry-run mode or not

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

1147

kubeadm token list

List bootstrap tokens on the server.

Synopsis

This command will list all bootstrap tokens for you.

```
kubeadm token list [flags]
```

Options

-h, --help

help for list

Options inherited from parent commands

--dry-run

Whether to enable dry-run mode or not

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

What's next

- kubeadm join to bootstrap a Kubernetes worker node and join it to the cluster

Edit This Page

kubeadm version

This command prints the version of kubeadm.

Print the version of kubeadm

Synopsis

Print the version of kubeadm

```
kubeadm version [flags]
```

Options

-h, --help

help for version

-o, --output string

Output format; available options are 'yaml', 'json' and 'short'

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Edit This Page

kubeadm alpha

- – kubeadm alpha phase preflight
  – kubeadm alpha phase certs
  – kubeadm alpha phase certs renew
  – kubeadm alpha phase kubeconfig
  – kubeadm alpha phase kubelet
  – kubeadm alpha phase controlplane
  – kubeadm alpha phase etcd
  – kubeadm alpha phase mark-master
  – kubeadm alpha phase bootstrap-token
  – kubeadm alpha phase upload-config
  – kubeadm alpha phase addon
  – kubeadm alpha phase self-hosting
  – What's next

  Caution: `kubeadm alpha` provides a preview of a set of features
  made available for gathering feedback from the community. Please
  try it out and give us feedback!

In v1.8.0, kubeadm introduced the `kubeadm alpha phase` command with the
aim of making kubeadm more modular. This modularity enables you to invoke

atomic sub-steps of the bootstrap process; you can let kubeadm do some parts and fill in yourself where you need customizations.

`kubeadm alpha phase` is consistent with kubeadm init workflow, and behind the scene both use the same code.

kubeadm alpha phase preflight

You can execute preflight checks both for the master node, like in `kubeadm init`, or for the worker node like in `kubeadm join`.

- master
- node

Run master pre-flight checks

Synopsis

Run master pre-flight checks, functionally equivalent to what implemented by kubeadm init.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase preflight master [flags]
```

Examples

```
  # Run master pre-flight checks.
  kubeadm alpha phase preflight master
```

Options

-h, --help

help for master

Options inherited from parent commands

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilege-dUser,Swap'. Value 'all' ignores errors from all checks.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Run node pre-flight checks

Synopsis

Run node pre-flight checks, functionally equivalent to what implemented by kubeadm join.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase preflight node [flags]
```

Examples

```
  # Run node pre-flight checks.
  kubeadm alpha phase preflight node
```

Options

-h, --help

help for node

Options inherited from parent commands

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

--ignore-preflight-errors stringSlice

A list of checks whose errors will be shown as warnings. Example: 'IsPrivilege-dUser,Swap'. Value 'all' ignores errors from all checks.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase certs

You can create all required certificates with the `all` subcommand or selectively create certificates.

- all
- ca
- apiserver
- apiserver-kubelet-client
- sa
- front-proxy-ca
- front-proxy-client

Generates all PKI assets necessary to establish the control plane

Synopsis

Generates a self-signed CA to provision identities for each component in the cluster (including nodes) and client certificates to be used by various components.

If a given certificate and private key pair both exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs all [flags]
```

Examples

```
# Creates all PKI assets necessary to establish the control plane,
# functionally equivalent to what generated by kubeadm init.
kubeadm alpha phase certs all

# Creates all PKI assets using options read from a configuration file.
kubeadm alpha phase certs all --config masterconfiguration.yaml
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on, to use for the API server serving cert

--apiserver-cert-extra-sans stringSlice

Optional extra altnames to use for the API server serving cert. Can be both IP addresses and DNS names

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for all

--service-cidr string   Default: "10.96.0.0/12"

Alternative range of IP address for service VIPs, from which derives the internal API server VIP that will be added to the API Server serving cert

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services, to use for the API server serving cert

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the self-signed kubernetes CA to provision identities for other kuberenets components

Synopsis

Generates the self-signed kubernetes CA to provision identities for other kuberenets components, and saves them into ca.cert and ca.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs ca [flags]
```


Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for ca

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the certificate for serving the kubernetes API

Synopsis

Generates the certificate for serving the kubernetes API, and saves them into apiserver.cert and apiserver.key files.

Default SANs are kubernetes, kubernetes.default, kubernetes.default.svc, kubernetes.default.svc.cluster.local, 10.96.0.1, 127.0.0.1

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs apiserver [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on, to use for the API server serving cert

--apiserver-cert-extra-sans stringSlice

Optional extra altnames to use for the API server serving cert. Can be both IP addresses and DNS names

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver

--service-cidr string   Default: "10.96.0.0/12"

Alternative range of IP address for service VIPs, from which derives the internal API server VIP that will be added to the API Server serving cert

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services, to use for the API server serving cert

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the Client certificate for the API server to connect to kubelet

Synopsis

Generates the Client certificate for the API server to connect to kubelet, and saves them into apiserver-kubelet-client.cert and apiserver-kubelet-client.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs apiserver-kubelet-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver-kubelet-client

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a private key for signing service account tokens along with its public key

Synopsis

Generates the private key for signing service account tokens along with its public key, and saves them into sa.key and sa.pub files. If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs sa [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for sa

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the self-signed CA to provision identities for front proxy

Synopsis

Generates the self-signed CA to provision identities for front proxy, and saves them into front-proxy-ca.cert and front-proxy-ca.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs front-proxy-ca [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for front-proxy-ca

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client for the front proxy

Synopsis

Generates the client for the front proxy, and saves them into front-proxy-client.cert and front-proxy-client.key files.

If both files already exist, kubeadm skips the generation step and existing files will be used.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase certs front-proxy-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

1157

-h, --help

help for front-proxy-client

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase certs renew

You can renew all Kubernetes certificates using the `all` subcommand or renew them selectively.

- all
- apiserver-etcd-client
- apiserver-kubelet-client
- apiserver
- etcd-healthcheck-client
- etcd-peer
- etcd-server
- front-proxy-client

renew all available certificates

Synopsis

Renews all known certificates necessary to run the control plan. Renewals are run unconditionally, regardless of expiration date. Renewals can also be run individually for more control.

```
kubeadm alpha phase certs renew all [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for all

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client apiserver uses to access etcd

Synopsis

Renews the client apiserver uses to access etcd, and saves them into apiserver-etcd-client.cert and apiserver-etcd-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew apiserver-etcd-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver-etcd-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the Client certificate for the API server to connect to kubelet

Synopsis

Renews the Client certificate for the API server to connect to kubelet, and saves them into apiserver-kubelet-client.cert and apiserver-kubelet-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew apiserver-kubelet-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver-kubelet-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the certificate for serving the kubernetes API

1160

Synopsis

Renews the certificate for serving the kubernetes API, and saves them into apiserver.cert and apiserver.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew apiserver [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for apiserver

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client certificate for liveness probes to healtcheck etcd

Synopsis

Renews the client certificate for liveness probes to healtcheck etcd, and saves them into etcd/healthcheck-client.cert and etcd/healthcheck-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew etcd-healthcheck-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for etcd-healthcheck-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the credentials for etcd nodes to communicate with each other

Synopsis

Renews the credentials for etcd nodes to communicate with each other, and saves them into etcd/peer.cert and etcd/peer.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew etcd-peer [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for etcd-peer

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the certificate for serving etcd

Synopsis

Renews the certificate for serving etcd, and saves them into etcd/server.cert and etcd/server.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew etcd-server [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for etcd-server

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the client for the front proxy

Synopsis

Renews the client for the front proxy, and saves them into front-proxy-client.cert and front-proxy-client.key files.

Extra attributes such as SANs will be based on the existing certificates, there is no need to resupply them.

```
kubeadm alpha phase certs renew front-proxy-client [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where to save the certificates

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for front-proxy-client

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--use-api

Use the Kubernetes certificate API to renew certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase kubeconfig

You can create all required kubeconfig files with the `all` subcommand, or selectively create the files. Additionally, the `user` subcommand supports the creation of kubeconfig files for additional users.

- all
- admin
- kubelet
- controller-manager
- scheduler
- user

Generates all kubeconfig files necessary to establish the control plane and the admin kubeconfig file

Synopsis

Generates all kubeconfig files necessary to establish the control plane and the admin kubeconfig file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig all [flags]
```

Examples

```
  # Generates all kubeconfig files, functionally equivalent to what generated
  # by kubeadm init.
  kubeadm alpha phase kubeconfig all

  # Generates all kubeconfig files using options read from a configuration file.
  kubeadm alpha phase kubeconfig all --config masterconfiguration.yaml
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for all

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

--node-name string

The node name that should be used for the kubelet client certificate

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the admin to use and for kubeadm itself

Synopsis

Generates the kubeconfig file for the admin and for kubeadm itself, and saves it to admin.conf file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig admin [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for admin

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the kubelet to use. Please note that this should be used *only* for bootstrapping purposes

Synopsis

Generates the kubeconfig file for the kubelet to use and saves it to /etc/kubernetes/kubelet.conf file.

Please note that this should only be used for bootstrapping purposes. After your control plane is up, you should request all kubelet credentials from the CSR API.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig kubelet [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for kubelet

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

--node-name string

The node name that should be used for the kubelet client certificate

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the controller manager to use

Synopsis

Generates the kubeconfig file for the controller manager to use and saves it to /etc/kubernetes/controller-manager.conf file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig controller-manager [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for controller-manager

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates a kubeconfig file for the scheduler to use

Synopsis

Generates the kubeconfig file for the scheduler to use and saves it to /etc/kubernetes/scheduler.conf file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig scheduler [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for scheduler

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Outputs a kubeconfig file for an additional user

Synopsis

Outputs a kubeconfig file for an additional user.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubeconfig user [flags]
```

Examples

```
  # Outputs a kubeconfig file for an additional user named foo
  kubeadm alpha phase kubeconfig user --client-name=foo
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--client-name string

The name of user. It will be used as the CN if client certificates are created

-h, --help

help for user

--kubeconfig-dir string   Default: "/etc/kubernetes"

The path where to save the kubeconfig file

--org stringSlice

The orgnizations of the client certificate. It will be used as the O if client certificates are created

--token string

The token that should be used as the authentication mechanism for this kube-config, instead of client certificates

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase kubelet

Use the following commands to manage the kubelet phase.

- config annotate-cri
- config download
- config enable-dynamic
- config upload
- config write-to-disk
- write-env-file

annotates the node with the given crisocket

Synopsis

Adds an annotation to the current node with the CRI socket specified in the kubeadm InitConfiguration object.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config annotate-cri [flags]
```

Examples

```
  kubeadm alpha phase kubelet config annotate-cri --config kubeadm.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

1171

help for annotate-cri

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a
set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Downloads the kubelet configuration from the cluster ConfigMap kubelet-config-
1.X, where X is the minor version of the kubelet.

Synopsis

Downloads the kubelet configuration from a ConfigMap of the form "kubelet-
config-1.X" in the cluster, where X is the minor version of the kubelet. Either
kubeadm autodetects the kubelet version by exec-ing "kubelet –version" or re-
spects the –kubelet-version parameter.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config download [flags]
```

Examples

```
  # Downloads the kubelet configuration from the ConfigMap in the cluster. Autodetects the k
  kubeadm alpha phase kubelet config download

  # Downloads the kubelet configuration from the ConfigMap in the cluster. Uses a specific c
  kubeadm alpha phase kubelet config download --kubelet-version v1.12.0
```

Options

-h, --help

help for download

--kubeconfig string   Default: "/etc/kubernetes/kubelet.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a
set of standard locations are searched for an existing KubeConfig file.

--kubelet-version string

The desired version for the kubelet. Defaults to being autodetected from 'kubelet --version'.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

EXPERIMENTAL: Enables or updates dynamic kubelet configuration for a Node

Synopsis

Enables or updates dynamic kubelet configuration for a Node, against the kubelet-config-1.X ConfigMap in the cluster, where X is the minor version of the desired kubelet version.

WARNING: This feature is still experimental, and disabled by default. Enable only if you know what you are doing, as it may have surprising side-effects at this stage.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config enable-dynamic [flags]
```

Examples

```
  # Enables dynamic kubelet configuration for a Node.
  kubeadm alpha phase kubelet enable-dynamic-config --node-name node-1 --kubelet-version v1.

  WARNING: This feature is still experimental, and disabled by default. Enable only if you k
  may have surprising side-effects at this stage.
```

Options

-h, --help

help for enable-dynamic

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubelet-version string

The desired version for the kubelet

1173

--node-name string

Name of the node that should enable the dynamic kubelet configuration

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Uploads kubelet configuration to a ConfigMap based on a kubeadm InitConfiguration file.

Synopsis

Uploads kubelet configuration extracted from the kubeadm InitConfiguration object to a ConfigMap of the form kubelet-config-1.X in the cluster, where X is the minor version of the current (API Server) Kubernetes version.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config upload [flags]
```

Examples

```
  # Uploads the kubelet configuration from the kubeadm Config file to a ConfigMap in the clu
  kubeadm alpha phase kubelet config upload --config kubeadm.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for upload

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Writes kubelet configuration to disk, either based on the –config argument.

Synopsis

Writes kubelet configuration to disk, based on the kubeadm configuration passed via "–config".

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet config write-to-disk [flags]
```

Examples

```
  # Extracts the kubelet configuration from a kubeadm configuration file
  kubeadm alpha phase kubelet config write-to-disk --config kubeadm.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for write-to-disk

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Writes an environment file with runtime flags for the kubelet.

Synopsis

Writes an environment file with flags that should be passed to the kubelet executing on the master or node. This –config flag can either consume a InitConfiguration object or a JoinConfiguration one, as this function is used for both "kubeadm init" and "kubeadm join".

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase kubelet write-env-file [flags]
```

Examples

```
  # Writes a dynamic environment file with kubelet flags from a InitConfiguration file.
  kubeadm alpha phase kubelet write-env-file --config masterconfig.yaml

  # Writes a dynamic environment file with kubelet flags from a JoinConfiguration file.
  kubeadm alpha phase kubelet write-env-file --config nodeconfig.yaml
```

Options

--config string

Path to kubeadm config file (WARNING: Usage of a configuration file is experimental)

-h, --help

help for write-env-file

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase controlplane

You can create all required static Pod files for the control plane components with the `all` subcommand, or selectively create the files.

- all
- apiserver
- controller-manager
- scheduler

Generates all static Pod manifest files necessary to establish the control plane

Synopsis

Generates all static Pod manifest files necessary to establish the control plane.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane all [flags]
```

Examples

```
# Generates all static Pod manifest files for control plane components,
# functionally equivalent to what generated by kubeadm init.
kubeadm alpha phase controlplane all

# Generates all static Pod manifest files using options read from a configuration file.
kubeadm alpha phase controlplane --config masterconfiguration.yaml
```

Options

--apiserver-advertise-address string

The IP address of the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--apiserver-extra-args mapStringString

A set of extra flags to pass to the API Server or override default ones in form of <flagname>=<value>

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--controller-manager-extra-args mapStringString

A set of extra flags to pass to the Controller Manager or override default ones in form of <flagname>=<value>

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for all

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

--scheduler-extra-args mapStringString

A set of extra flags to pass to the Scheduler or override default ones in form of <flagname>=<value>

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the API server static Pod manifest

Synopsis

Generates the static Pod manifest file for the API server and saves it into /etc/kubernetes/manifests/kube-apiserver.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane apiserver [flags]
```

Options

--apiserver-advertise-address string

The IP address of the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--apiserver-extra-args mapStringString

A set of extra flags to pass to the API Server or override default ones in form of <flagname>=<value>

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for apiserver

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the controller-manager static Pod manifest

Synopsis

Generates the static Pod manifest file for the controller-manager and saves it into /etc/kubernetes/manifests/kube-controller-manager.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane controller-manager [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--controller-manager-extra-args mapStringString

A set of extra flags to pass to the Controller Manager or override default ones in form of <flagname>=<value>

-h, --help

help for controller-manager

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Generates the scheduler static Pod manifest

Synopsis

Generates the static Pod manifest file for the scheduler and saves it into /etc/kubernetes/manifests/kube-scheduler.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase controlplane scheduler [flags]
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for scheduler

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--scheduler-extra-args mapStringString

A set of extra flags to pass to the Scheduler or override default ones in form of <flagname>=<value>

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase etcd

Use the following command to create a self-hosted, local etcd instance based on a static Pod file.

- etcd local

Generates the static Pod manifest file for a local, single-node etcd instance

Synopsis

Generates the static Pod manifest file for a local, single-node etcd instance and saves it to /etc/kubernetes/manifests/etcd.yaml file.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase etcd local [flags]
```

Examples

```
  # Generates the static Pod manifest file for etcd, functionally
  # equivalent to what generated by kubeadm init.
  kubeadm alpha phase etcd local

  #  Generates the static Pod manifest file for etcd.
  kubeadm alpha phase etcd local --config masterconfiguration.yaml
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for local

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase mark-master

Use the following command to label and taint the node with the `node-role.kubernetes.io/master=""` key-value pair.

- mark-master

Mark a node as master

Synopsis

Applies a label that specifies that a node is a master and a taint that forces workloads to be deployed accordingly.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase mark-master [flags]
```


Examples

```
  # Applies master label and taint to the current node, functionally equivalent to what exec
  kubeadm alpha phase mark-master

  # Applies master label and taint to a specific node
  kubeadm alpha phase mark-master --node-name myNode
```

1182

Options

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for mark-master

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--node-name string

The node name to which label and taints should apply

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase bootstrap-token

Use the following actions to fully configure bootstrap tokens. You can fully configure bootstrap tokens with the `all` subcommand, or selectively configure single elements.

- all
- create
- cluster-info
- node allow-auto-approve
- node allow-post-csrs

Makes all the bootstrap token configurations and creates an initial token

Synopsis

Bootstrap tokens are used for establishing bidirectional trust between a node joining the cluster and a the master node.

This command makes all the configurations required to make bootstrap tokens works and then creates an initial token.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token all [flags]
```

Examples

```
# Makes all the bootstrap token configurations and creates an initial token, functionally
# equivalent to what generated by kubeadm init.
kubeadm alpha phase bootstrap-token all
```

Options

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--description string

A human friendly description of how this token is used.

--groups stringSlice   Default: [system:bootstrappers:kubeadm:default-node-token]

Extra groups that this token will authenticate as when used for authentication. Must match "\\Asystem:bootstrappers:[a-z0-9:-]{0,255}[a-z0-9]\\z"

-h, --help

help for all

--skip-token-print

Skip printing of the bootstrap token

--token string

The token to use for establishing bidirectional trust between nodes and masters. The format is [a-z0-9]{6}\.[a-z0-9]{16} - e.g. abcdef.0123456789abcdef

--token-ttl duration   Default: 24h0m0s

The duration before the token is automatically deleted (e.g. 1s, 2m, 3h). If set to '0', the token will never expire

--usages stringSlice   Default: [signing,authentication]

Describes the ways in which this token can be used. You can pass --usages multiple times or provide a comma separated list of options. Valid options: [signing,authentication]

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Creates a bootstrap token to be used for node joining

Synopsis

Creates a bootstrap token. If no token value is given, kubeadm will generate a random token instead.

Alternatively, you can use kubeadm token.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token create [flags]
```

Options

--config string

Path to kubeadm config file. WARNING: Usage of a configuration file is experimental

--description string

A human friendly description of how this token is used.

--groups stringSlice   Default: [system:bootstrappers:kubeadm:default-node-token]

Extra groups that this token will authenticate as when used for authentication. Must match "\\Asystem:bootstrappers:[a-z0-9:-]{0,255}[a-z0-9]\\z"

-h, --help

help for create

--skip-token-print

Skip printing of the bootstrap token

--token string

The token to use for establishing bidirectional trust between nodes and masters. The format is [a-z0-9]{6}\.[a-z0-9]{16} - e.g. abcdef.0123456789abcdef

1185

--token-ttl duration   Default: 24h0m0s

The duration before the token is automatically deleted (e.g. 1s, 2m, 3h). If set to '0', the token will never expire

--usages stringSlice   Default: [signing,authentication]

Describes the ways in which this token can be used. You can pass --usages multiple times or provide a comma separated list of options. Valid options: [signing,authentication]

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Uploads the cluster-info ConfigMap from the given kubeconfig file

Synopsis

Uploads the "cluster-info" ConfigMap in the "kube-public" namespace, populating it with cluster information extracted from the given kubeconfig file. The ConfigMap is used for the node bootstrap process in its initial phases, before the client trusts the API server.

See online documentation about Authenticating with Bootstrap Tokens for more details.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token cluster-info [flags]
```

Options

-h, --help

help for cluster-info

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Configures RBAC rules to allow the csrapprover controller automatically approve CSRs from a node bootstrap token

Synopsis

Configures RBAC rules to allow the csrapprover controller to automatically approve certificate signing requests generated by nodes joining the cluster. It configures also RBAC rules for certificates rotation (with auto approval of new certificates).

See online documentation about TLS bootstrapping for more details.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token node allow-auto-approve [flags]
```

Options

-h, --help

help for allow-auto-approve

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Configures RBAC to allow node bootstrap tokens to post CSRs in order for nodes to get long term certificate credentials

Synopsis

Configures RBAC rules to allow node bootstrap tokens to post a certificate signing request, thus enabling nodes joining the cluster to request long term certificate credentials.

See online documentation about TLS bootstrapping for more details.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase bootstrap-token node allow-post-csrs [flags]
```

Options

-h, --help

help for allow-post-csrs

Options inherited from parent commands

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase upload-config

You can use this command to upload the kubeadm configuration to your cluster. Alternatively, you can use kubeadm config.

- mark-master

Uploads the currently used configuration for kubeadm to a ConfigMap

Synopsis

Uploads the kubeadm init configuration of your cluster to a ConfigMap called kubeadm-config in the kube-system namespace. This enables correct configuration of system components and a seamless user experience when upgrading.

Alternatively, you can use kubeadm config.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase upload-config [flags]
```

Examples

```
# uploads the configuration of your cluster
kubeadm alpha phase upload-config --config=myConfig.yaml
```

Options

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

-h, --help

help for upload-config

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase addon

You can install all the available addons with the `all` subcommand, or install them selectively.

> **Note:** If `kubeadm` is invoked with `--feature-gates=CoreDNS=false`, kube-dns is installed.

- all
- kube-proxy
- coredns

Installs all addons to a Kubernetes cluster

Synopsis

Installs the CoreDNS and the kube-proxy addons components via the API server. Please note that although the DNS server is deployed, it will not be scheduled until CNI is installed.

Alpha Disclaimer: this command is currently alpha.

1189

```
kubeadm alpha phase addon all [flags]
```

Examples

```
# Installs the CoreDNS and the kube-proxy addons components via the API server,
# functionally equivalent to what installed by kubeadm init.

kubeadm alpha phase selfhosting from-staticpods
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is
experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options
are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for all

--image-repository string   Default: "k8s.gcr.io"

Choose a container registry to pull control plane images from

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a
set of standard locations are searched for an existing KubeConfig file.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Installs the kube-proxy addon to a Kubernetes cluster

Synopsis

Installs the kube-proxy addon components via the API server.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase addon kube-proxy [flags]
```

Options

--apiserver-advertise-address string

The IP address the API server is accessible on

--apiserver-bind-port int32   Default: 6443

The port the API server is accessible on

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is
experimental

-h, --help

help for kube-proxy

--image-repository string   Default: "k8s.gcr.io"

Choose a container registry to pull control plane images from

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a
set of standard locations are searched for an existing KubeConfig file.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--pod-network-cidr string

The range of IP addresses used for the Pod network

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

Installs the CoreDNS addon to a Kubernetes cluster

Synopsis

Installs the CoreDNS addon components via the API server. Please note that although the DNS server is deployed, it will not be scheduled until CNI is installed.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase addon coredns [flags]
```

Options

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for coredns

--image-repository string   Default: "k8s.gcr.io"

Choose a container registry to pull control plane images from

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

--kubernetes-version string   Default: "stable-1"

Choose a specific Kubernetes version for the control plane

--service-cidr string   Default: "10.96.0.0/12"

The range of IP address used for service VIPs

--service-dns-domain string   Default: "cluster.local"

Alternative domain for services

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

kubeadm alpha phase self-hosting

> **Caution:** Self-hosting is an alpha feature. See kubeadm init documentation for self-hosting limitations.

- self-hosting

Converts a static Pod-hosted control plane into a self-hosted one

Synopsis

Converts static Pod files for control plane components into self-hosted Daemon-Sets configured via the Kubernetes API.

See the documentation for self-hosting limitations.

Alpha Disclaimer: this command is currently alpha.

```
kubeadm alpha phase selfhosting convert-from-staticpods [flags]
```

Examples

```
# Converts a static Pod-hosted control plane into a self-hosted one,
# functionally equivalent to what generated by kubeadm init executed
# with --feature-gates=SelfHosting=true.

kubeadm alpha phase selfhosting convert-from-staticpods
```

Options

--cert-dir string   Default: "/etc/kubernetes/pki"

The path where certificates are stored

--config string

Path to a kubeadm config file. WARNING: Usage of a configuration file is experimental

--feature-gates string

A set of key=value pairs that describe feature gates for various features. Options are:
Auditing=true|false (ALPHA - default=false)
CoreDNS=true|false (default=true)
DynamicKubeletConfig=true|false (BETA - default=false)

-h, --help

help for convert-from-staticpods

--kubeconfig string   Default: "/etc/kubernetes/admin.conf"

The KubeConfig file to use when talking to the cluster. If the flag is not set, a set of standard locations are searched for an existing KubeConfig file.

Options inherited from parent commands

--rootfs string

[EXPERIMENTAL] The path to the 'real' host root filesystem.

What's next

- kubeadm init to bootstrap a Kubernetes master node
- kubeadm join to connect a node to the cluster
- kubeadm reset to revert any changes made to this host by `kubeadm init` or `kubeadm join`

Edit This Page

Implementation details

FEATURE STATE: `Kubernetes v1.10` stable

This feature is *stable*, meaning:

- The version name is vX where X is an integer.
- Stable versions of features will appear in released software for many subsequent versions.

`kubeadm init` and `kubeadm join` together provides a nice user experience for creating a best-practice but bare Kubernetes cluster from scratch. However, it might not be obvious *how* kubeadm does that.

This document provide additional details on what happen under the hood, with the aim of sharing knowledge on Kubernetes cluster best practices.

- Core design principles
- Constants and well-known values and paths
- kubeadm init workflow internal design
- kubeadm join phases internal design
- TLS Bootstrap

Core design principles

The cluster that `kubeadm init` and `kubeadm join` set up should be:

- **Secure**: It should adopt latest best-practices like:
    - enforcing RBAC
    - using the Node Authorizer
    - using secure communication between the control plane components
    - using secure communication between the API server and the kubelets
    - lock-down the kubelet API
    - locking down access to the API for system components like the kube-proxy and CoreDNS
    - locking down what a Bootstrap Token can access
    - etc.
- **Easy to use**: The user should not have to run anything more than a couple of commands:
    - `kubeadm init`
    - `export KUBECONFIG=/etc/kubernetes/admin.conf`
    - `kubectl apply -f <network-of-choice.yaml>`
    - `kubeadm join --token <token> <master-ip>:<master-port>`
- **Extendable**:
    - It should for example *not* favor any network provider, instead configuring a network is out-of-scope
    - Should provide the possibility to use a config file for customizing various parameters

1195

Constants and well-known values and paths

In order to reduce complexity and to simplify development of an on-top-of-kubeadm-implemented deployment solution, kubeadm uses a limited set of constants values for well know-known paths and file names.

The Kubernetes directory `/etc/kubernetes` is a constant in the application, since it is clearly the given path in a majority of cases, and the most intuitive location; other constants paths and file names are:

- `/etc/kubernetes/manifests` as the path where kubelet should look for static Pod manifests. Names of static Pod manifests are:
  - `etcd.yaml`
  - `kube-apiserver.yaml`
  - `kube-controller-manager.yaml`
  - `kube-scheduler.yaml`
- `/etc/kubernetes/` as the path where kubeconfig files with identities for control plane components are stored. Names of kubeconfig files are:
  - `kubelet.conf` (`bootstrap-kubelet.conf` during TLS bootstrap)
  - `controller-manager.conf`
  - `scheduler.conf`
  - `admin.conf` for the cluster admin and kubeadm itself
- Names of certificates and key files :
  - `ca.crt`, `ca.key` for the Kubernetes certificate authority
  - `apiserver.crt`, `apiserver.key` for the API server certificate
  - `apiserver-kubelet-client.crt`, `apiserver-kubelet-client.key` for the client certificate used by the API server to connect to the kubelets securely
  - `sa.pub`, `sa.key` for the key used by the controller manager when signing ServiceAccount
  - `front-proxy-ca.crt`, `front-proxy-ca.key` for the front proxy certificate authority
  - `front-proxy-client.crt`, `front-proxy-client.key` for the front proxy client

kubeadm init workflow internal design

The `kubeadm init` internal workflow consists of a sequence of atomic work tasks to perform, as described in `kubeadm init`.

The `kubeadm alpha phase` command allows users to invoke individually each task, and ultimately offers a reusable and composable API/toolbox that can be used by other Kubernetes bootstrap tools, by any IT automation tool or by advanced user for creating custom clusters.

Preflight checks

Kubeadm executes a set of preflight checks before starting the init, with the aim to verify preconditions and avoid common cluster startup problems. In any case the user can skip specific preflight checks (or eventually all preflight checks) with the `--ignore-preflight-errors` option.

- [warning] If the Kubernetes version to use (specified with the `--kubernetes-version` flag) is at least one minor version higher than the kubeadm CLI version.
- Kubernetes system requirements:
  - if running on linux:
  - [error] if not Kernel 3.10+ or 4+ with specific KernelSpec
  - [error] if required cgroups subsystem aren't in set up
  - if using docker:
  - [warning/error] if Docker service does not exist, if it is disabled, if it is not active.
  - [error] if Docker endpoint does not exist or does not work
  - [warning] if docker version >17.03
  - If using other cri engine:
  - [error] if crictl socket does not answer
- [error] if user is not root
- [error] if the machine hostname is not a valid DNS subdomain
- [warning] if the host name cannot be reached via network lookup
- [error] if kubelet version is lower that the minimum kubelet version supported by kubeadm (current minor -1)
- [error] if kubelet version is at least one minor higher than the required controlplane version (unsupported version skew)
- [warning] if kubelet service does not exist or if it is disabled
- [warning] if firewalld is active
- [error] if API server bindPort or ports 10250/10251/10252 are used
- [Error] if `/etc/kubernetes/manifest` folder already exists and it is not empty
- [Error] if `/proc/sys/net/bridge/bridge-nf-call-iptables` file does not exist/does not contain 1
- [Error] if advertise address is ipv6 and `/proc/sys/net/bridge/bridge-nf-call-ip6tables` does not exist/does not contain 1.
- [Error] if swap is on
- [Error] if `ip`, `iptables`, `mount`, `nsenter` commands are not present in the command path
- [warning] if `ebtables`, `ethtool`, `socat`, `tc`, `touch`, `crictl` commands are not present in the command path
- [warning] if extra arg flags for API server, controller manager, scheduler contains some invalid options
- [warning] if connection to https://API.AdvertiseAddress:API.BindPort goes through proxy

- [warning] if connection to services subnet goes through proxy (only first address checked)
- [warning] if connection to Pods subnet goes through proxy (only first address checked)

- If external etcd is provided:
    - [Error] if etcd version less than 3.0.14
    - [Error] if etcd certificates or keys are specified, but not provided
- If external etcd is NOT provided (and thus local etcd will be installed):
    - [Error] if ports 2379 is used
    - [Error] if Etcd.DataDir folder already exists and it is not empty
- If authorization mode is ABAC:
    - [Error] if abac_policy.json does not exist
- If authorization mode is WebHook
    - [Error] if webhook_authz.conf does not exist

Please note that:

1. Preflight checks can be invoked individually with the `kubeadm alpha phase preflight` command

Generate the necessary certificates

Kubeadm generates certificate and private key pairs for different purposes:

- A self signed certificate authority for the Kubernetes cluster saved into `ca.crt` file and `ca.key` private key file
- A serving certificate for the API server, generated using `ca.crt` as the CA, and saved into `apiserver.crt` file with its private key `apiserver.key`. This certificate should contains following alternative names:
    - The Kubernetes service's internal clusterIP (the first address in the services CIDR, e.g. `10.96.0.1` if service subnet is `10.96.0.0/12`)
    - Kubernetes DNS names, e.g. `kubernetes.default.svc.cluster.local` if `--service-dns-domain` flag value is `cluster.local`, plus default DNS names `kubernetes.default.svc`, `kubernetes.default`, `kubernetes`
    - The node-name
    - The `--apiserver-advertise-address`
    - Additional alternative names specified by the user
- A client certificate for the API server to connect to the kubelets securely, generated using `ca.crt` as the CA and saved into `apiserver-kubelet-client.crt` file with its private key `apiserver-kubelet-client.key`. This certificate should be in the `system:masters` organization
- A private key for signing ServiceAccount Tokens saved into `sa.key` file along with its public key `sa.pub`

- A certificate authority for the front proxy saved into `front-proxy-ca.crt` file with its key `front-proxy-ca.key`
- A client cert for the front proxy client, generate using `front-proxy-ca.crt` as the CA and saved into `front-proxy-client.crt` file with its private key`front-proxy-client.key`

Certificates are stored by default in `/etc/kubernetes/pki`, but this directory is configurable using the `--cert-dir` flag.

Please note that:

1. If a given certificate and private key pair both exist, and its content is evaluated compliant with the above specs, the existing files will be used and the generation phase for the given certificate skipped. This means the user can, for example, copy an existing CA to `/etc/kubernetes/pki/ca.{crt,key}`, and then kubeadm will use those files for signing the rest of the certs. See also using custom certificates
2. Only for the CA, it is possible to provide the `ca.crt` file but not the `ca.key` file, if all other certificates and kubeconfig files already are in place kubeadm recognize this condition and activates the ExternalCA , which also implies the `csrsigner`controller in controller-manager won't be started
3. If kubeadm is running in ExternalCA mode; all the certificates must be provided by the user, because kubeadm cannot generate them by itself
4. In case of kubeadm is executed in the `--dry-run` mode, certificates files are written in a temporary folder
5. Certificate generation can be invoked individually with the `kubeadm alpha phase certs all` command

Generate kubeconfig files for control plane components

Kubeadm kubeconfig files with identities for control plane components:

- A kubeconfig file for kubelet to use, `/etc/kubernetes/kubelet.conf`; inside this file is embedded a client certificate with kubelet identity. This client cert should:
  - Be in the `system:nodes` organization, as required by the Node Authorization module
  - Have the CN `system:node:<hostname-lowercased>`
- A kubeconfig file for controller-manager, `/etc/kubernetes/controller-manager.conf`; inside this file is embedded a client certificate with controller-manager identity. This client cert should have the CN `system:kube-controller-manager`, as defined by default RBAC core components roles
- A kubeconfig file for scheduler, `/etc/kubernetes/scheduler.conf`; inside this file is embedded a client certificate with scheduler identity. This client cert should have the CN `system:kube-scheduler`, as defined by default RBAC core components roles

1199

Additionally, a kubeconfig file for kubeadm to use itself and the admin is generated and save into the `/etc/kubernetes/admin.conf` file. The "admin" here is defined the actual person(s) that is administering the cluster and want to have full control (**root**) over the cluster. The embedded client certificate for admin should: - Be in the `system:masters` organization, as defined by default RBAC user facing role bindings - Include a CN, but that can be anything. Kubeadm uses the `kubernetes-admin` CN

Please note that:

1. `ca.crt` certificate is embedded in all the kubeconfig files.
2. If a given kubeconfig file exists, and its content is evaluated compliant with the above specs, the existing file will be used and the generation phase for the given kubeconfig skipped
3. If kubeadm is running in ExternalCA mode, all the required kubeconfig must be provided by the user as well, because kubeadm cannot generate any of them by itself
4. In case of kubeadm is executed in the `--dry-run` mode, kubeconfig files are written in a temporary folder
5. Kubeconfig files generation can be invoked individually with the `kubeadm alpha phase kubeconfig all` command

Generate static Pod manifests for control plane components

Kubeadm writes static Pod manifest files for control plane components to `/etc/kubernetes/manifests`; the kubelet watches this directory for Pods to create on startup.

Static Pod manifest share a set of common properties:

- All static Pods are deployed on `kube-system` namespace
- All static Pods gets `tier:control-plane` and `component:{component-name}` labels
- All static Pods gets `scheduler.alpha.kubernetes.io/critical-pod` annotation (this will be moved over to the proper solution of using Pod Priority and Preemption when ready)
- `hostNetwork: true` is set on all static Pods to allow control plane startup before a network is configured; as a consequence:
  - The `address` that the controller-manager and the scheduler use to refer the API server is `127.0.0.1`
  - If using a local etcd server, `etcd-servers` address will be set to `127.0.0.1:2379`
- Leader election is enabled for both the controller-manager and the scheduler
- Controller-manager and the scheduler will reference kubeconfig files with their respective, unique identities

- All static Pods gets any extra flags specified by the user as described in passing custom arguments to control plane components
- All static Pods gets any extra Volumes specified by the user (Host path)

Please note that:

1. All the images, for the `--kubernetes-version`/current architecture, will be pulled from `k8s.gcr.io`; In case an alternative image repository or CI image repository is specified this one will be used; In case a specific container image should be used for all control plane components, this one will be used. see using custom images for more details
2. In case of kubeadm is executed in the `--dry-run` mode, static Pods files are written in a temporary folder
3. Static Pod manifest generation for master components can be invoked individually with the `kubeadm alpha phase controlplane all` command

API server

The static Pod manifest for the API server is affected by following parameters provided by the users:

- The `apiserver-advertise-address` and `apiserver-bind-port` to bind to; if not provided, those value defaults to the IP address of the default network interface on the machine and port 6443
- The `service-cluster-ip-range` to use for services
- If an external etcd server is specified, the `etcd-servers` address and related TLS settings (`etcd-cafile`, `etcd-certfile`, `etcd-keyfile`); if an external etcd server is not be provided, a local etcd will be used (via host network)
- If a cloud provider is specified, the corresponding `--cloud-provider` is configured, together with the `--cloud-config` path if such file exists (this is experimental, alpha and will be removed in a future version)
- If kubeadm is invoked with `--feature-gates=HighAvailability`, the flag `--endpoint-reconciler-type=lease` is set, thus enabling automatic reconciliation of endpoints for the internal API server VIP
- If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig`, the corresponding feature on API server is activated with the `--feature-gates=DynamicKubeletConfig=true` flag

Other API server flags that are set unconditionally are:

- `--insecure-port=0` to avoid insecure connections to the api server
- `--enable-bootstrap-token-auth=true` to enable the `BootstrapTokenAuthenticator` authentication module. See TLS Bootstrapping for more details
- `--allow-privileged` to `true` (required e.g. by kube proxy)
- `--requestheader-client-ca-file` to `front-proxy-ca.crt`
- `--enable-admission-plugins` to:
    - `Initializers` to enable Dynamic Admission Control.

1201

- – `NamespaceLifecycle` e.g. to avoid deletion of system reserved namespaces
- – `LimitRanger` and `ResourceQuota` to enforce limits on namespaces
- – `ServiceAccount` to enforce service account automation
- – `PersistentVolumeLabel` attaches region or zone labels to PersistentVolumes as defined by the cloud provider (This admission controller is deprecated and will be removed in a future version. It is not deployed by kubeadm by default with v1.9 onwards when not explicitly opting into using `gce` or `aws` as cloud providers)
- – `DefaultStorageClass` to enforce default storage class on `PersistentVolumeClaim` objects
- – `DefaultTolerationSeconds`
- – `NodeRestriction` to limit what a kubelet can modify (e.g. only pods on this node)
- `--kubelet-preferred-address-types` to `InternalIP,ExternalIP,Hostname`; this makes `kubectl logs` and other API server-kubelet communication work in environments where the hostnames of the nodes aren't resolvable
- Flags for using certificates generated in previous steps:
  - – `--client-ca-file` to `ca.crt`
  - – `--tls-cert-file` to `apiserver.crt`
  - – `--tls-private-key-file` to `apiserver.key`
  - – `--kubelet-client-certificate` to `apiserver-kubelet-client.crt`
  - – `--kubelet-client-key` to `apiserver-kubelet-client.key`
  - – `--service-account-key-file` to `sa.pub`
  - – `--requestheader-client-ca-file` to `front-proxy-ca.crt`
  - – `--proxy-client-cert-file` to `front-proxy-client.crt`
  - – `--proxy-client-key-file` to `front-proxy-client.key`
- Other flags for securing the front proxy (API Aggregation) communications:
  - – `--requestheader-username-headers=X-Remote-User`
  - – `--requestheader-group-headers=X-Remote-Group`
  - – `--requestheader-extra-headers-prefix=X-Remote-Extra-`
  - – `--requestheader-allowed-names=front-proxy-client`

Controller manager

The static Pod manifest for the API server is affected by following parameters provided by the users:

- If kubeadm is invoked specifying a `--pod-network-cidr`, the subnet manager feature required for some CNI network plugins is enabled by setting:
  - – `--allocate-node-cidrs=true`
  - – `--cluster-cidr` and `--node-cidr-mask-size` flags according to the given CIDR
  - – If a cloud provider is specified, the corresponding `--cloud-provider` is specified, together with the `--cloud-config` path if such configu-

1202

ration file exists (this is experimental, alpha and will be removed in a future version)

Other flags that are set unconditionally are:

- `--controllers` enabling all the default controllers plus `BootstrapSigner` and `TokenCleaner` controllers for TLS bootstrap. See TLS Bootstrapping for more details
- `--use-service-account-credentials` to `true`
- Flags for using certificates generated in previous steps:
    - `--root-ca-file` to `ca.crt`
    - `--cluster-signing-cert-file` to `ca.crt`, if External CA mode is disabled, otherwise to `""`
    - `--cluster-signing-key-file` to `ca.key`, if External CA mode is disabled, otherwise to `""`
    - `--service-account-private-key-file` to `sa.key`

Scheduler

The static Pod manifest for the scheduler is not affected by parameters provided by the users.

Generate static Pod manifest for local etcd

If the user specified an external etcd this step will be skipped, otherwise kubeadm generates a static Pod manifest file for creating a local etcd instance running in a Pod with following attributes:

- listen on `localhost:2379` and use `HostNetwork=true`
- make a `hostPath` mount out from the `dataDir` to the host's filesystem
- Any extra flags specified by the user

Please note that:

1. The etcd image will be pulled from `k8s.gcr.io`. In case an alternative image repository is specified this one will be used; In case an alternative image name is specified, this one will be used. see using custom images for more details
2. in case of kubeadm is executed in the `--dry-run` mode, the etcd static Pod manifest is written in a temporary folder
3. Static Pod manifest generation for local etcd can be invoked individually with the `kubeadm alpha phase etcd local` command

(optional and alpha in v1.9) Write init kubelet configuration

If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig`, it writes the kubelet init configuration into **/var/lib/kubelet/config/init/kubelet**

file.

The init configuration is used for starting the kubelet on this specific node, providing an alternative for the kubelet drop-in file; such configuration will be replaced by the kubelet base configuration as described in following steps. See set Kubelet parameters via a config file for additional info.

Please note that:

1. To make dynamic kubelet configuration work, flag `--dynamic-config-dir=/var/lib/kubelet/config/` should be specified in `/etc/systemd/system/kubelet.service.d/10-kubeadm.conf`
2. The kubelet configuration can be changed by passing a `KubeletConfiguration` object to `kubeadm init` or `kubeadm join` by using a configuration file `--config some-file.yaml`. The `KubeletConfiguration` object can be separated from other objects such as `InitConfiguration` using the `---` separator. For more details have a look at the `kubeadm config print-default` command.

Wait for the control plane to come up

This is a critical moment in time for kubeadm clusters. kubeadm waits until `localhost:6443/healthz` returns `ok`, however in order to detect deadlock conditions, kubeadm fails fast if `localhost:10255/healthz` (kubelet liveness) or `localhost:10255/healthz/syncloop` (kubelet readiness) don't return `ok`, respectively after 40 and 60 second.

kubeadm relies on the kubelet to pull the control plane images and run them properly as static Pods. After the control plane is up, kubeadm completes a the tasks described in following paragraphs.

(optional and alpha in v1.9) Write base kubelet configuration

If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig`:

1. Write the kubelet base configuration into the `kubelet-base-config-v1.9` ConfigMap in the `kube-system` namespace
2. Creates RBAC rules for granting read access to that ConfigMap to all boot-strap tokens and all kubelet instances (that is `system:bootstrappers:kubeadm:default-node-token` and `system:nodes` groups)
3. Enable the dynamic kubelet configuration feature for the initial master node by pointing `Node.spec.configSource` to the newly-created ConfigMap

Save the kubeadm ClusterConfiguration in a ConfigMap for later reference

kubeadm saves the configuration passed to `kubeadm init`, either via flags or the config file, in a ConfigMap named `kubeadm-config` under `kube-system` namespace.

This will ensure that kubeadm actions executed in future (e.g `kubeadm upgrade`) will be able to determine the actual/current cluster state and make new decisions based on that data.

Please note that:

1. Before uploading, sensitive information like e.g. the token are stripped from the configuration
2. Upload of master configuration can be invoked individually with the `kubeadm alpha phase upload-config` command
3. If you initialized your cluster using kubeadm v1.7.x or lower, you must create manually the master configuration ConfigMap before `kubeadm upgrade` to v1.8 . In order to facilitate this task, the `kubeadm config upload (from-flags|from-file)` was implemented

Mark master

As soon as the control plane is available, kubeadm executes following actions:

- Label the master with `node-role.kubernetes.io/master=""`
- Taints the master with `node-role.kubernetes.io/master:NoSchedule`

Please note that:

1. Mark master phase can be invoked individually with the `kubeadm alpha phase mark-master` command

Configure TLS-Bootstrapping for node joining

Kubeadm uses Authenticating with Bootstrap Tokens for joining new nodes to an existing cluster; for more details see also design proposal.

`kubeadm init` ensures that everything is properly configured for this process, and this includes following steps as well as setting API server and controller flags as already described in previous paragraphs. Please note that:

1. TLS bootstrapping for nodes can be configured with the `kubeadm alpha phase bootstrap-token all`
   command, executing all the configuration steps described in following paragraphs; alternatively, each step can be invoked individually

Create a bootstrap token

`kubeadm init` create a first bootstrap token, either generated automatically or provided by the user with the `--token` flag; as documented in bootstrap token specification, token should be saved as secrets with name `bootstrap-token-<token-id>` under `kube-system` namespace. Please note that:

1. The default token created by `kubeadm init` will be used to validate temporary user during TLS bootstrap process; those users will be member of `system:bootstrappers:kubeadm:default-node-token` group
2. The token has a limited validity, default 24 hours (the interval may be changed with the `-token-ttl` flag)
3. Additional tokens can be created with the `kubeadm token` command, that provide as well other useful functions for token management

Allow joining nodes to call CSR API

Kubeadm ensure that users in `system:bootstrappers:kubeadm:default-node-token` group are able to access the certificate signing API.

This is implemented by creating a ClusterRoleBinding named `kubeadm:kubelet-bootstrap` between the group above and the default RBAC role `system:node-bootstrapper`.

Setup auto approval for new bootstrap tokens

Kubeadm ensures that the Bootstrap Token will get its CSR request automatically approved by the csrapprover controller.

This is implemented by creating ClusterRoleBinding named `kubeadm:node-autoapprove-bootstrap` between the `system:bootstrappers:kubeadm:default-node-token` group and the default role `system:certificates.k8s.io:certificatesigningrequests:nodeclient`.

The role `system:certificates.k8s.io:certificatesigningrequests:nodeclient` should be created as well, granting POST permission to `/apis/certificates.k8s.io/certificatesigningre`

Setup nodes certificate rotation with auto approval

Kubeadm ensures that certificate rotation is enabled for nodes, and that new certificate request for nodes will get its CSR request automatically approved by the csrapprover controller.

This is implemented by creating ClusterRoleBinding named `kubeadm:node-autoapprove-certificate-rotati` between the `system:nodes` group and the default role `system:certificates.k8s.io:certificatesigningre`

Create the public cluster-info ConfigMap

This phase creates the `cluster-info` ConfigMap in the `kube-public` namespace.

Additionally it is created a role and a RoleBinding granting access to the ConfigMap for unauthenticated users (i.e. users in RBAC group `system:unauthenticated`)

Please note that:

1. The access to the `cluster-info` ConfigMap *is not* rate-limited. This may or may not be a problem if you expose your master to the internet; worst-case scenario here is a DoS attack where an attacker uses all the in-flight requests the kube-apiserver can handle to serving the `cluster-info` ConfigMap.

Install addons

Kubeadm installs the internal DNS server and the kube-proxy addon components via the API server. Please note that:

1. This phase can be invoked individually with the `kubeadm alpha phase addon all` command.

proxy

A ServiceAccount for `kube-proxy` is created in the `kube-system` namespace; then kube-proxy is deployed as a DaemonSet:

- The credentials (`ca.crt` and `token`) to the master come from the ServiceAccount
- The location of the master comes from a ConfigMap
- The `kube-proxy` ServiceAccount is bound to the privileges in the `system:node-proxier` ClusterRole

DNS

Note that:

- The CoreDNS service is named `kube-dns`. This is done to prevent any interruption in service when the user is switching the cluster DNS from kube-dns to CoreDNS or vice-versa
- In Kubernetes version 1.11 and later, CoreDNS is the default DNS server and you must invoke kubeadm with `--feature-gates=CoreDNS=false` to install kube-dns instead
- In Kubernetes version 1.10 and earlier, you must enable CoreDNS with `--feature-gates=CoreDNS=true`

1207

A ServiceAccount for CoreDNS/kube-dns is created in the `kube-system` namespace.

Deploy the `kube-dns` Deployment and Service:

- It's the upstream CoreDNS deployment relatively unmodified
- The `kube-dns` ServiceAccount is bound to the privileges in the `system:kube-dns` ClusterRole

(Optional and alpha in v1.9) self-hosting

This phase is performed only if `kubeadm init` is invoked with `–features-gates=selfHosting`

The self hosting phase basically replaces static Pods for control plane components with DaemonSets; this is achieved by executing following procedure for API server, scheduler and controller manager static Pods:

- Load the static Pod specification from disk
- Extract the PodSpec from static Pod manifest file
- Mutate the PodSpec to be compatible with self-hosting, and more in detail:
    - Add node selector attribute targeting nodes with `node-role.kubernetes.io/master=""` label,
    - Add a toleration for `node-role.kubernetes.io/master:NoSchedule` taint,
    - Set `spec.DNSPolicy` to `ClusterFirstWithHostNet`
- Build a new DaemonSet object for the self-hosted component in question. Use the above mentioned PodSpec
- Create the DaemonSet resource in `kube-system` namespace. Wait until the Pods are running.
- Remove the static Pod manifest file. The kubelet will stop the original static Pod-hosted component that was running

Please note that:

1. Self hosting is not yet resilient to node restarts; this can be fixed with external checkpointing or with kubelet checkpointing for the control plane Pods. See self-hosting for more details.

2. If invoked with `–features-gates=StoreCertsInSecrets` following additional steps will be executed

    - Creation of `ca`, `apiserver`, `apiserver-kubelet-client`, `sa`, `front-proxy-ca`, `front-proxy-client` TLS secrets in `kube-system` namespace with respective certificates and keys. Important! storing the CA key in a Secret might have security implications
    - Creation of `schedler.conf` and `controller-manager.conf` secrets in`kube-system` namespace with respective kubeconfig files
    - Mutation of all the Pod specs by replacing host path volumes with projected volumes from the secrets above

3. This phase can be invoked individually with the `kubeadm alpha phase selfhosting convert-from-staticpods` command.

kubeadm join phases internal design

Similarly to `kubeadm init`, also `kubeadm join` internal workflow consists of a sequence of atomic work tasks to perform.

This is split into discovery (having the Node trust the Kubernetes Master) and TLS bootstrap (having the Kubernetes Master trust the Node).

see Authenticating with Bootstrap Tokens or the corresponding design proposal.

Preflight checks

`kubeadm` executes a set of preflight checks before starting the join, with the aim to verify preconditions and avoid common cluster startup problems.

Please note that:

1. `kubeadm join` preflight checks are basically a subset `kubeadm init` preflight checks
2. Starting from 1.9, kubeadm provides better support for CRI-generic functionality; in that case, docker specific controls are skipped or replaced by similar controls for crictl.
3. Starting from 1.9, kubeadm provides support for joining nodes running on Windows; in that case, linux specific controls are skipped.
4. In any case the user can skip specific preflight checks (or eventually all preflight checks) with the `--ignore-preflight-errors` option.

Discovery cluster-info

There are 2 main schemes for discovery. The first is to use a shared token along with the IP address of the API server. The second is to provide a file (that is a subset of the standard kubeconfig file).

Shared token discovery

If `kubeadm join` is invoked with `--discovery-token`, token discovery is used; in this case the node basically retrieves the cluster CA certificates from the `cluster-info` ConfigMap in the `kube-public` namespace.

In order to prevent "man in the middle" attacks, several steps are taken:

- First, the CA certificate is retrieved via insecure connection (this is possible because `kubeadm init` granted access to `cluster-info` users for `system:unauthenticated`)
- Then the CA certificate goes trough following validation steps:
  - Basic validation: using the token ID against a JWT signature
  - Pub key validation: using provided `--discovery-token-ca-cert-hash`. This value is available in the output of `kubeadm init` or can be calculated using standard tools (the hash is calculated over the bytes of the Subject Public Key Info (SPKI) object as in RFC7469). The `--discovery-token-ca-cert-hash flag` may be repeated multiple times to allow more than one public key.
  - As a additional validation, the CA certificate is retrieved via secure connection and then compared with the CA retrieved initially

Please note that:

1. Pub key validation can be skipped passing `--discovery-token-unsafe-skip-ca-verification` flag; This weakens the kubeadm security model since others can potentially impersonate the Kubernetes Master.

File/https discovery

If `kubeadm join` is invoked with `--discovery-file`, file discovery is used; this file can be a local file or downloaded via an HTTPS URL; in case of HTTPS, the host installed CA bundle is used to verify the connection.

With file discovery, the cluster CA certificates is provided into the file itself; in fact, the discovery file is a kubeconfig file with only `server` and `certificate-authority-data` attributes set, as described in `kubeadm join` reference doc; when the connection with the cluster is established, kubeadm try to access the `cluster-info` ConfigMap, and if available, uses it.

TLS Bootstrap

Once the cluster info are known, the file `bootstrap-kubelet.conf` is written, thus allowing kubelet to do TLS Bootstrapping (conversely until v.1.7 TLS bootstrapping were managed by kubeadm).

The TLS bootstrap mechanism uses the shared token to temporarily authenticate with the Kubernetes Master to submit a certificate signing request (CSR) for a locally created key pair.

The request is then automatically approved and the operation completes saving `ca.crt` file and `kubelet.conf` file to be used by kubelet for joining the cluster, while`bootstrap-kubelet.conf` is deleted.

Please note that:

- The temporary authentication is validated against the token saved during the `kubeadm init` process (or with additional tokens created with `kubeadm token`)
- The temporary authentication resolve to a user member of `system:bootstrappers:kubeadm:default-no` group which was granted access to CSR api during the `kubeadm init` process
- The automatic CSR approval is managed by the csrapprover controller, according with configuration done the `kubeadm init` process

(optional and alpha in v1.9) Write init kubelet configuration

If kubeadm is invoked with `--feature-gates=DynamicKubeletConfig`:

1. Read the kubelet base configuration from the `kubelet-base-config-v1.9` ConfigMap in the `kube-system` namespace using the Bootstrap Token credentials, and write it to disk as kubelet init configuration file `/var/lib/kubelet/config/init/kubelet`
2. As soon as kubelet starts with the Node's own credential (`/etc/kubernetes/kubelet.conf`), update current node configuration specifying that the source for the node/kubelet configuration is the above ConfigMap.

Please note that:

1. To make dynamic kubelet configuration work, flag `--dynamic-config-dir=/var/lib/kubelet/config/d` should be specified in `/etc/systemd/system/kubelet.service.d/10-kubeadm.conf`

Edit This Page

Feature Gates

This page contains an overview of the various feature gates an administrator can specify on different Kubernetes components.

- Overview
- Using a Feature

Overview

Feature gates are a set of key=value pairs that describe alpha or experimental features. An administrator can use the `--feature-gates` command line flag on each component to turn a feature on or off. The following table is a summary of the feature gates that you can set on different Kubernetes components.

- The "Since" column contains the Kubernetes release when a feature is introduced or its release stage is changed.

- The "Until" column, if not empty, contains the last Kubernetes release in which you can still use a feature gate.

Feature	Default	Stage	Since	Until
`Accelerators`	`false`	Alpha	1.6	1.10
`AdvancedAuditing`	`false`	Alpha	1.7	1.7
`AdvancedAuditing`	`true`	Beta	1.8	1.11
`AdvancedAuditing`	`true`	GA	1.12	-
`AffinityInAnnotations`	`false`	Alpha	1.6	1.7
`AllowExtTrafficLocalEndpoints`	`false`	Beta	1.4	1.6
`AllowExtTrafficLocalEndpoints`	`true`	GA	1.7	-
`APIListChunking`	`false`	Alpha	1.8	1.8
`APIListChunking`	`true`	Beta	1.9	
`APIResponseCompression`	`false`	Alpha	1.7	
`AppArmor`	`true`	Beta	1.4	
`AttachVolumeLimit`	`true`	Alpha	1.11	
`BlockVolume`	`false`	Alpha	1.9	
`CPUManager`	`false`	Alpha	1.8	1.9
`CPUManager`	`true`	Beta	1.10	
`CRIContainerLogRotation`	`false`	Alpha	1.10	1.10
`CRIContainerLogRotation`	`true`	Beta	1.11	
`CSIBlockVolume`	`false`	Alpha	1.11	1.11
`CSIPersistentVolume`	`false`	Alpha	1.9	1.9
`CSIPersistentVolume`	`true`	Beta	1.10	
`CustomPodDNS`	`false`	Alpha	1.9	1.9
`CustomPodDNS`	`true`	Beta	1.10	
`CustomResourceSubresources`	`false`	Alpha	1.10	
`CustomResourceValidation`	`false`	Alpha	1.8	1.8
`CustomResourceValidation`	`true`	Beta	1.9	
`DebugContainers`	`false`	Alpha	1.10	
`DevicePlugins`	`false`	Alpha	1.8	1.9
`DevicePlugins`	`true`	Beta	1.10	
`DynamicKubeletConfig`	`false`	Alpha	1.4	1.10
`DynamicKubeletConfig`	`true`	Beta	1.11	
`DynamicProvisioningScheduling`	`false`	Alpha	1.11	1.11
`DynamicVolumeProvisioning`	`true`	Alpha	1.3	1.7
`DynamicVolumeProvisioning`	`true`	GA	1.8	
`EnableEquivalenceClassCache`	`false`	Alpha	1.8	
`ExpandInUsePersistentVolumes`	`false`	Alpha	1.11	
`ExpandPersistentVolumes`	`false`	Alpha	1.8	1.10
`ExpandPersistentVolumes`	`true`	Beta	1.11	
`ExperimentalCriticalPodAnnotation`	`false`	Alpha	1.5	
`ExperimentalHostUserNamespaceDefaulting`	`false`	Beta	1.5	
`GCERegionalPersistentDisk`	`true`	Beta	1.10	
`HugePages`	`false`	Alpha	1.8	1.9

Feature	Default	Stage	Since	Until
HugePages	true	Beta	1.10	
HyperVContainer	false	Alpha	1.10	
Initializers	false	Alpha	1.7	
KubeletConfigFile	false	Alpha	1.8	1.9
KubeletPluginsWatcher	false	Alpha	1.11	1.11
KubeletPluginsWatcher	true	Beta	1.12	
LocalStorageCapacityIsolation	false	Alpha	1.7	1.9
LocalStorageCapacityIsolation	true	Beta	1.10	
MountContainers	false	Alpha	1.9	
MountPropagation	false	Alpha	1.8	1.9
MountPropagation	true	Beta	1.10	1.11
MountPropagation	true	GA	1.12	
PersistentLocalVolumes	false	Alpha	1.7	1.9
PersistentLocalVolumes	true	Beta	1.10	
PodPriority	false	Alpha	1.8	
PodReadinessGates	false	Alpha	1.11	
PodReadinessGates	true	Beta	1.12	
PodShareProcessNamespace	false	Alpha	1.10	
PodShareProcessNamespace	true	Beta	1.12	
PVCProtection	false	Alpha	1.9	1.9
ReadOnlyAPIDataVolumes	true	Deprecated	1.10	
ResourceLimitsPriorityFunction	false	Alpha	1.9	
RotateKubeletClientCertificate	true	Beta	1.7	
RotateKubeletServerCertificate	false	Alpha	1.7	
RunAsGroup	false	Alpha	1.10	
RuntimeClass	false	Alpha	1.12	
SCTPSupport	false	Alpha	1.12	
ServiceNodeExclusion	false	Alpha	1.8	
StorageObjectInUseProtection	true	Beta	1.10	1.10
StorageObjectInUseProtection	true	GA	1.11	
StreamingProxyRedirects	true	Beta	1.5	
SupportIPVSProxyMode	false	Alpha	1.8	1.8
SupportIPVSProxyMode	false	Beta	1.9	1.9
SupportIPVSProxyMode	true	Beta	1.10	1.10
SupportIPVSProxyMode	true	GA	1.11	
SupportPodPidsLimit	false	Alpha	1.10	
Sysctls	true	Beta	1.11	
TaintBasedEvictions	false	Alpha	1.6	
TaintNodesByCondition	false	Alpha	1.8	
TaintNodesByCondition	true	Beta	1.12	
TokenRequest	false	Alpha	1.10	1.11
TokenRequest	True	Beta	1.12	
TokenRequestProjection	false	Alpha	1.11	1.11
TokenRequestProjection	True	Beta	1.12	

Feature	Default	Stage	Since	Until
`TTLAfterFinished`	`false`	Alpha	1.12	
`VolumeScheduling`	`false`	Alpha	1.9	1.9
`VolumeScheduling`	`true`	Beta	1.10	
`VolumeSubpathEnvExpansion`	`false`	Alpha	1.11	
`ScheduleDaemonSetPods`	`true`	Beta	1.12	

Using a Feature

Feature Stages

A feature can be in *Alpha*, *Beta* or *GA* stage. An *Alpha* feature means:

- Disabled by default.
- Might be buggy. Enabling the feature may expose bugs.
- Support for feature may be dropped at any time without notice.
- The API may change in incompatible ways in a later software release without notice.
- Recommended for use only in short-lived testing clusters, due to increased risk of bugs and lack of long-term support.

A *Beta* feature means:

- Enabled by default.
- The feature is well tested. Enabling the feature is considered safe.
- Support for the overall feature will not be dropped, though details may change.
- The schema and/or semantics of objects may change in incompatible ways in a subsequent beta or stable release. When this happens, we will provide instructions for migrating to the next version. This may require deleting, editing, and re-creating API objects. The editing process may require some thought. This may require downtime for applications that rely on the feature.
- Recommended for only non-business-critical uses because of potential for incompatible changes in subsequent releases. If you have multiple clusters that can be upgraded independently, you may be able to relax this restriction.

  Note: Please do try *Beta* features and give feedback on them! After they exit beta, it may not be practical for us to make more changes.

A *GA* feature is also referred to as a *stable* feature. It means:

- The corresponding feature gate is no longer needed.
- Stable versions of features will appear in released software for many subsequent versions.

Feature Gates

Each feature gate is designed for enabling/disabling a specific feature:

- `Accelerators`: Enable Nvidia GPU support when using Docker
- `AdvancedAuditing`: Enable advanced auditing
- `AffinityInAnnotations`(*deprecated*): Enable setting Pod affinity or anti-affinitys.
- `AllowExtTrafficLocalEndpoints`: Enable a service to route external requests to node local endpoints.
- `APIListChunking`: Enable the API clients to retrieve (`LIST` or `GET`) resources from API server in chunks.
- `APIResponseCompression`: Compress the API responses for `LIST` or `GET` requests.
- `AppArmor`: Enable AppArmor based mandatory access control on Linux nodes when using Docker. See AppArmor Tutorial for more details.
- `AttachVolumeLimit`: Enable volume plugins to report limits on number of volumes that can be attached to a node. See dynamic volume limits for more details.
- `BlockVolume`: Enable the definition and consumption of raw block devices in Pods. See Raw Block Volume Support for more details.
- `CPUManager`: Enable container level CPU affinity support, see CPU Management Policies.
- `CRIContainerLogRotation`: Enable container log rotation for cri container runtime.
- `CSIBlockVolume`: Enable external CSI volume drivers to support block storage. See the `csi` raw block volume support documentation for more details.
- `CSIPersistentVolume`: Enable discovering and mounting volumes provisioned through a CSI (Container Storage Interface) compatible volume plugin. Check the `csi` volume type documentation for more details.
- `CustomPodDNS`: Enable customizing the DNS settings for a Pod using its `dnsConfig` property. Check Pod's DNS Config for more details.
- `CustomResourceSubresources`: Enable `/status` and `/scale` subresources on resources created from CustomResourceDefinition.
- `CustomResourceValidation`: Enable schema based validation on resources created from CustomResourceDefinition.
- `DebugContainers`: Enable running a "debugging" container in a Pod's namespace to troubleshoot a running Pod.
- `DevicePlugins`: Enable the device-plugins based resource provisioning on nodes.
- `DynamicKubeletConfig`: Enable the dynamic configuration of kubelet. See Reconfigure kubelet.
- `DynamicProvisioningScheduling`: Extend the default scheduler to be aware of volume topology and handle PV provisioning. This feature is superceded by the `VolumeScheduling` feature completely in v1.12.

1215

- `DynamicVolumeProvisioning`(*deprecated*): Enable the dynamic provisioning of persistent volumes to Pods.
- `EnableEquivalenceClassCache`: Enable the scheduler to cache equivalence of nodes when scheduling Pods.
- `ExpandInUsePersistentVolumes`: Enable expanding in-use PVCs. See Resizing an in-use PersistentVolumeClaim.
- `ExpandPersistentVolumes`: Enable the expanding of persistent volumes. See Expanding Persistent Volumes Claims.
- `ExperimentalCriticalPodAnnotation`: Enable annotating specific pods as *critical* so that their scheduling is guaranteed.
- `ExperimentalHostUserNamespaceDefaultingGate`: Enabling the defaulting user namespace to host. This is for containers that are using other host namespaces, host mounts, or containers that are privileged or using specific non-namespaced capabilities (e.g. `MKNODE`, `SYS_MODULE` etc.). This should only be enabled if user namespace remapping is enabled in the Docker daemon.
- `GCERegionalPersistentDisk`: Enable the regional PD feature on GCE.
- `HugePages`: Enable the allocation and consumption of pre-allocated huge pages.
- `HyperVContainer`: Enable Hyper-V isolation for Windows containers.
- `Intializers`: Enable the dynamic admission control as an extension to the built-in admission controllers. When the `Initializers` admission controller is enabled, this feature is automatically enabled.
- `KubeletConfigFile`: Enable loading kubelet configuration from a file specified using a config file. See setting kubelet parameters via a config file for more details.
- `KubeletPluginsWatcher`: Enable probe-based plugin watcher utility to enable kubelet to discover plugins such as CSI volume drivers.
- `LocalStorageCapacityIsolation`: Enable the consumption of local ephemeral storage and also the `sizeLimit` property of an emptyDir volume.
- `MountContainers`: Enable using utility containers on host as the volume mounter.
- `MountPropagation`: Enable sharing volume mounted by one container to other containers or pods. For more details, please see mount propagation.
- `PersistentLocalVolumes`: Enable the usage of `local` volume type in Pods. Pod affinity has to be specified if requesting a `local` volume.
- `PodPriority`: Enable the descheduling and preemption of Pods based on their priorities.
- `PodReadinessGates`: Enable the setting of `PodReadinessGate` field for extending Pod readiness evaluation. For more details, please see Pod readiness gate.
- `PVCProtection`: Enable the prevention of a PersistentVolumeClaim (PVC) from being deleted when it is still used by any Pod. More details can be found here.
- `ReadOnlyAPIDataVolumes`: Set Secret, ConfigMap, DownwardAPI and

projected volumes to be mounted in read-only mode. This gate exists
only for backward compatibility. It will be removed in 1.11 release.

- `ResourceLimitsPriorityFunction`: Enable a scheduler priority function
  that assigns a lowest possible score of 1 to a node that satisfies at least
  one of the input Pod's cpu and memory limits. The intent is to break ties
  between nodes with same scores.
- `RotateKubeletClientCertificate`: Enable the rotation of the client
  TLS certificate on the kubelet. See kubelet configuration for more details.
- `RotateKubeletServerCertificate`: Enable the rotation of the server
  TLS certificate on the kubelet. See kubelet configuration for more details.
- `RunAsGroup`: Enable control over the primary group ID set on the init
  processes of containers.
- `RuntimeClass`: Enable the RuntimeClass feature for selecting container
  runtime configurations.
- `ScheduleDaemonSetPods`: Enable DaemonSet Pods to be scheduled by
  the default scheduler instead of the DaemonSet controller.
- `SCTPSupport`: Enables the usage of SCTP as `protocol` value in `Service`,
  `Endpoint`, `NetworkPolicy` and `Pod` definitions
- `ServiceNodeExclusion`: Enable the exclusion of nodes from load bal-
  ancers created by a cloud provider. A node is eligible for exclusion if anno-
  tated with "`alpha.service-controller.kubernetes.io/exclude-balancer`"
  key.
- `StorageObjectInUseProtection`: Postpone the deletion of PersistentVol-
  ume or PersistentVolumeClaim objects if they are still being used.
- `StreamingProxyRedirects`: Instructs the API server to intercept (and
  follow) redirects from the backend (kubelet) for streaming requests. Ex-
  amples of streaming requests include the `exec`, `attach` and `port-forward`
  requests.
- `SupportIPVSProxyMode`: Enable providing in-cluster service load balanc-
  ing using IPVS. See service proxies for more details.
- `SupportPodPidsLimit`: Enable the support to limiting PIDs in Pods.
- `Sysctls`: Enable support for namespaced kernel parameters (sysctls) that
  can be set for each pod. See sysctls for more details.
- `TaintBasedEvictions`: Enable evicting pods from nodes based on taints
  on nodes and tolerations on Pods. See taints and tolerations for more
  details.
- `TaintNodesByCondition`: Enable automatic tainting nodes based on node
  conditions.
- `TokenRequest`: Enable the `TokenRequest` endpoint on service account
  resources.
- `TokenRequestProjection`: Enable the injection of service account tokens
  into a Pod through the `projected` volume.
- `TTLAfterFinished`: Allow a TTL controller to clean up resources after
  they finish execution.
- `VolumeScheduling`: Enable volume topology aware scheduling and make
  the PersistentVolumeClaim (PVC) binding aware of scheduling decisions.

It also enables the usage of `local` volume type when used together with the `PersistentLocalVolumes` feature gate.

Edit This Page

Kubelet authentication/authorization

-
  - Overview
  - Kubelet authentication
  - Kubelet authorization

Overview

A kubelet's HTTPS endpoint exposes APIs which give access to data of varying sensitivity, and allow you to perform operations with varying levels of power on the node and within containers.

This document describes how to authenticate and authorize access to the kubelet's HTTPS endpoint.

Kubelet authentication

By default, requests to the kubelet's HTTPS endpoint that are not rejected by other configured authentication methods are treated as anonymous requests, and given a username of `system:anonymous` and a group of `system:unauthenticated`.

To disable anonymous access and send `401 Unauthorized` responses to unauthenticated requests:

- start the kubelet with the `--anonymous-auth=false` flag

To enable X509 client certificate authentication to the kubelet's HTTPS endpoint:

- start the kubelet with the `--client-ca-file` flag, providing a CA bundle to verify client certificates with
- start the apiserver with `--kubelet-client-certificate` and `--kubelet-client-key` flags
- see the apiserver authentication documentation for more details

To enable API bearer tokens (including service account tokens) to be used to authenticate to the kubelet's HTTPS endpoint:

- ensure the `authentication.k8s.io/v1beta1` API group is enabled in the API server

1218

- start the kubelet with the `--authentication-token-webhook` and `--kubeconfig` flags
- the kubelet calls the `TokenReview` API on the configured API server to determine user information from bearer tokens

Kubelet authorization

Any request that is successfully authenticated (including an anonymous request) is then authorized. The default authorization mode is `AlwaysAllow`, which allows all requests.

There are many possible reasons to subdivide access to the kubelet API:

- anonymous auth is enabled, but anonymous users' ability to call the kubelet API should be limited
- bearer token auth is enabled, but arbitrary API users' (like service accounts) ability to call the kubelet API should be limited
- client certificate auth is enabled, but only some of the client certificates signed by the configured CA should be allowed to use the kubelet API

To subdivide access to the kubelet API, delegate authorization to the API server:

- ensure the `authorization.k8s.io/v1beta1` API group is enabled in the API server
- start the kubelet with the `--authorization-mode=Webhook` and the `--kubeconfig` flags
- the kubelet calls the `SubjectAccessReview` API on the configured API server to determine whether each request is authorized

The kubelet authorizes API requests using the same request attributes approach as the apiserver.

The verb is determined from the incoming request's HTTP verb:

HTTP verb	request verb
POST	create
GET, HEAD	get
PUT	update
PATCH	patch
DELETE	delete

The resource and subresource is determined from the incoming request's path:

Kubelet API	resource	subresource
/stats/*	nodes	stats
/metrics/*	nodes	metrics

1219

Kubelet API	resource	subresource
/logs/*	nodes	log
/spec/*	nodes	spec
all others	nodes	proxy

The namespace and API group attributes are always an empty string, and the resource name is always the name of the kubelet's `Node` API object.

When running in this mode, ensure the user identified by the `--kubelet-client-certificate` and `--kubelet-client-key` flags passed to the apiserver is authorized for the following attributes:

- verb=*, resource=nodes, subresource=proxy
- verb=*, resource=nodes, subresource=stats
- verb=*, resource=nodes, subresource=log
- verb=*, resource=nodes, subresource=spec
- verb=*, resource=nodes, subresource=metrics

Edit This Page

TLS bootstrapping

This document describes how to set up TLS client certificate bootstrapping for kubelets. Kubernetes 1.4 introduced an API for requesting certificates from a cluster-level Certificate Authority (CA). The original intent of this API is to enable provisioning of TLS client certificates for kubelets. The proposal can be found here.

- kube-apiserver configuration
- kube-controller-manager configuration
- kubelet configuration
- kubectl approval

kube-apiserver configuration

The API server should be configured with an authenticator that can authenticate tokens as a user in the `system:bootstrappers` group.

This group will later be used in the controller-manager configuration to scope approvals in the default approval controller. As this feature matures, you should ensure tokens are bound to a Role Based Access Control (RBAC) policy which limits requests (using the bootstrap token) strictly to client requests related to certificate provisioning. With RBAC in place, scoping the tokens to a group

allows for great flexibility (e.g. you could disable a particular bootstrap group's access when you are done provisioning the nodes).

While any authentication strategy can be used for the kubelet's initial bootstrap credentials, the following two authenticators are recommended for ease of provisioning.

1. Bootstrap Tokens - **beta**
2. Token authentication file

Using bootstrap tokens is currently **beta** and will simplify the management of bootstrap token management especially in a HA scenario.

Token authentication file

Tokens are arbitrary but should represent at least 128 bits of entropy derived from a secure random number generator (such as /dev/urandom on most modern Linux systems). There are multiple ways you can generate a token. For example:

```
head -c 16 /dev/urandom | od -An -t x | tr -d ' '
```

will generate tokens that look like `02b50b05283e98dd0fd71db496ef01e8`.

The token file should look like the following example, where the first three values can be anything and the quoted group name should be as depicted:

```
02b50b05283e98dd0fd71db496ef01e8,kubelet-bootstrap,10001,"system:bootstrappers"
```

Add the `--token-auth-file=FILENAME` flag to the kube-apiserver command (in your systemd unit file perhaps) to enable the token file. See docs here for further details.

Client certificate CA bundle

Add the `--client-ca-file=FILENAME` flag to the kube-apiserver command to enable client certificate authentication, referencing a certificate authority bundle containing the signing certificate (e.g. `--client-ca-file=/var/lib/kubernetes/ca.pem`).

kube-controller-manager configuration

The API for requesting certificates adds a certificate-issuing control loop to the Kubernetes Controller Manager. This takes the form of a cfssl local signer using assets on disk. Currently, all certificates issued have one year validity and a default set of key usages.

Signing assets

You must provide a Certificate Authority in order to provide the cryptographic materials necessary to issue certificates. This CA should be trusted by kube-apiserver for authentication with the `--client-ca-file=FILENAME` flag. The management of the CA is beyond the scope of this document but it is recommended that you generate a dedicated CA for Kubernetes. Both certificate and key are assumed to be PEM-encoded.

The kube-controller-manager flags are:

```
--cluster-signing-cert-file="/etc/path/to/kubernetes/ca/ca.crt" --cluster-signing-key-file='
```

The validity duration of signed certificates can be configured with flag:

```
--experimental-cluster-signing-duration
```

SubjectAccessReview Approval Controller

The `csrapproving` controller that ships as part of kube-controller-manager and is enabled by default. The controller uses the `SubjectAccessReview` API to determine if a given user is authorized to request a CSR, then approves based on the authorization outcome. To prevent conflicts with other approvers, the builtin approver doesn't explicitly deny CSRs. It only ignores unauthorized requests. The controller also prunes expired certificates as part of garbage collection.

The controller categorizes CSRs into three subresources:

1. `nodeclient` - a request by a user for a client certificate with `O=system:nodes` and `CN=system:node:(node name)`.
2. `selfnodeclient` - a node renewing a client certificate with the same `O` and `CN`. A node can use its existing client certificate to authenticate this request.

The following RBAC `ClusterRoles` represent the `nodeclient` and `selfnodeclient`, capabilities.

```
# A ClusterRole which instructs the CSR approver to approve a user requesting
# node client credentials.
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: approve-node-client-csr
rules:
- apiGroups: ["certificates.k8s.io"]
  resources: ["certificatesigningrequests/nodeclient"]
  verbs: ["create"]
---
```

```
# A ClusterRole which instructs the CSR approver to approve a node renewing its
# own client credentials.
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: approve-node-client-renewal-csr
rules:
- apiGroups: ["certificates.k8s.io"]
  resources: ["certificatesigningrequests/selfnodeclient"]
  verbs: ["create"]
```

As of 1.8, equivalent roles to the ones listed above are automatically created as part of the default RBAC roles. For 1.8 clusters admins are recommended to bind node bootstrap identities to the following roles instead of creating their own:

- `system:certificates.k8s.io:certificatesigningrequests:nodeclient`
    - Automatically approve CSRs for client certs bound to this role.
- `system:certificates.k8s.io:certificatesigningrequests:selfnodeclient`
    - Automatically approve CSRs when a client bound to its role renews its own certificate.

For example, to grant these permissions to identities attached to bootstrap tokens, an admin would create a `ClusterRoleBinding` targeting the `system:bootstrappers` group:

```
# Approve all CSRs for the group "system:bootstrappers"
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: auto-approve-csrs-for-group
subjects:
- kind: Group
  name: system:bootstrappers
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: approve-node-client-csr
  apiGroup: rbac.authorization.k8s.io
```

To let all nodes renew their own credentials, an admin can create a `ClusterRoleBinding` targeting node identities:

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: node1-client-cert-renewal
subjects:
- kind: Group
```

1223

```
  name: system:nodes
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: approve-node-client-renewal-csr
  apiGroup: rbac.authorization.k8s.io
```

kubelet configuration

To request a client certificate from kube-apiserver, the kubelet first needs a path to a kubeconfig file that contains the credentials for the identity that it will use to bootstrap its individual node identity.

If you are using a bootstrap token, you can use `kubectl config set-cluster`, `set-credentials`, and `set-context` to build this kubeconfig. Provide the name `kubelet-bootstrap` to `kubectl config set-credentials` and include `--token=<token-value>` as follows:

```
kubectl config set-credentials kubelet-bootstrap --token=${BOOTSTRAP_TOKEN} --kubeconfig=boo
```

When starting the kubelet, if the file specified via `--kubeconfig` does not exist, the bootstrap kubeconfig specified via `--bootstrap-kubeconfig` is used to request a client certificate from the API server. On approval of the certificate request and receipt back by the kubelet, a kubeconfig file referencing the generated key and obtained certificate is written to the path specified by `--kubeconfig`. The certificate and key file will be placed in the directory specified by `--cert-dir`.

> **Note:**
>
> The following flags are required to enable this bootstrapping when starting the kubelet:
>
> ```
> --bootstrap-kubeconfig="/path/to/bootstrap/kubeconfig"
> ```

Additionally, in 1.7 the kubelet implements **beta** features for enabling rotation of both its client and/or serving certs. These can be enabled through the respective `RotateKubeletClientCertificate` and `RotateKubeletServerCertificate` feature flags on the kubelet and are enabled by default.

`RotateKubeletClientCertificate` causes the kubelet to rotate its client certificates by creating new CSRs as its existing credentials expire. To enable this feature pass the following flag to the kubelet:

```
--rotate-certificates
```

`RotateKubeletServerCertificate` causes the kubelet to both request a serving certificate after bootstrapping its client credentials and to rotate that certificate. To enable this feature pass the following flag to the kubelet:

```
--rotate-server-certificates
```

> **Note:** The CSR approving controllers implemented in core Kubernetes do not approve node serving certificates for security reasons. To use `RotateKubeletServerCertificate` operators need to run a custom approving controller, or manually approve the serving certificate requests.

kubectl approval

CSRs can be approved outside of the approval flows builtin to the controller manager.

The signing controller does not immediately sign all certificate requests. Instead, it waits until they have been flagged with an "Approved" status by an appropriately-privileged user. This flow is intended to allow for automated approval handled by an external approval controller or the approval controller implemented in the core controller-manager. However cluster administrators can also manually approve certificate requests using kubectl. An administrator can list CSRs with `kubectl get csr` and describe one in detail with `kubectl describe csr <name>`. An administrator can approve or deny a CSR with `kubectl certificate approve <name>` and `kubectl certificate deny <name>`.

Edit This Page

- – cloud-controller-manager
    * Synopsis
    * Options

cloud-controller-manager

Synopsis

The Cloud controller manager is a daemon that embeds the cloud specific control loops shipped with Kubernetes.

```
cloud-controller-manager [flags]
```

Options

--allocate-node-cidrs

Should CIDRs for Pods be allocated and set on the cloud provider.

--authentication-kubeconfig string

kubeconfig file pointing at the 'core' kubernetes server with enough rights to create tokenaccessreviews.authentication.k8s.io. This is optional. If empty, all token requests are considered to be anonymous and no client CA is looked up in the cluster.

--authentication-skip-lookup

If false, the authentication-kubeconfig will be used to lookup missing authentication configuration from the cluster.

--authentication-token-webhook-cache-ttl duration   Default: 10s

The duration to cache responses from the webhook token authenticator.

--authorization-always-allow-paths stringSlice   Default: [/healthz]

A list of HTTP paths to skip during authorization, i.e. these are authorized without contacting the 'core' kubernetes server.

--authorization-kubeconfig string

kubeconfig file pointing at the 'core' kubernetes server with enough rights to create subjectaccessreviews.authorization.k8s.io. This is optional. If empty, all requests not skipped by authorization are forbidden.

--authorization-webhook-cache-authorized-ttl duration   Default: 10s

The duration to cache 'authorized' responses from the webhook authorizer.

--authorization-webhook-cache-unauthorized-ttl duration   Default: 10s

The duration to cache 'unauthorized' responses from the webhook authorizer.

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--bind-address ip   Default: 0.0.0.0

The IP address on which to listen for the --secure-port port. The associated interface(s) must be reachable by the rest of the cluster, and by CLI/web clients. If blank, all interfaces will be used (0.0.0.0 for all IPv4 interfaces and :: for all IPv6 interfaces).

--cert-dir string   Default: "/var/run/kubernetes"

The directory where the TLS certs are located. If --tls-cert-file and --tls-private-key-file are provided, this flag will be ignored.

--cidr-allocator-type string   Default: "RangeAllocator"

Type of CIDR allocator to use

--client-ca-file string

If set, any request presenting a client certificate signed by one of the authorities in the client-ca-file is authenticated with an identity corresponding to the CommonName of the client certificate.

--cloud-config string

The path to the cloud provider configuration file. Empty string for no configuration file.

--cloud-provider string

The provider for cloud services. Empty string for no provider.

--cluster-cidr string

CIDR Range for Pods in cluster. Requires --allocate-node-cidrs to be true

--cluster-name string   Default: "kubernetes"

The instance prefix for the cluster.

--concurrent-service-syncs int32   Default: 1

The number of services that are allowed to sync concurrently. Larger number = more responsive service management, but more CPU (and network) load

--configure-cloud-routes   Default: true

Should CIDRs allocated by allocate-node-cidrs be configured on the cloud provider.

--contention-profiling

Enable lock contention profiling, if profiling is enabled

--controller-start-interval duration

Interval between starting controller managers.

--external-cloud-volume-plugin string

The plugin to use when cloud provider is set to external. Can be empty, should only be set when cloud-provider is external. Currently used to allow node and volume controllers to work for in tree cloud providers.

--feature-gates mapStringBool

A set of key=value pairs that describe feature gates for alpha/experimental features. Options are:
APIListChunking=true|false (BETA - default=true)
APIResponseCompression=true|false (ALPHA - default=false)
AllAlpha=true|false (ALPHA - default=false)
AppArmor=true|false (BETA - default=true)
AttachVolumeLimit=true|false (BETA - default=false)
BalanceAttachedNodeVolumes=true|false (ALPHA - default=false)
BlockVolume=true|false (ALPHA - default=false)

1227

CPUManager=true|false (BETA - default=true)
CRIContainerLogRotation=true|false (BETA - default=true)
CSIBlockVolume=true|false (ALPHA - default=false)
CSIDriverRegistry=true|false (ALPHA - default=false)
CSINodeInfo=true|false (ALPHA - default=false)
CSIPersistentVolume=true|false (BETA - default=true)
CustomCPUCFSQuotaPeriod=true|false (ALPHA - default=false)
CustomPodDNS=true|false (BETA - default=true)
CustomResourceSubresources=true|false (BETA - default=true)
CustomResourceValidation=true|false (BETA - default=true)
DebugContainers=true|false (ALPHA - default=false)
DevicePlugins=true|false (BETA - default=true)
DryRun=true|false (ALPHA - default=false)
DynamicKubeletConfig=true|false (BETA - default=true)
EnableEquivalenceClassCache=true|false (ALPHA - default=false)
ExpandInUsePersistentVolumes=true|false (ALPHA - default=false)
ExpandPersistentVolumes=true|false (BETA - default=true)
ExperimentalCriticalPodAnnotation=true|false (ALPHA - default=false)
ExperimentalHostUserNamespaceDefaulting=true|false (BETA - default=false)
GCERegionalPersistentDisk=true|false (BETA - default=true)
HugePages=true|false (BETA - default=true)
HyperVContainer=true|false (ALPHA - default=false)
Initializers=true|false (ALPHA - default=false)
KubeletPluginsWatcher=true|false (BETA - default=true)
LocalStorageCapacityIsolation=true|false (BETA - default=true)
MountContainers=true|false (ALPHA - default=false)
NodeLease=true|false (ALPHA - default=false)
PersistentLocalVolumes=true|false (BETA - default=true)
PodPriority=true|false (BETA - default=true)
PodReadinessGates=true|false (BETA - default=true)
PodShareProcessNamespace=true|false (BETA - default=true)
ProcMountType=true|false (ALPHA - default=false)
QOSReserved=true|false (ALPHA - default=false)
ResourceLimitsPriorityFunction=true|false (ALPHA - default=false)
ResourceQuotaScopeSelectors=true|false (BETA - default=true)
RotateKubeletClientCertificate=true|false (BETA - default=true)
RotateKubeletServerCertificate=true|false (BETA - default=true)
RunAsGroup=true|false (ALPHA - default=false)
RuntimeClass=true|false (ALPHA - default=false)
SCTPSupport=true|false (ALPHA - default=false)
ScheduleDaemonSetPods=true|false (BETA - default=true)
ServiceNodeExclusion=true|false (ALPHA - default=false)
StreamingProxyRedirects=true|false (BETA - default=true)
SupportPodPidsLimit=true|false (ALPHA - default=false)
Sysctls=true|false (BETA - default=true)
TTLAfterFinished=true|false (ALPHA - default=false)

TaintBasedEvictions=true|false (ALPHA - default=false)
TaintNodesByCondition=true|false (BETA - default=true)
TokenRequest=true|false (BETA - default=true)
TokenRequestProjection=true|false (BETA - default=true)
VolumeScheduling=true|false (BETA - default=true)
VolumeSnapshotDataSource=true|false (ALPHA - default=false)
VolumeSubpathEnvExpansion=true|false (ALPHA - default=false)

-h, --help

help for cloud-controller-manager

--http2-max-streams-per-connection int

The limit that the server gives to clients for the maximum number of streams in an HTTP/2 connection. Zero means to use golang's default.

--kube-api-burst int32   Default: 30

Burst to use while talking with kubernetes apiserver.

--kube-api-content-type string   Default: "application/vnd.kubernetes.protobuf"

Content type of requests sent to apiserver.

--kube-api-qps float32   Default: 20

QPS to use while talking with kubernetes apiserver.

--kubeconfig string

Path to kubeconfig file with authorization and master location information.

--leader-elect   Default: true

Start a leader election client and gain leadership before executing the main loop. Enable this when running replicated components for high availability.

--leader-elect-lease-duration duration   Default: 15s

The duration that non-leader candidates will wait after observing a leadership renewal until attempting to acquire leadership of a led but unrenewed leader slot. This is effectively the maximum duration that a leader can be stopped before it is replaced by another candidate. This is only applicable if leader election is enabled.

--leader-elect-renew-deadline duration   Default: 10s

The interval between attempts by the acting master to renew a leadership slot before it stops leading. This must be less than or equal to the lease duration. This is only applicable if leader election is enabled.

--leader-elect-resource-lock endpoints   Default: "endpoints"

The type of resource object that is used for locking during leader election. Supported options are endpoints (default) and 'configmaps'.

--leader-elect-retry-period duration   Default: 2s

The duration the clients should wait between attempting acquisition and renewal of a leadership. This is only applicable if leader election is enabled.

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--master string

The address of the Kubernetes API server (overrides any value in kubeconfig).

--min-resync-period duration   Default: 12h0m0s

The resync period in reflectors will be random between MinResyncPeriod and 2*MinResyncPeriod.

--node-monitor-period duration   Default: 5s

The period for syncing NodeStatus in NodeController.

--node-status-update-frequency duration   Default: 5m0s

Specifies how often the controller updates nodes' status.

--profiling

Enable profiling via web interface host:port/debug/pprof/

--requestheader-allowed-names stringSlice

List of client certificate common names to allow to provide usernames in headers specified by --requestheader-username-headers. If empty, any client certificate validated by the authorities in --requestheader-client-ca-file is allowed.

--requestheader-client-ca-file string

Root certificate bundle to use to verify client certificates on incoming requests before trusting usernames in headers specified by --requestheader-username-headers. WARNING: generally do not depend on authorization being already done for incoming requests.

--requestheader-extra-headers-prefix stringSlice   Default: [x-remote-extra-]

List of request header prefixes to inspect. X-Remote-Extra- is suggested.

--requestheader-group-headers stringSlice   Default: [x-remote-group]

List of request headers to inspect for groups. X-Remote-Group is suggested.

--requestheader-username-headers stringSlice   Default: [x-remote-user]

List of request headers to inspect for usernames. X-Remote-User is common.

--route-reconciliation-period duration   Default: 10s

The period for reconciling routes created for Nodes by cloud provider.

--secure-port int   Default: 10258

The port on which to serve HTTPS with authentication and authorization.If 0, don't serve HTTPS at all.

--tls-cert-file string

File containing the default x509 Certificate for HTTPS. (CA cert, if any, concatenated after server cert). If HTTPS serving is enabled, and --tls-cert-file and --tls-private-key-file are not provided, a self-signed certificate and key are generated for the public address and saved to the directory specified by --cert-dir.

--tls-cipher-suites stringSlice

Comma-separated list of cipher suites for the server. If omitted, the default Go cipher suites will be use. Possible values: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH

--tls-min-version string

Minimum TLS version supported. Possible values: VersionTLS10, VersionTLS11, VersionTLS12

--tls-private-key-file string

File containing the default x509 private key matching --tls-cert-file.

--tls-sni-cert-key namedCertKey   Default: []

A pair of x509 certificate and private key file paths, optionally suffixed with a list of domain patterns which are fully qualified domain names, possibly with prefixed wildcard segments. If no domain patterns are provided, the names of the certificate are extracted. Non-wildcard matches trump over wildcard matches, explicit domain patterns trump over extracted names. For multiple key/certificate pairs, use the --tls-sni-cert-key multiple times. Examples: "example.crt,example.key" or "foo.crt,foo.key:*.foo.com,foo.com".

--use-service-account-credentials

If true, use individual service account credentials for each controller.

--version version[=true]

Print version information and quit

Edit This Page

- – kube-apiserver
    * Synopsis
    * Options

1231

kube-apiserver

Synopsis

The Kubernetes API server validates and configures data for the api objects which include pods, services, replicationcontrollers, and others. The API Server services REST operations and provides the frontend to the cluster's shared state through which all other components interact.

```
kube-apiserver [flags]
```

Options

--admission-control-config-file string

File with admission control configuration.

--advertise-address ip

The IP address on which to advertise the apiserver to members of the cluster. This address must be reachable by the rest of the cluster. If blank, the --bind-address will be used. If --bind-address is unspecified, the host's default interface will be used.

--allow-privileged

If true, allow privileged containers. [default=false]

--anonymous-auth   Default: true

Enables anonymous requests to the secure port of the API server. Requests that are not rejected by another authentication method are treated as anonymous requests. Anonymous requests have a username of system:anonymous, and a group name of system:unauthenticated.

--apiserver-count int   Default: 1

The number of apiservers running in the cluster, must be a positive number. (In use when --endpoint-reconciler-type=master-count is enabled.)

--audit-log-batch-buffer-size int   Default: 10000

The size of the buffer to store events before batching and writing. Only used in batch mode.

--audit-log-batch-max-size int   Default: 1

The maximum size of a batch. Only used in batch mode.

--audit-log-batch-max-wait duration

The amount of time to wait before force writing the batch that hadn't reached the max size. Only used in batch mode.

--audit-log-batch-throttle-burst int

Maximum number of requests sent at the same moment if ThrottleQPS was not utilized before. Only used in batch mode.

--audit-log-batch-throttle-enable

Whether batching throttling is enabled. Only used in batch mode.

--audit-log-batch-throttle-qps float32

Maximum average number of batches per second. Only used in batch mode.

--audit-log-format string   Default: "json"

Format of saved audits. "legacy" indicates 1-line text format for each event. "json" indicates structured json format. Known formats are legacy,json.

--audit-log-maxage int

The maximum number of days to retain old audit log files based on the timestamp encoded in their filename.

--audit-log-maxbackup int

The maximum number of old audit log files to retain.

--audit-log-maxsize int

The maximum size in megabytes of the audit log file before it gets rotated.

--audit-log-mode string   Default: "blocking"

Strategy for sending audit events. Blocking indicates sending events should block server responses. Batch causes the backend to buffer and write events asynchronously. Known modes are batch,blocking.

--audit-log-path string

If set, all requests coming to the apiserver will be logged to this file. '-' means standard out.

--audit-log-truncate-enabled

Whether event and batch truncating is enabled.

--audit-log-truncate-max-batch-size int   Default: 10485760

Maximum size of the batch sent to the underlying backend. Actual serialized size can be several hundreds of bytes greater. If a batch exceeds this limit, it is split into several batches of smaller size.

--audit-log-truncate-max-event-size int   Default: 102400

Maximum size of the audit event sent to the underlying backend. If the size of an event is greater than this number, first request and response are removed, and if this doesn't reduce the size enough, event is discarded.

--audit-log-version string   Default: "audit.k8s.io/v1beta1"

API group and version used for serializing audit events written to log.

--audit-policy-file string

Path to the file that defines the audit policy configuration.

--audit-webhook-batch-buffer-size int   Default: 10000

The size of the buffer to store events before batching and writing. Only used in batch mode.

--audit-webhook-batch-max-size int   Default: 400

The maximum size of a batch. Only used in batch mode.

--audit-webhook-batch-max-wait duration   Default: 30s

The amount of time to wait before force writing the batch that hadn't reached the max size. Only used in batch mode.

--audit-webhook-batch-throttle-burst int   Default: 15

Maximum number of requests sent at the same moment if ThrottleQPS was not utilized before. Only used in batch mode.

--audit-webhook-batch-throttle-enable   Default: true

Whether batching throttling is enabled. Only used in batch mode.

--audit-webhook-batch-throttle-qps float32   Default: 10

Maximum average number of batches per second. Only used in batch mode.

--audit-webhook-config-file string

Path to a kubeconfig formatted file that defines the audit webhook configuration.

--audit-webhook-initial-backoff duration   Default: 10s

The amount of time to wait before retrying the first failed request.

--audit-webhook-mode string   Default: "batch"

Strategy for sending audit events. Blocking indicates sending events should block server responses. Batch causes the backend to buffer and write events asynchronously. Known modes are batch,blocking.

--audit-webhook-truncate-enabled

Whether event and batch truncating is enabled.

--audit-webhook-truncate-max-batch-size int   Default: 10485760

Maximum size of the batch sent to the underlying backend. Actual serialized size can be several hundreds of bytes greater. If a batch exceeds this limit, it is split into several batches of smaller size.

--audit-webhook-truncate-max-event-size int   Default: 102400

Maximum size of the audit event sent to the underlying backend. If the size of an event is greater than this number, first request and response are removed, and if this doesn't reduce the size enough, event is discarded.

--audit-webhook-version string   Default: "audit.k8s.io/v1beta1"

API group and version used for serializing audit events written to webhook.

--authentication-token-webhook-cache-ttl duration   Default: 2m0s

The duration to cache responses from the webhook token authenticator.

--authentication-token-webhook-config-file string

File with webhook configuration for token authentication in kubeconfig format. The API server will query the remote service to determine authentication for bearer tokens.

--authorization-mode stringSlice   Default: [AlwaysAllow]

Ordered list of plug-ins to do authorization on secure port. Comma-delimited list of: AlwaysAllow,AlwaysDeny,ABAC,Webhook,RBAC,Node.

--authorization-policy-file string

File with authorization policy in csv format, used with --authorization-mode=ABAC, on the secure port.

--authorization-webhook-cache-authorized-ttl duration   Default: 5m0s

The duration to cache 'authorized' responses from the webhook authorizer.

--authorization-webhook-cache-unauthorized-ttl duration   Default: 30s

The duration to cache 'unauthorized' responses from the webhook authorizer.

--authorization-webhook-config-file string

File with webhook configuration in kubeconfig format, used with --authorization-mode=Webhook. The API server will query the remote service to determine access on the API server's secure port.

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--basic-auth-file string

If set, the file that will be used to admit requests to the secure port of the API server via http basic authentication.

--bind-address ip   Default: 0.0.0.0

The IP address on which to listen for the --secure-port port. The associated interface(s) must be reachable by the rest of the cluster, and by CLI/web clients.

If blank, all interfaces will be used (0.0.0.0 for all IPv4 interfaces and :: for all IPv6 interfaces).

--cert-dir string   Default: "/var/run/kubernetes"

The directory where the TLS certs are located. If --tls-cert-file and --tls-private-key-file are provided, this flag will be ignored.

--client-ca-file string

If set, any request presenting a client certificate signed by one of the authorities in the client-ca-file is authenticated with an identity corresponding to the CommonName of the client certificate.

--cloud-config string

The path to the cloud provider configuration file. Empty string for no configuration file.

--cloud-provider string

The provider for cloud services. Empty string for no provider.

--contention-profiling

Enable lock contention profiling, if profiling is enabled

--cors-allowed-origins stringSlice

List of allowed origins for CORS, comma separated. An allowed origin can be a regular expression to support subdomain matching. If this list is empty CORS will not be enabled.

--default-watch-cache-size int   Default: 100

Default watch cache size. If zero, watch cache will be disabled for resources that do not have a default watch size set.

--delete-collection-workers int   Default: 1

Number of workers spawned for DeleteCollection call. These are used to speed up namespace cleanup.

--deserialization-cache-size int

Number of deserialized json objects to cache in memory.

--disable-admission-plugins stringSlice

admission plugins that should be disabled although they are in the default enabled plugins list (NamespaceLifecycle, LimitRanger, ServiceAccount, Priority, DefaultTolerationSeconds, DefaultStorageClass, PersistentVolumeClaimResize, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota). Comma-delimited list of admission plugins: AlwaysAdmit, AlwaysDeny,

AlwaysPullImages, DefaultStorageClass, DefaultTolerationSeconds, DenyEsca-latingExec, DenyExecOnPrivileged, EventRateLimit, ExtendedResourceTol-eration, ImagePolicyWebhook, Initializers, LimitPodHardAntiAffinityTopol-ogy, LimitRanger, MutatingAdmissionWebhook, NamespaceAutoProvision, NamespaceExists, NamespaceLifecycle, NodeRestriction, OwnerReferencesPer-missionEnforcement, PersistentVolumeClaimResize, PersistentVolumeLabel, PodNodeSelector, PodPreset, PodSecurityPolicy, PodTolerationRestriction, Priority, ResourceQuota, SecurityContextDeny, ServiceAccount, StorageOb-jectInUseProtection, ValidatingAdmissionWebhook. The order of plugins in this flag does not matter.

--enable-admission-plugins stringSlice

admission plugins that should be enabled in addition to default enabled ones (NamespaceLifecycle, LimitRanger, ServiceAccount, Priority, De-faultTolerationSeconds, DefaultStorageClass, PersistentVolumeClaimResize, MutatingAdmissionWebhook, ValidatingAdmissionWebhook, ResourceQuota). Comma-delimited list of admission plugins: AlwaysAdmit, AlwaysDeny, AlwaysPullImages, DefaultStorageClass, DefaultTolerationSeconds, DenyEsca-latingExec, DenyExecOnPrivileged, EventRateLimit, ExtendedResourceTol-eration, ImagePolicyWebhook, Initializers, LimitPodHardAntiAffinityTopol-ogy, LimitRanger, MutatingAdmissionWebhook, NamespaceAutoProvision, NamespaceExists, NamespaceLifecycle, NodeRestriction, OwnerReferencesPer-missionEnforcement, PersistentVolumeClaimResize, PersistentVolumeLabel, PodNodeSelector, PodPreset, PodSecurityPolicy, PodTolerationRestriction, Priority, ResourceQuota, SecurityContextDeny, ServiceAccount, StorageOb-jectInUseProtection, ValidatingAdmissionWebhook. The order of plugins in this flag does not matter.

--enable-aggregator-routing

Turns on aggregator routing requests to endpoints IP rather than cluster IP.

--enable-bootstrap-token-auth

Enable to allow secrets of type 'bootstrap.kubernetes.io/token' in the 'kube-system' namespace to be used for TLS bootstrapping authentication.

--enable-garbage-collector   Default: true

Enables the generic garbage collector. MUST be synced with the corresponding flag of the kube-controller-manager.

--enable-logs-handler   Default: true

If true, install a /logs handler for the apiserver logs.

--enable-swagger-ui

Enables swagger ui on the apiserver at /swagger-ui

--endpoint-reconciler-type string   Default: "lease"

Use an endpoint reconciler (master-count, lease, none)

--etcd-cafile string

SSL Certificate Authority file used to secure etcd communication.

--etcd-certfile string

SSL certification file used to secure etcd communication.

--etcd-compaction-interval duration   Default: 5m0s

The interval of compaction requests. If 0, the compaction request from apiserver is disabled.

--etcd-count-metric-poll-period duration   Default: 1m0s

Frequency of polling etcd for number of resources per type. 0 disables the metric collection.

--etcd-keyfile string

SSL key file used to secure etcd communication.

--etcd-prefix string   Default: "/registry"

The prefix to prepend to all resource paths in etcd.

--etcd-servers stringSlice

List of etcd servers to connect with (scheme://ip:port), comma separated.

--etcd-servers-overrides stringSlice

Per-resource etcd servers overrides, comma separated. The individual override format: group/resource#servers, where servers are URLs, semicolon separated.

--event-ttl duration   Default: 1h0m0s

Amount of time to retain events.

--experimental-encryption-provider-config string

The file containing configuration for encryption providers to be used for storing secrets in etcd

--external-hostname string

The hostname to use when generating externalized URLs for this master (e.g. Swagger API Docs).

--feature-gates mapStringBool

A set of key=value pairs that describe feature gates for alpha/experimental features. Options are:
APIListChunking=true|false (BETA - default=true)
APIResponseCompression=true|false (ALPHA - default=false)
AllAlpha=true|false (ALPHA - default=false)

1238

AppArmor=true|false (BETA - default=true)
AttachVolumeLimit=true|false (BETA - default=false)
BalanceAttachedNodeVolumes=true|false (ALPHA - default=false)
BlockVolume=true|false (ALPHA - default=false)
CPUManager=true|false (BETA - default=true)
CRIContainerLogRotation=true|false (BETA - default=true)
CSIBlockVolume=true|false (ALPHA - default=false)
CSIDriverRegistry=true|false (ALPHA - default=false)
CSINodeInfo=true|false (ALPHA - default=false)
CSIPersistentVolume=true|false (BETA - default=true)
CustomCPUCFSQuotaPeriod=true|false (ALPHA - default=false)
CustomPodDNS=true|false (BETA - default=true)
CustomResourceSubresources=true|false (BETA - default=true)
CustomResourceValidation=true|false (BETA - default=true)
DebugContainers=true|false (ALPHA - default=false)
DevicePlugins=true|false (BETA - default=true)
DryRun=true|false (ALPHA - default=false)
DynamicKubeletConfig=true|false (BETA - default=true)
EnableEquivalenceClassCache=true|false (ALPHA - default=false)
ExpandInUsePersistentVolumes=true|false (ALPHA - default=false)
ExpandPersistentVolumes=true|false (BETA - default=true)
ExperimentalCriticalPodAnnotation=true|false (ALPHA - default=false)
ExperimentalHostUserNamespaceDefaulting=true|false (BETA - default=false)
GCERegionalPersistentDisk=true|false (BETA - default=true)
HugePages=true|false (BETA - default=true)
HyperVContainer=true|false (ALPHA - default=false)
Initializers=true|false (ALPHA - default=false)
KubeletPluginsWatcher=true|false (BETA - default=true)
LocalStorageCapacityIsolation=true|false (BETA - default=true)
MountContainers=true|false (ALPHA - default=false)
NodeLease=true|false (ALPHA - default=false)
PersistentLocalVolumes=true|false (BETA - default=true)
PodPriority=true|false (BETA - default=true)
PodReadinessGates=true|false (BETA - default=true)
PodShareProcessNamespace=true|false (BETA - default=true)
ProcMountType=true|false (ALPHA - default=false)
QOSReserved=true|false (ALPHA - default=false)
ResourceLimitsPriorityFunction=true|false (ALPHA - default=false)
ResourceQuotaScopeSelectors=true|false (BETA - default=true)
RotateKubeletClientCertificate=true|false (BETA - default=true)
RotateKubeletServerCertificate=true|false (BETA - default=true)
RunAsGroup=true|false (ALPHA - default=false)
RuntimeClass=true|false (ALPHA - default=false)
SCTPSupport=true|false (ALPHA - default=false)
ScheduleDaemonSetPods=true|false (BETA - default=true)
ServiceNodeExclusion=true|false (ALPHA - default=false)

StreamingProxyRedirects=true|false (BETA - default=true)
SupportPodPidsLimit=true|false (ALPHA - default=false)
Sysctls=true|false (BETA - default=true)
TTLAfterFinished=true|false (ALPHA - default=false)
TaintBasedEvictions=true|false (ALPHA - default=false)
TaintNodesByCondition=true|false (BETA - default=true)
TokenRequest=true|false (BETA - default=true)
TokenRequestProjection=true|false (BETA - default=true)
VolumeScheduling=true|false (BETA - default=true)
VolumeSnapshotDataSource=true|false (ALPHA - default=false)
VolumeSubpathEnvExpansion=true|false (ALPHA - default=false)

-h, --help

help for kube-apiserver

--http2-max-streams-per-connection int

The limit that the server gives to clients for the maximum number of streams in an HTTP/2 connection. Zero means to use golang's default.

--kubelet-certificate-authority string

Path to a cert file for the certificate authority.

--kubelet-client-certificate string

Path to a client cert file for TLS.

--kubelet-client-key string

Path to a client key file for TLS.

--kubelet-https   Default: true

Use https for kubelet connections.

--kubelet-preferred-address-types stringSlice   Default: [Hostname,InternalDNS,InternalIP,ExternalDNS,Exter

List of the preferred NodeAddressTypes to use for kubelet connections.

--kubelet-read-only-port uint   Default: 10255

DEPRECATED: kubelet port.

--kubelet-timeout duration   Default: 5s

Timeout for kubelet operations.

--kubernetes-service-node-port int

If non-zero, the Kubernetes master service (which apiserver creates/maintains) will be of type NodePort, using this as the value of the port. If zero, the Kubernetes master service will be of type ClusterIP.

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--master-service-namespace string   Default: "default"

DEPRECATED: the namespace from which the kubernetes master services should be injected into pods.

--max-connection-bytes-per-sec int

If non-zero, throttle each user connection to this number of bytes/sec. Currently only applies to long-running requests.

--max-mutating-requests-inflight int   Default: 200

The maximum number of mutating requests in flight at a given time. When the server exceeds this, it rejects requests. Zero for no limit.

--max-requests-inflight int   Default: 400

The maximum number of non-mutating requests in flight at a given time. When the server exceeds this, it rejects requests. Zero for no limit.

--min-request-timeout int   Default: 1800

An optional field indicating the minimum number of seconds a handler must keep a request open before timing it out. Currently only honored by the watch request handler, which picks a randomized value above this number as the connection timeout, to spread out load.

--oidc-ca-file string

If set, the OpenID server's certificate will be verified by one of the authorities in the oidc-ca-file, otherwise the host's root CA set will be used.

--oidc-client-id string

The client ID for the OpenID Connect client, must be set if oidc-issuer-url is set.

--oidc-groups-claim string

If provided, the name of a custom OpenID Connect claim for specifying user groups. The claim value is expected to be a string or array of strings. This flag is experimental, please see the authentication documentation for further details.

--oidc-groups-prefix string

If provided, all groups will be prefixed with this value to prevent conflicts with other authentication strategies.

--oidc-issuer-url string

The URL of the OpenID issuer, only HTTPS scheme will be accepted. If set, it will be used to verify the OIDC JSON Web Token (JWT).

--oidc-required-claim mapStringString

A key=value pair that describes a required claim in the ID Token. If set, the claim is verified to be present in the ID Token with a matching value. Repeat this flag to specify multiple claims.

--oidc-signing-algs stringSlice   Default: [RS256]

Comma-separated list of allowed JOSE asymmetric signing algorithms. JWTs with a 'alg' header value not in this list will be rejected. Values are defined by RFC 7518 https://tools.ietf.org/html/rfc7518#section-3.1.

--oidc-username-claim string   Default: "sub"

The OpenID claim to use as the user name. Note that claims other than the default ('sub') is not guaranteed to be unique and immutable. This flag is experimental, please see the authentication documentation for further details.

--oidc-username-prefix string

If provided, all usernames will be prefixed with this value. If not provided, username claims other than 'email' are prefixed by the issuer URL to avoid clashes. To skip any prefixing, provide the value '-'.

--profiling   Default: true

Enable profiling via web interface host:port/debug/pprof/

--proxy-client-cert-file string

Client certificate used to prove the identity of the aggregator or kube-apiserver when it must call out during a request. This includes proxying requests to a user api-server and calling out to webhook admission plugins. It is expected that this cert includes a signature from the CA in the --requestheader-client-ca-file flag. That CA is published in the 'extension-apiserver-authentication' configmap in the kube-system namespace. Components receiving calls from kube-aggregator should use that CA to perform their half of the mutual TLS verification.

--proxy-client-key-file string

Private key for the client certificate used to prove the identity of the aggregator or kube-apiserver when it must call out during a request. This includes proxying requests to a user api-server and calling out to webhook admission plugins.

--request-timeout duration   Default: 1m0s

An optional field indicating the duration a handler must keep a request open before timing it out. This is the default request timeout for requests but may be overridden by flags such as --min-request-timeout for specific types of requests.

--requestheader-allowed-names stringSlice

List of client certificate common names to allow to provide usernames in headers specified by --requestheader-username-headers. If empty, any client certificate validated by the authorities in --requestheader-client-ca-file is allowed.

--requestheader-client-ca-file string

Root certificate bundle to use to verify client certificates on incoming requests before trusting usernames in headers specified by --requestheader-username-headers. WARNING: generally do not depend on authorization being already done for incoming requests.

--requestheader-extra-headers-prefix stringSlice

List of request header prefixes to inspect. X-Remote-Extra- is suggested.

--requestheader-group-headers stringSlice

List of request headers to inspect for groups. X-Remote-Group is suggested.

--requestheader-username-headers stringSlice

List of request headers to inspect for usernames. X-Remote-User is common.

--runtime-config mapStringString

A set of key=value pairs that describe runtime configuration that may be passed to apiserver. <group>/<version> (or <version> for the core group) key can be used to turn on/off specific api versions. api/all is special key to control all api versions, be careful setting it false, unless you know what you do. api/legacy is deprecated, we will remove it in the future, so stop using it.

--secure-port int   Default: 6443

The port on which to serve HTTPS with authentication and authorization.It cannot be switched off with 0.

--service-account-api-audiences stringSlice

Identifiers of the API. The service account token authenticator will validate that tokens used against the API are bound to at least one of these audiences.

--service-account-issuer string

Identifier of the service account token issuer. The issuer will assert this identifier in ”iss” claim of issued tokens. This value is a string or URI.

--service-account-key-file stringArray

File containing PEM-encoded x509 RSA or ECDSA private or public keys, used to verify ServiceAccount tokens. The specified file can contain multiple keys, and the flag can be specified multiple times with different files. If unspecified, --tls-private-key-file is used. Must be specified when --service-account-signing-key is provided

--service-account-lookup   Default: true

If true, validate ServiceAccount tokens exist in etcd as part of authentication.

--service-account-max-token-expiration duration

1243

The maximum validity duration of a token created by the service account token issuer. If an otherwise valid TokenRequest with a validity duration larger than this value is requested, a token will be issued with a validity duration of this value.

--service-account-signing-key-file string

Path to the file that contains the current private key of the service account token issuer. The issuer will sign issued ID tokens with this private key. (Requires the 'TokenRequest' feature gate.)

--service-cluster-ip-range ipNet   Default: 10.0.0.0/24

A CIDR notation IP range from which to assign service cluster IPs. This must not overlap with any IP ranges assigned to nodes for pods.

--service-node-port-range portRange   Default: 30000-32767

A port range to reserve for services with NodePort visibility. Example: '30000-32767'. Inclusive at both ends of the range.

--storage-backend string

The storage backend for persistence. Options: 'etcd3' (default), 'etcd2'.

--storage-media-type string   Default: "application/vnd.kubernetes.protobuf"

The media type to use to store objects in storage. Some resources or storage backends may only support a specific media type and will ignore this setting.

--target-ram-mb int

Memory limit for apiserver in MB (used to configure sizes of caches, etc.)

--tls-cert-file string

File containing the default x509 Certificate for HTTPS. (CA cert, if any, concatenated after server cert). If HTTPS serving is enabled, and --tls-cert-file and --tls-private-key-file are not provided, a self-signed certificate and key are generated for the public address and saved to the directory specified by --cert-dir.

--tls-cipher-suites stringSlice

Comma-separated list of cipher suites for the server. If omitted, the default Go cipher suites will be use. Possible values: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH

--tls-min-version string

Minimum TLS version supported. Possible values: VersionTLS10, VersionTLS11, VersionTLS12

--tls-private-key-file string

File containing the default x509 private key matching --tls-cert-file.

--tls-sni-cert-key namedCertKey   Default: []

A pair of x509 certificate and private key file paths, optionally suffixed with a list of domain patterns which are fully qualified domain names, possibly with prefixed wildcard segments. If no domain patterns are provided, the names of the certificate are extracted. Non-wildcard matches trump over wildcard matches, explicit domain patterns trump over extracted names. For multiple key/certificate pairs, use the --tls-sni-cert-key multiple times. Examples: "example.crt,example.key" or "foo.crt,foo.key:*.foo.com,foo.com".

--token-auth-file string

If set, the file that will be used to secure the secure port of the API server via token authentication.

--version version[=true]

Print version information and quit

--watch-cache   Default: true

Enable watch caching in the apiserver

--watch-cache-sizes stringSlice

List of watch cache sizes for every resource (pods, nodes, etc.), comma separated. The individual override format: resource[.group]#size, where resource is lower-case plural (no version), group is optional, and size is a number. It takes effect when watch-cache is enabled. Some resources (replicationcontrollers, endpoints, nodes, pods, services, apiservices.apiregistration.k8s.io) have system defaults set by heuristics, others default to default-watch-cache-size

Edit This Page

- – kube-controller-manager
  - ∗ Synopsis
  - ∗ Options

kube-controller-manager

Synopsis

The Kubernetes controller manager is a daemon that embeds the core control loops shipped with Kubernetes. In applications of robotics and automation, a control loop is a non-terminating loop that regulates the state of the system. In Kubernetes, a controller is a control loop that watches the shared state of the cluster through the apiserver and makes changes attempting to move the current state towards the desired state. Examples of controllers that ship with Kubernetes today are the replication controller, endpoints controller, namespace controller, and serviceaccounts controller.

```
kube-controller-manager [flags]
```

Options

--allocate-node-cidrs

Should CIDRs for Pods be allocated and set on the cloud provider.

--attach-detach-reconcile-sync-period duration   Default: 1m0s

The reconciler sync wait time between volume attach detach. This duration must be larger than one second, and increasing this value from the default may allow for volumes to be mismatched with pods.

--authentication-kubeconfig string

kubeconfig file pointing at the 'core' kubernetes server with enough rights to create tokenaccessreviews.authentication.k8s.io. This is optional. If empty, all token requests are considered to be anonymous and no client CA is looked up in the cluster.

--authentication-skip-lookup

If false, the authentication-kubeconfig will be used to lookup missing authentication configuration from the cluster.

--authentication-token-webhook-cache-ttl duration   Default: 10s

The duration to cache responses from the webhook token authenticator.

--authorization-always-allow-paths stringSlice   Default: [/healthz]

A list of HTTP paths to skip during authorization, i.e. these are authorized without contacting the 'core' kubernetes server.

--authorization-kubeconfig string

kubeconfig file pointing at the 'core' kubernetes server with enough rights to create subjectaccessreviews.authorization.k8s.io. This is optional. If empty, all requests not skipped by authorization are forbidden.

--authorization-webhook-cache-authorized-ttl duration   Default: 10s

The duration to cache 'authorized' responses from the webhook authorizer.

--authorization-webhook-cache-unauthorized-ttl duration   Default: 10s

The duration to cache 'unauthorized' responses from the webhook authorizer.

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--bind-address ip   Default: 0.0.0.0

The IP address on which to listen for the --secure-port port. The associated interface(s) must be reachable by the rest of the cluster, and by CLI/web clients.

1246

If blank, all interfaces will be used (0.0.0.0 for all IPv4 interfaces and :: for all IPv6 interfaces).

--cert-dir string   Default: "/var/run/kubernetes"

The directory where the TLS certs are located. If --tls-cert-file and --tls-private-key-file are provided, this flag will be ignored.

--cidr-allocator-type string   Default: "RangeAllocator"

Type of CIDR allocator to use

--client-ca-file string

If set, any request presenting a client certificate signed by one of the authorities in the client-ca-file is authenticated with an identity corresponding to the CommonName of the client certificate.

--cloud-config string

The path to the cloud provider configuration file. Empty string for no configuration file.

--cloud-provider string

The provider for cloud services. Empty string for no provider.

--cluster-cidr string

CIDR Range for Pods in cluster. Requires --allocate-node-cidrs to be true

--cluster-name string   Default: "kubernetes"

The instance prefix for the cluster.

--cluster-signing-cert-file string   Default: "/etc/kubernetes/ca/ca.pem"

Filename containing a PEM-encoded X509 CA certificate used to issue cluster-scoped certificates

--cluster-signing-key-file string   Default: "/etc/kubernetes/ca/ca.key"

Filename containing a PEM-encoded RSA or ECDSA private key used to sign cluster-scoped certificates

--concurrent-deployment-syncs int32   Default: 5

The number of deployment objects that are allowed to sync concurrently. Larger number = more responsive deployments, but more CPU (and network) load

--concurrent-endpoint-syncs int32   Default: 5

The number of endpoint syncing operations that will be done concurrently. Larger number = faster endpoint updating, but more CPU (and network) load

--concurrent-gc-syncs int32   Default: 20

The number of garbage collector workers that are allowed to sync concurrently.

--concurrent-namespace-syncs int32   Default: 10

The number of namespace objects that are allowed to sync concurrently. Larger number = more responsive namespace termination, but more CPU (and network) load

--concurrent-replicaset-syncs int32   Default: 5

The number of replica sets that are allowed to sync concurrently. Larger number = more responsive replica management, but more CPU (and network) load

--concurrent-resource-quota-syncs int32   Default: 5

The number of resource quotas that are allowed to sync concurrently. Larger number = more responsive quota management, but more CPU (and network) load

--concurrent-service-syncs int32   Default: 1

The number of services that are allowed to sync concurrently. Larger number = more responsive service management, but more CPU (and network) load

--concurrent-serviceaccount-token-syncs int32   Default: 5

The number of service account token objects that are allowed to sync concurrently. Larger number = more responsive token generation, but more CPU (and network) load

--concurrent-ttl-after-finished-syncs int32   Default: 5

The number of TTL-after-finished controller workers that are allowed to sync concurrently.

--concurrent_rc_syncs int32   Default: 5

The number of replication controllers that are allowed to sync concurrently. Larger number = more responsive replica management, but more CPU (and network) load

--configure-cloud-routes   Default: true

Should CIDRs allocated by allocate-node-cidrs be configured on the cloud provider.

--contention-profiling

Enable lock contention profiling, if profiling is enabled

--controller-start-interval duration

Interval between starting controller managers.

--controllers stringSlice   Default: [*]

A list of controllers to enable. '*' enables all on-by-default controllers, 'foo' enables the controller named 'foo', '-foo' disables the controller named 'foo'.

All controllers: attachdetach, bootstrapsigner, clusterrole-aggregation, cronjob, csrapproving, csrcleaner, csrsigning, daemonset, deployment, disruption, endpoint, garbagecollector, horizontalpodautoscaling, job, namespace, nodeipam, nodelifecycle, persistentvolume-binder, persistentvolume-expander, podgc, pv-protection, pvc-protection, replicaset, replicationcontroller, resourcequota, route, service, serviceaccount, serviceaccount-token, statefulset, tokencleaner, ttl, ttl-after-finished
Disabled-by-default controllers: bootstrapsigner, tokencleaner

--deployment-controller-sync-period duration   Default: 30s

Period for syncing the deployments.

--disable-attach-detach-reconcile-sync

Disable volume attach detach reconciler sync. Disabling this may cause volumes to be mismatched with pods. Use wisely.

--enable-dynamic-provisioning   Default: true

Enable dynamic provisioning for environments that support it.

--enable-garbage-collector   Default: true

Enables the generic garbage collector. MUST be synced with the corresponding flag of the kube-apiserver.

--enable-hostpath-provisioner

Enable HostPath PV provisioning when running without a cloud provider. This allows testing and development of provisioning features. HostPath provisioning is not supported in any way, won't work in a multi-node cluster, and should not be used for anything other than testing or development.

--enable-taint-manager   Default: true

WARNING: Beta feature. If set to true enables NoExecute Taints and will evict all not-tolerating Pod running on Nodes tainted with this kind of Taints.

--experimental-cluster-signing-duration duration   Default: 8760h0m0s

The length of duration signed certificates will be given.

--external-cloud-volume-plugin string

The plugin to use when cloud provider is set to external. Can be empty, should only be set when cloud-provider is external. Currently used to allow node and volume controllers to work for in tree cloud providers.

--feature-gates mapStringBool

A set of key=value pairs that describe feature gates for alpha/experimental features. Options are:
APIListChunking=true|false (BETA - default=true)
APIResponseCompression=true|false (ALPHA - default=false)

AllAlpha=true|false (ALPHA - default=false)
AppArmor=true|false (BETA - default=true)
AttachVolumeLimit=true|false (BETA - default=false)
BalanceAttachedNodeVolumes=true|false (ALPHA - default=false)
BlockVolume=true|false (ALPHA - default=false)
CPUManager=true|false (BETA - default=true)
CRIContainerLogRotation=true|false (BETA - default=true)
CSIBlockVolume=true|false (ALPHA - default=false)
CSIDriverRegistry=true|false (ALPHA - default=false)
CSINodeInfo=true|false (ALPHA - default=false)
CSIPersistentVolume=true|false (BETA - default=true)
CustomCPUCFSQuotaPeriod=true|false (ALPHA - default=false)
CustomPodDNS=true|false (BETA - default=true)
CustomResourceSubresources=true|false (BETA - default=true)
CustomResourceValidation=true|false (BETA - default=true)
DebugContainers=true|false (ALPHA - default=false)
DevicePlugins=true|false (BETA - default=true)
DryRun=true|false (ALPHA - default=false)
DynamicKubeletConfig=true|false (BETA - default=true)
EnableEquivalenceClassCache=true|false (ALPHA - default=false)
ExpandInUsePersistentVolumes=true|false (ALPHA - default=false)
ExpandPersistentVolumes=true|false (BETA - default=true)
ExperimentalCriticalPodAnnotation=true|false (ALPHA - default=false)
ExperimentalHostUserNamespaceDefaulting=true|false (BETA - default=false)
GCERegionalPersistentDisk=true|false (BETA - default=true)
HugePages=true|false (BETA - default=true)
HyperVContainer=true|false (ALPHA - default=false)
Initializers=true|false (ALPHA - default=false)
KubeletPluginsWatcher=true|false (BETA - default=true)
LocalStorageCapacityIsolation=true|false (BETA - default=true)
MountContainers=true|false (ALPHA - default=false)
NodeLease=true|false (ALPHA - default=false)
PersistentLocalVolumes=true|false (BETA - default=true)
PodPriority=true|false (BETA - default=true)
PodReadinessGates=true|false (BETA - default=true)
PodShareProcessNamespace=true|false (BETA - default=true)
ProcMountType=true|false (ALPHA - default=false)
QOSReserved=true|false (ALPHA - default=false)
ResourceLimitsPriorityFunction=true|false (ALPHA - default=false)
ResourceQuotaScopeSelectors=true|false (BETA - default=true)
RotateKubeletClientCertificate=true|false (BETA - default=true)
RotateKubeletServerCertificate=true|false (BETA - default=true)
RunAsGroup=true|false (ALPHA - default=false)
RuntimeClass=true|false (ALPHA - default=false)
SCTPSupport=true|false (ALPHA - default=false)
ScheduleDaemonSetPods=true|false (BETA - default=true)

ServiceNodeExclusion=true|false (ALPHA - default=false)
StreamingProxyRedirects=true|false (BETA - default=true)
SupportPodPidsLimit=true|false (ALPHA - default=false)
Sysctls=true|false (BETA - default=true)
TTLAfterFinished=true|false (ALPHA - default=false)
TaintBasedEvictions=true|false (ALPHA - default=false)
TaintNodesByCondition=true|false (BETA - default=true)
TokenRequest=true|false (BETA - default=true)
TokenRequestProjection=true|false (BETA - default=true)
VolumeScheduling=true|false (BETA - default=true)
VolumeSnapshotDataSource=true|false (ALPHA - default=false)
VolumeSubpathEnvExpansion=true|false (ALPHA - default=false)

--flex-volume-plugin-dir string   Default: ”/usr/libexec/kubernetes/kubelet-plugins/volume/exec/”

Full path of the directory in which the flex volume plugin should search for additional third party volume plugins.

-h, --help

help for kube-controller-manager

--horizontal-pod-autoscaler-cpu-initialization-period duration   Default: 5m0s

The period after pod start when CPU samples might be skipped.

--horizontal-pod-autoscaler-downscale-stabilization duration   Default: 5m0s

The period for which autoscaler will look backwards and not scale down below any recommendation it made during that period.

--horizontal-pod-autoscaler-initial-readiness-delay duration   Default: 30s

The period after pod start during which readiness changes will be treated as initial readiness.

--horizontal-pod-autoscaler-sync-period duration   Default: 15s

The period for syncing the number of pods in horizontal pod autoscaler.

--horizontal-pod-autoscaler-tolerance float   Default: 0.1

The minimum change (from 1.0) in the desired-to-actual metrics ratio for the horizontal pod autoscaler to consider scaling.

--http2-max-streams-per-connection int

The limit that the server gives to clients for the maximum number of streams in an HTTP/2 connection. Zero means to use golang’s default.

--insecure-experimental-approve-all-kubelet-csrs-for-group string

This flag does nothing.

1251

--kube-api-burst int32   Default: 30

Burst to use while talking with kubernetes apiserver.

--kube-api-content-type string   Default: "application/vnd.kubernetes.protobuf"

Content type of requests sent to apiserver.

--kube-api-qps float32   Default: 20

QPS to use while talking with kubernetes apiserver.

--kubeconfig string

Path to kubeconfig file with authorization and master location information.

--large-cluster-size-threshold int32   Default: 50

Number of nodes from which NodeController treats the cluster as large for the
eviction logic purposes. --secondary-node-eviction-rate is implicitly overridden
to 0 for clusters this size or smaller.

--leader-elect   Default: true

Start a leader election client and gain leadership before executing the main loop.
Enable this when running replicated components for high availability.

--leader-elect-lease-duration duration   Default: 15s

The duration that non-leader candidates will wait after observing a leadership
renewal until attempting to acquire leadership of a led but unrenewed leader slot.
This is effectively the maximum duration that a leader can be stopped before
it is replaced by another candidate. This is only applicable if leader election is
enabled.

--leader-elect-renew-deadline duration   Default: 10s

The interval between attempts by the acting master to renew a leadership slot
before it stops leading. This must be less than or equal to the lease duration.
This is only applicable if leader election is enabled.

--leader-elect-resource-lock endpoints   Default: "endpoints"

The type of resource object that is used for locking during leader election. Sup-
ported options are endpoints (default) and 'configmaps'.

--leader-elect-retry-period duration   Default: 2s

The duration the clients should wait between attempting acquisition and renewal
of a leadership. This is only applicable if leader election is enabled.

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--master string

The address of the Kubernetes API server (overrides any value in kubeconfig).

--min-resync-period duration   Default: 12h0m0s

The resync period in reflectors will be random between MinResyncPeriod and 2*MinResyncPeriod.

--namespace-sync-period duration   Default: 5m0s

The period for syncing namespace life-cycle updates

--node-cidr-mask-size int32   Default: 24

Mask size for node cidr in cluster.

--node-eviction-rate float32   Default: 0.1

Number of nodes per second on which pods are deleted in case of node failure when a zone is healthy (see --unhealthy-zone-threshold for definition of healthy/unhealthy). Zone refers to entire cluster in non-multizone clusters.

--node-monitor-grace-period duration   Default: 40s

Amount of time which we allow running Node to be unresponsive before marking it unhealthy. Must be N times more than kubelet's nodeStatusUpdateFrequency, where N means number of retries allowed for kubelet to post node status.

--node-monitor-period duration   Default: 5s

The period for syncing NodeStatus in NodeController.

--node-startup-grace-period duration   Default: 1m0s

Amount of time which we allow starting Node to be unresponsive before marking it unhealthy.

--pod-eviction-timeout duration   Default: 5m0s

The grace period for deleting pods on failed nodes.

--profiling

Enable profiling via web interface host:port/debug/pprof/

--pv-recycler-increment-timeout-nfs int32   Default: 30

the increment of time added per Gi to ActiveDeadlineSeconds for an NFS scrubber pod

--pv-recycler-minimum-timeout-hostpath int32   Default: 60

The minimum ActiveDeadlineSeconds to use for a HostPath Recycler pod. This is for development and testing only and will not work in a multi-node cluster.

--pv-recycler-minimum-timeout-nfs int32   Default: 300

The minimum ActiveDeadlineSeconds to use for an NFS Recycler pod

--pv-recycler-pod-template-filepath-hostpath string

The file path to a pod definition used as a template for HostPath persistent volume recycling. This is for development and testing only and will not work in a multi-node cluster.

--pv-recycler-pod-template-filepath-nfs string

The file path to a pod definition used as a template for NFS persistent volume recycling

--pv-recycler-timeout-increment-hostpath int32   Default: 30

the increment of time added per Gi to ActiveDeadlineSeconds for a HostPath scrubber pod. This is for development and testing only and will not work in a multi-node cluster.

--pvclaimbinder-sync-period duration   Default: 15s

The period for syncing persistent volumes and persistent volume claims

--requestheader-allowed-names stringSlice

List of client certificate common names to allow to provide usernames in headers specified by --requestheader-username-headers. If empty, any client certificate validated by the authorities in --requestheader-client-ca-file is allowed.

--requestheader-client-ca-file string

Root certificate bundle to use to verify client certificates on incoming requests before trusting usernames in headers specified by --requestheader-username-headers. WARNING: generally do not depend on authorization being already done for incoming requests.

--requestheader-extra-headers-prefix stringSlice   Default: [x-remote-extra-]

List of request header prefixes to inspect. X-Remote-Extra- is suggested.

--requestheader-group-headers stringSlice   Default: [x-remote-group]

List of request headers to inspect for groups. X-Remote-Group is suggested.

--requestheader-username-headers stringSlice   Default: [x-remote-user]

List of request headers to inspect for usernames. X-Remote-User is common.

--resource-quota-sync-period duration   Default: 5m0s

The period for syncing quota usage status in the system

--root-ca-file string

If set, this root certificate authority will be included in service account's token secret. This must be a valid PEM-encoded CA bundle.

--route-reconciliation-period duration   Default: 10s

The period for reconciling routes created for Nodes by cloud provider.

--secondary-node-eviction-rate float32   Default: 0.01

Number of nodes per second on which pods are deleted in case of node failure when a zone is unhealthy (see --unhealthy-zone-threshold for definition of healthy/unhealthy). Zone refers to entire cluster in non-multizone clusters. This value is implicitly overridden to 0 if the cluster size is smaller than --large-cluster-size-threshold.

--secure-port int   Default: 10257

The port on which to serve HTTPS with authentication and authorization.If 0, don't serve HTTPS at all.

--service-account-private-key-file string

Filename containing a PEM-encoded private RSA or ECDSA key used to sign service account tokens.

--service-cluster-ip-range string

CIDR Range for Services in cluster. Requires --allocate-node-cidrs to be true

--terminated-pod-gc-threshold int32   Default: 12500

Number of terminated pods that can exist before the terminated pod garbage collector starts deleting terminated pods. If $<= 0$, the terminated pod garbage collector is disabled.

--tls-cert-file string

File containing the default x509 Certificate for HTTPS. (CA cert, if any, concatenated after server cert). If HTTPS serving is enabled, and --tls-cert-file and --tls-private-key-file are not provided, a self-signed certificate and key are generated for the public address and saved to the directory specified by --cert-dir.

--tls-cipher-suites stringSlice

Comma-separated list of cipher suites for the server. If omitted, the default Go cipher suites will be use. Possible values: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH

--tls-min-version string

Minimum TLS version supported. Possible values: VersionTLS10, VersionTLS11, VersionTLS12

--tls-private-key-file string

File containing the default x509 private key matching --tls-cert-file.

--tls-sni-cert-key namedCertKey   Default: []

A pair of x509 certificate and private key file paths, optionally suffixed with a list of domain patterns which are fully qualified domain names, possibly with prefixed wildcard segments. If no domain patterns are provided, the names

of the certificate are extracted. Non-wildcard matches trump over wildcard matches, explicit domain patterns trump over extracted names. For multiple key/certificate pairs, use the --tls-sni-cert-key multiple times. Examples: "example.crt,example.key" or "foo.crt,foo.key:*.foo.com,foo.com".

--unhealthy-zone-threshold float32   Default: 0.55

Fraction of Nodes in a zone which needs to be not Ready (minimum 3) for zone to be treated as unhealthy.

--use-service-account-credentials

If true, use individual service account credentials for each controller.

--version version[=true]

Print version information and quit

Edit This Page

- – kube-proxy
  - * Synopsis
  - * Options

kube-proxy

Synopsis

The Kubernetes network proxy runs on each node. This reflects services as defined in the Kubernetes API on each node and can do simple TCP, UDP, and SCTP stream forwarding or round robin TCP, UDP, and SCTP forwarding across a set of backends. Service cluster IPs and ports are currently found through Docker-links-compatible environment variables specifying ports opened by the service proxy. There is an optional addon that provides cluster DNS for these cluster IPs. The user must create a service with the apiserver API to configure the proxy.

```
kube-proxy [flags]
```

Options

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--bind-address 0.0.0.0   Default: 0.0.0.0

The IP address for the proxy server to serve on (set to 0.0.0.0 for all IPv4 interfaces and '::' for all IPv6 interfaces)

--cleanup

If true cleanup iptables and ipvs rules and exit.

--cleanup-ipvs   Default: true

If true make kube-proxy cleanup ipvs rules before running. Default is true

--cluster-cidr string

The CIDR range of pods in the cluster. When configured, traffic sent to a Service cluster IP from outside this range will be masqueraded and traffic sent from pods to an external LoadBalancer IP will be directed to the respective cluster IP instead

--config string

The path to the configuration file.

--config-sync-period duration   Default: 15m0s

How often configuration from the apiserver is refreshed. Must be greater than 0.

--conntrack-max-per-core int32   Default: 32768

Maximum number of NAT connections to track per CPU core (0 to leave the limit as-is and ignore conntrack-min).

--conntrack-min int32   Default: 131072

Minimum number of conntrack entries to allocate, regardless of conntrack-max-per-core (set conntrack-max-per-core=0 to leave the limit as-is).

--conntrack-tcp-timeout-close-wait duration   Default: 1h0m0s

NAT timeout for TCP connections in the CLOSE_WAIT state

--conntrack-tcp-timeout-established duration   Default: 24h0m0s

Idle timeout for established TCP connections (0 to leave as-is)

--feature-gates mapStringBool

A set of key=value pairs that describe feature gates for alpha/experimental features. Options are:
APIListChunking=true|false (BETA - default=true)
APIResponseCompression=true|false (ALPHA - default=false)
AllAlpha=true|false (ALPHA - default=false)
AppArmor=true|false (BETA - default=true)
AttachVolumeLimit=true|false (BETA - default=false)
BalanceAttachedNodeVolumes=true|false (ALPHA - default=false)
BlockVolume=true|false (ALPHA - default=false)
CPUManager=true|false (BETA - default=true)
CRIContainerLogRotation=true|false (BETA - default=true)

CSIBlockVolume=true|false (ALPHA - default=false)
CSIDriverRegistry=true|false (ALPHA - default=false)
CSINodeInfo=true|false (ALPHA - default=false)
CSIPersistentVolume=true|false (BETA - default=true)
CustomCPUCFSQuotaPeriod=true|false (ALPHA - default=false)
CustomPodDNS=true|false (BETA - default=true)
CustomResourceSubresources=true|false (BETA - default=true)
CustomResourceValidation=true|false (BETA - default=true)
DebugContainers=true|false (ALPHA - default=false)
DevicePlugins=true|false (BETA - default=true)
DryRun=true|false (ALPHA - default=false)
DynamicKubeletConfig=true|false (BETA - default=true)
EnableEquivalenceClassCache=true|false (ALPHA - default=false)
ExpandInUsePersistentVolumes=true|false (ALPHA - default=false)
ExpandPersistentVolumes=true|false (BETA - default=true)
ExperimentalCriticalPodAnnotation=true|false (ALPHA - default=false)
ExperimentalHostUserNamespaceDefaulting=true|false (BETA - default=false)
GCERegionalPersistentDisk=true|false (BETA - default=true)
HugePages=true|false (BETA - default=true)
HyperVContainer=true|false (ALPHA - default=false)
Initializers=true|false (ALPHA - default=false)
KubeletPluginsWatcher=true|false (BETA - default=true)
LocalStorageCapacityIsolation=true|false (BETA - default=true)
MountContainers=true|false (ALPHA - default=false)
NodeLease=true|false (ALPHA - default=false)
PersistentLocalVolumes=true|false (BETA - default=true)
PodPriority=true|false (BETA - default=true)
PodReadinessGates=true|false (BETA - default=true)
PodShareProcessNamespace=true|false (BETA - default=true)
ProcMountType=true|false (ALPHA - default=false)
QOSReserved=true|false (ALPHA - default=false)
ResourceLimitsPriorityFunction=true|false (ALPHA - default=false)
ResourceQuotaScopeSelectors=true|false (BETA - default=true)
RotateKubeletClientCertificate=true|false (BETA - default=true)
RotateKubeletServerCertificate=true|false (BETA - default=true)
RunAsGroup=true|false (ALPHA - default=false)
RuntimeClass=true|false (ALPHA - default=false)
SCTPSupport=true|false (ALPHA - default=false)
ScheduleDaemonSetPods=true|false (BETA - default=true)
ServiceNodeExclusion=true|false (ALPHA - default=false)
StreamingProxyRedirects=true|false (BETA - default=true)
SupportPodPidsLimit=true|false (ALPHA - default=false)
Sysctls=true|false (BETA - default=true)
TTLAfterFinished=true|false (ALPHA - default=false)
TaintBasedEvictions=true|false (ALPHA - default=false)
TaintNodesByCondition=true|false (BETA - default=true)

TokenRequest=true|false (BETA - default=true)
TokenRequestProjection=true|false (BETA - default=true)
VolumeScheduling=true|false (BETA - default=true)
VolumeSnapshotDataSource=true|false (ALPHA - default=false)
VolumeSubpathEnvExpansion=true|false (ALPHA - default=false)

--healthz-bind-address 0.0.0.0   Default: 0.0.0.0:10256

The IP address and port for the health check server to serve on (set to 0.0.0.0 for all IPv4 interfaces and '::' for all IPv6 interfaces)

--healthz-port int32   Default: 10256

The port to bind the health check server. Use 0 to disable.

-h, --help

help for kube-proxy

--hostname-override string

If non-empty, will use this string as identification instead of the actual hostname.

--iptables-masquerade-bit int32   Default: 14

If using the pure iptables proxy, the bit of the fwmark space to mark packets requiring SNAT with. Must be within the range [0, 31].

--iptables-min-sync-period duration

The minimum interval of how often the iptables rules can be refreshed as endpoints and services change (e.g. '5s', '1m', '2h22m').

--iptables-sync-period duration   Default: 30s

The maximum interval of how often iptables rules are refreshed (e.g. '5s', '1m', '2h22m'). Must be greater than 0.

--ipvs-exclude-cidrs stringSlice

A comma-separated list of CIDR's which the ipvs proxier should not touch when cleaning up IPVS rules.

--ipvs-min-sync-period duration

The minimum interval of how often the ipvs rules can be refreshed as endpoints and services change (e.g. '5s', '1m', '2h22m').

--ipvs-scheduler string

The ipvs scheduler type when proxy mode is ipvs

--ipvs-sync-period duration   Default: 30s

The maximum interval of how often ipvs rules are refreshed (e.g. '5s', '1m', '2h22m'). Must be greater than 0.

--kube-api-burst int32   Default: 10

Burst to use while talking with kubernetes apiserver

--kube-api-content-type string   Default: "application/vnd.kubernetes.protobuf"

Content type of requests sent to apiserver.

--kube-api-qps float32   Default: 5

QPS to use while talking with kubernetes apiserver

--kubeconfig string

Path to kubeconfig file with authorization information (the master location is set by the master flag).

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--masquerade-all

If using the pure iptables proxy, SNAT all traffic sent via Service cluster IPs (this not commonly needed)

--master string

The address of the Kubernetes API server (overrides any value in kubeconfig)

--metrics-bind-address 0.0.0.0   Default: 127.0.0.1:10249

The IP address and port for the metrics server to serve on (set to 0.0.0.0 for all IPv4 interfaces and '::' for all IPv6 interfaces)

--nodeport-addresses stringSlice

A string slice of values which specify the addresses to use for NodePorts. Values may be valid IP blocks (e.g. 1.2.3.0/24, 1.2.3.4/32). The default empty string slice ([]) means to use all local addresses.

--oom-score-adj int32   Default: -999

The oom-score-adj value for kube-proxy process. Values must be within the range [-1000, 1000]

--profiling

If true enables profiling via web interface on /debug/pprof handler.

--proxy-mode ProxyMode

Which proxy mode to use: 'userspace' (older) or 'iptables' (faster) or 'ipvs' (experimental). If blank, use the best-available proxy (currently iptables). If the iptables proxy is selected, regardless of how, but the system's kernel or iptables versions are insufficient, this always falls back to the userspace proxy.

--proxy-port-range port-range

Range of host ports (beginPort-endPort, single port or beginPort+offset, inclusive) that may be consumed in order to proxy service traffic. If (unspecified, 0, or 0-0) then ports will be randomly chosen.

--udp-timeout duration   Default: 250ms

How long an idle UDP connection will be kept open (e.g. '250ms', '2s'). Must be greater than 0. Only applicable for proxy-mode=userspace

--version version[=true]

Print version information and quit

--write-config-to string

If set, write the default configuration values to this file and exit.

Edit This Page

- – kube-scheduler
    * Synopsis
    * Options

kube-scheduler

Synopsis

The Kubernetes scheduler is a policy-rich, topology-aware, workload-specific function that significantly impacts availability, performance, and capacity. The scheduler needs to take into account individual and collective resource requirements, quality of service requirements, hardware/software/policy constraints, affinity and anti-affinity specifications, data locality, inter-workload interference, deadlines, and so on. Workload-specific requirements will be exposed through the API as necessary.

```
kube-scheduler [flags]
```

Options

--address string   Default: "0.0.0.0"

DEPRECATED: the IP address on which to listen for the --port port (set to 0.0.0.0 for all IPv4 interfaces and :: for all IPv6 interfaces). See --bind-address instead.

--algorithm-provider string

DEPRECATED: the scheduling algorithm provider to use, one of: ClusterAutoscalerProvider | DefaultProvider

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--config string

The path to the configuration file. Flags override values in this file.

--contention-profiling

DEPRECATED: enable lock contention profiling, if profiling is enabled

--feature-gates mapStringBool

A set of key=value pairs that describe feature gates for alpha/experimental features. Options are:
APIListChunking=true|false (BETA - default=true)
APIResponseCompression=true|false (ALPHA - default=false)
AllAlpha=true|false (ALPHA - default=false)
AppArmor=true|false (BETA - default=true)
AttachVolumeLimit=true|false (BETA - default=false)
BalanceAttachedNodeVolumes=true|false (ALPHA - default=false)
BlockVolume=true|false (ALPHA - default=false)
CPUManager=true|false (BETA - default=true)
CRIContainerLogRotation=true|false (BETA - default=true)
CSIBlockVolume=true|false (ALPHA - default=false)
CSIDriverRegistry=true|false (ALPHA - default=false)
CSINodeInfo=true|false (ALPHA - default=false)
CSIPersistentVolume=true|false (BETA - default=true)
CustomCPUCFSQuotaPeriod=true|false (ALPHA - default=false)
CustomPodDNS=true|false (BETA - default=true)
CustomResourceSubresources=true|false (BETA - default=true)
CustomResourceValidation=true|false (BETA - default=true)
DebugContainers=true|false (ALPHA - default=false)
DevicePlugins=true|false (BETA - default=true)
DryRun=true|false (ALPHA - default=false)
DynamicKubeletConfig=true|false (BETA - default=true)
EnableEquivalenceClassCache=true|false (ALPHA - default=false)
ExpandInUsePersistentVolumes=true|false (ALPHA - default=false)
ExpandPersistentVolumes=true|false (BETA - default=true)
ExperimentalCriticalPodAnnotation=true|false (ALPHA - default=false)
ExperimentalHostUserNamespaceDefaulting=true|false (BETA - default=false)
GCERegionalPersistentDisk=true|false (BETA - default=true)
HugePages=true|false (BETA - default=true)
HyperVContainer=true|false (ALPHA - default=false)
Initializers=true|false (ALPHA - default=false)
KubeletPluginsWatcher=true|false (BETA - default=true)
LocalStorageCapacityIsolation=true|false (BETA - default=true)
MountContainers=true|false (ALPHA - default=false)

NodeLease=true|false (ALPHA - default=false)
PersistentLocalVolumes=true|false (BETA - default=true)
PodPriority=true|false (BETA - default=true)
PodReadinessGates=true|false (BETA - default=true)
PodShareProcessNamespace=true|false (BETA - default=true)
ProcMountType=true|false (ALPHA - default=false)
QOSReserved=true|false (ALPHA - default=false)
ResourceLimitsPriorityFunction=true|false (ALPHA - default=false)
ResourceQuotaScopeSelectors=true|false (BETA - default=true)
RotateKubeletClientCertificate=true|false (BETA - default=true)
RotateKubeletServerCertificate=true|false (BETA - default=true)
RunAsGroup=true|false (ALPHA - default=false)
RuntimeClass=true|false (ALPHA - default=false)
SCTPSupport=true|false (ALPHA - default=false)
ScheduleDaemonSetPods=true|false (BETA - default=true)
ServiceNodeExclusion=true|false (ALPHA - default=false)
StreamingProxyRedirects=true|false (BETA - default=true)
SupportPodPidsLimit=true|false (ALPHA - default=false)
Sysctls=true|false (BETA - default=true)
TTLAfterFinished=true|false (ALPHA - default=false)
TaintBasedEvictions=true|false (ALPHA - default=false)
TaintNodesByCondition=true|false (BETA - default=true)
TokenRequest=true|false (BETA - default=true)
TokenRequestProjection=true|false (BETA - default=true)
VolumeScheduling=true|false (BETA - default=true)
VolumeSnapshotDataSource=true|false (ALPHA - default=false)
VolumeSubpathEnvExpansion=true|false (ALPHA - default=false)

-h, --help

help for kube-scheduler

--kube-api-burst int32   Default: 100

DEPRECATED: burst to use while talking with kubernetes apiserver

--kube-api-content-type string   Default: "application/vnd.kubernetes.protobuf"

DEPRECATED: content type of requests sent to apiserver.

--kube-api-qps float32   Default: 50

DEPRECATED: QPS to use while talking with kubernetes apiserver

--kubeconfig string

DEPRECATED: path to kubeconfig file with authorization and master location information.

--leader-elect   Default: true

Start a leader election client and gain leadership before executing the main loop. Enable this when running replicated components for high availability.

--leader-elect-lease-duration duration   Default: 15s

The duration that non-leader candidates will wait after observing a leadership renewal until attempting to acquire leadership of a led but unrenewed leader slot. This is effectively the maximum duration that a leader can be stopped before it is replaced by another candidate. This is only applicable if leader election is enabled.

--leader-elect-renew-deadline duration   Default: 10s

The interval between attempts by the acting master to renew a leadership slot before it stops leading. This must be less than or equal to the lease duration. This is only applicable if leader election is enabled.

--leader-elect-resource-lock endpoints   Default: "endpoints"

The type of resource object that is used for locking during leader election. Supported options are endpoints (default) and 'configmaps'.

--leader-elect-retry-period duration   Default: 2s

The duration the clients should wait between attempting acquisition and renewal of a leadership. This is only applicable if leader election is enabled.

--lock-object-name string   Default: "kube-scheduler"

DEPRECATED: define the name of the lock object.

--lock-object-namespace string   Default: "kube-system"

DEPRECATED: define the namespace of the lock object.

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--master string

The address of the Kubernetes API server (overrides any value in kubeconfig)

--policy-config-file string

DEPRECATED: file with scheduler policy configuration. This file is used if policy ConfigMap is not provided or --use-legacy-policy-config=true

--policy-configmap string

DEPRECATED: name of the ConfigMap object that contains scheduler's policy configuration. It must exist in the system namespace before scheduler initialization if --use-legacy-policy-config=false. The config must be provided as the value of an element in 'Data' map with the key='policy.cfg'

--policy-configmap-namespace string   Default: "kube-system"

DEPRECATED: the namespace where policy ConfigMap is located. The kube-system namespace will be used if this is not provided or is empty.

--port int   Default: 10251

DEPRECATED: the port on which to serve HTTP insecurely without authentication and authorization. If 0, don't serve HTTPS at all. See --secure-port instead.

--profiling

DEPRECATED: enable profiling via web interface host:port/debug/pprof/

--scheduler-name string   Default: "default-scheduler"

DEPRECATED: name of the scheduler, used to select which pods will be processed by this scheduler, based on pod's "spec.schedulerName".

--use-legacy-policy-config

DEPRECATED: when set to true, scheduler will ignore policy ConfigMap and uses policy config file

--version version[=true]

Print version information and quit

--write-config-to string

If set, write the configuration values to this file and exit.

Edit This Page

- – kubelet
  - ∗ Synopsis
  - ∗ Options

kubelet

Synopsis

The kubelet is the primary "node agent" that runs on each node. The kubelet works in terms of a PodSpec. A PodSpec is a YAML or JSON object that describes a pod. The kubelet takes a set of PodSpecs that are provided through various mechanisms (primarily through the apiserver) and ensures that the containers described in those PodSpecs are running and healthy. The kubelet doesn't manage containers which were not created by Kubernetes.

Other than from a PodSpec from the apiserver, there are three ways that a container manifest can be provided to the Kubelet.

File: Path passed as a flag on the command line. Files under this path will be monitored periodically for updates. The monitoring period is 20s by default and is configurable via a flag.

HTTP endpoint: HTTP endpoint passed as a parameter on the command line. This endpoint is checked every 20 seconds (also configurable with a flag).

HTTP server: The kubelet can also listen for HTTP and respond to a simple API (underspec'd currently) to submit a new manifest.

```
kubelet [flags]
```

Options

--address 0.0.0.0

The IP address for the Kubelet to serve on (set to 0.0.0.0 for all IPv4 interfaces and '::' for all IPv6 interfaces) (default 0.0.0.0)

--allow-privileged

If true, allow containers to request privileged mode.

--alsologtostderr

log to standard error as well as files

--anonymous-auth

Enables anonymous requests to the Kubelet server. Requests that are not rejected by another authentication method are treated as anonymous requests. Anonymous requests have a username of system:anonymous, and a group name of system:unauthenticated. (default true)

--application-metrics-count-limit int

Max number of application metrics to store (per container) (default 100)

--authentication-token-webhook

Use the TokenReview API to determine authentication for bearer tokens.

--authentication-token-webhook-cache-ttl duration

The duration to cache responses from the webhook token authenticator. (default 2m0s)

--authorization-mode string

Authorization mode for Kubelet server. Valid options are AlwaysAllow or Webhook. Webhook mode uses the SubjectAccessReview API to determine authorization. (default "AlwaysAllow")

--authorization-webhook-cache-authorized-ttl duration

1266

The duration to cache 'authorized' responses from the webhook authorizer. (default 5m0s)

--authorization-webhook-cache-unauthorized-ttl duration

The duration to cache 'unauthorized' responses from the webhook authorizer. (default 30s)

--azure-container-registry-config string

Path to the file container Azure container registry configuration information.

--boot-id-file string

Comma-separated list of files to check for boot-id. Use the first one that exists. (default "/proc/sys/kernel/random/boot_id")

--bootstrap-checkpoint-path string

Path to the directory where the checkpoints are stored

--bootstrap-kubeconfig string

Path to a kubeconfig file that will be used to get client certificate for kubelet. If the file specified by --kubeconfig does not exist, the bootstrap kubeconfig is used to request a client certificate from the API server. On success, a kubeconfig file referencing the generated client certificate and key is written to the path specified by --kubeconfig. The client certificate and key file will be stored in the directory pointed by --cert-dir.

--cert-dir string

The directory where the TLS certs are located. If --tls-cert-file and --tls-private-key-file are provided, this flag will be ignored. (default "/var/lib/kubelet/pki")

--cgroup-driver string

Driver that the kubelet uses to manipulate cgroups on the host.

--cgroup-root string

Optional root cgroup to use for pods. This is handled by the container runtime on a best effort basis. Default: '', which means use the container runtime default.

--cgroups-per-qos

Enable creation of QoS cgroup hierarchy, if true top level QoS and pod cgroups are created. (default true)

--chaos-chance float

If > 0.0, introduce random client errors and latency. Intended for testing.

--client-ca-file string

If set, any request presenting a client certificate signed by one of the authorities in the client-ca-file is authenticated with an identity corresponding to the CommonName of the client certificate.

--cloud-config string

The path to the cloud provider configuration file.

--cloud-provider string

The provider for cloud services. Specify empty string for running with no cloud provider.

--cloud-provider-gce-lb-src-cidrs cidrs

CIDRs opened in GCE firewall for LB traffic proxy & health checks (default 130.211.0.0/22,35.191.0.0/16,209.85.152.0/22,209.85.204.0/22)

--cluster-dns stringSlice

Comma-separated list of DNS server IP address.

--cluster-domain string

Domain for this cluster.

--cni-bin-dir string

The full path of the directory in which to search for CNI plugin binaries. Default: /opt/cni/bin

--cni-conf-dir string

The full path of the directory in which to search for CNI config files. Default: /etc/cni/net.d

--container-hints string

location of the container hints file (default "/etc/cadvisor/container_hints.json")

--container-runtime string

The container runtime to use. Possible values: 'docker', 'remote', 'rkt(deprecated)'. (default "docker")

--container-runtime-endpoint string

[Experimental] The endpoint of remote runtime service. Currently unix socket is supported on Linux, and tcp is supported on windows.

--containerd string

containerd endpoint (default "unix:///var/run/containerd.sock")

--containerized

Experimental support for running kubelet in a container.

--contention-profiling

Enable lock contention profiling, if profiling is enabled

--cpu-cfs-quota

Enable CPU CFS quota enforcement for containers that specify CPU limits (default true)

--cpu-manager-policy string

CPU Manager policy to use. Possible values: 'none', 'static'. (default "none")

--cpu-manager-reconcile-period NodeStatusUpdateFrequency

CPU Manager reconciliation period. Examples: '10s', or '1m'. If not supplied, defaults to NodeStatusUpdateFrequency (default 10s)

--docker string

docker endpoint (default "unix:///var/run/docker.sock")

--docker-disable-shared-pid

The Container Runtime Interface (CRI) defaults to using a shared PID namespace for containers in a pod when running with Docker 1.13.1 or higher. Setting this flag reverts to the previous behavior of isolated PID namespaces. This ability will be removed in a future Kubernetes release. (default true)

--docker-endpoint string

Use this for the docker endpoint to communicate with (default "unix:///var/run/docker.sock")

--docker-env-metadata-whitelist string

a comma-separated list of environment variable keys that needs to be collected for docker containers

--docker-only

Only report docker containers in addition to root stats

--docker-root string

DEPRECATED: docker root is read from docker info (this is a fallback, default: /var/lib/docker) (default "/var/lib/docker")

--docker-tls

use TLS to connect to docker

--docker-tls-ca string

path to trusted CA (default "ca.pem")

--docker-tls-cert string

path to client certificate (default "cert.pem")

--docker-tls-key string

path to private key (default "key.pem")

--dynamic-config-dir string

The Kubelet will use this directory for checkpointing downloaded configurations and tracking configuration health. The Kubelet will create this directory if it does not already exist. The path may be absolute or relative; relative paths start at the Kubelet's current working directory. Providing this flag enables dynamic Kubelet configuration. Presently, you must also enable the DynamicKubeletConfig feature gate to pass this flag.

--enable-controller-attach-detach

Enables the Attach/Detach controller to manage attachment/detachment of volumes scheduled to this node, and disables kubelet from executing any attach/detach operations (default true)

--enable-debugging-handlers

Enables server endpoints for log collection and local running of containers and commands (default true)

--enable-load-reader

Whether to enable cpu load reader

--enable-server

Enable the Kubelet's server (default true)

--enforce-node-allocatable stringSlice

A comma separated list of levels of node allocatable enforcement to be enforced by kubelet. Acceptable options are 'pods', 'system-reserved' & 'kube-reserved'. If the latter two options are specified, '--system-reserved-cgroup' & '--kube-reserved-cgroup' must also be set respectively. See https://kubernetes.io/docs/tasks/administer-cluster/reserve-compute-resources/ for more details. (default [pods])

--event-burst int32

Maximum size of a bursty event records, temporarily allows event records to burst to this number, while still not exceeding event-qps. Only used if --event-qps > 0 (default 10)

--event-qps int32

If > 0, limit event creations per second to this value. If 0, unlimited. (default 5)

--event-storage-age-limit string

Max length of time for which to store events (per type). Value is a comma separated list of key values, where the keys are event types (e.g.: creation, oom) or "default" and the value is a duration. Default is applied to all non-specified event types (default "default=0")

--event-storage-event-limit string

Max number of events to store (per type). Value is a comma separated list of key values, where the keys are event types (e.g.: creation, oom) or "default" and the value is an integer. Default is applied to all non-specified event types (default "default=0")

--eviction-hard mapStringString

A set of eviction thresholds (e.g. memory.available<1Gi) that if met would trigger a pod eviction. (default imagefs.available<15%,memory.available<100Mi,nodefs.available<10%,nodefs.inod

--eviction-max-pod-grace-period int32

Maximum allowed grace period (in seconds) to use when terminating pods in response to a soft eviction threshold being met.

--eviction-minimum-reclaim mapStringString

A set of minimum reclaims (e.g. imagefs.available=2Gi) that describes the minimum amount of resource the kubelet will reclaim when performing a pod eviction if that resource is under pressure.

--eviction-pressure-transition-period duration

Duration for which the kubelet has to wait before transitioning out of an eviction pressure condition. (default 5m0s)

--eviction-soft mapStringString

A set of eviction thresholds (e.g. memory.available<1.5Gi) that if met over a corresponding grace period would trigger a pod eviction.

--eviction-soft-grace-period mapStringString

A set of eviction grace periods (e.g. memory.available=1m30s) that correspond to how long a soft eviction threshold must hold before triggering a pod eviction.

--exit-on-lock-contention

Whether kubelet should exit upon lock-file contention.

--experimental-allocatable-ignore-eviction

When set to 'true', Hard Eviction Thresholds will be ignored while calculating Node Allocatable. See https://kubernetes.io/docs/tasks/administer-cluster/reserve-compute-resources/ for more details. [default=false]

--experimental-allowed-unsafe-sysctls stringSlice

Comma-separated whitelist of unsafe sysctls or unsafe sysctl patterns (ending in *). Use these at your own risk.

--experimental-bootstrap-kubeconfig string

deprecated: use --bootstrap-kubeconfig

--experimental-check-node-capabilities-before-mount

[Experimental] if set true, the kubelet will check the underlying node for required components (binaries, etc.) before performing the mount

--experimental-kernel-memcg-notification

If enabled, the kubelet will integrate with the kernel memcg notification to determine if memory eviction thresholds are crossed rather than polling.

--experimental-mounter-path string

[Experimental] Path of mounter binary. Leave empty to use the default mount.

--experimental-qos-reserved mapStringString

A set of ResourceName=Percentage (e.g. memory=50%) pairs that describe how pod resource requests are reserved at the QoS level. Currently only memory is supported. [default=none]

--fail-swap-on

Makes the Kubelet fail to start if swap is enabled on the node.

--feature-gates mapStringBool

A set of key=value pairs that describe feature gates for alpha/experimental features. Options are:
APIListChunking=true|false (BETA - default=true)
APIResponseCompression=true|false (ALPHA - default=false)
Accelerators=true|false
AdvancedAuditing=true|false (BETA - default=true)
AllAlpha=true|false (ALPHA - default=false)
AllowExtTrafficLocalEndpoints=true|false
AppArmor=true|false (BETA - default=true)
BlockVolume=true|false (ALPHA - default=false)
CPUManager=true|false (BETA - default=true)
CSIPersistentVolume=true|false (ALPHA - default=false)
CustomPodDNS=true|false (ALPHA - default=false)
CustomResourceValidation=true|false (BETA - default=true)
DebugContainers=true|false
DevicePlugins=true|false (ALPHA - default=false)
DynamicKubeletConfig=true|false (ALPHA - default=false)
EnableEquivalenceClassCache=true|false (ALPHA - default=false)
ExpandPersistentVolumes=true|false (ALPHA - default=false)
ExperimentalCriticalPodAnnotation=true|false (ALPHA - default=false)

ExperimentalHostUserNamespaceDefaulting=true|false (BETA - default=false)
HugePages=true|false (ALPHA - default=false)
Initializers=true|false (ALPHA - default=false)
KubeletConfigFile=true|false (ALPHA - default=false)
LocalStorageCapacityIsolation=true|false (ALPHA - default=false)
MountContainers=true|false (ALPHA - default=false)
MountPropagation=true|false (ALPHA - default=false)
PVCProtection=true|false (ALPHA - default=false)
PersistentLocalVolumes=true|false (ALPHA - default=false)
PodPriority=true|false (ALPHA - default=false)
ReadOnlyAPIDataVolumes=true|false
ResourceLimitsPriorityFunction=true|false (ALPHA - default=false)
RotateKubeletClientCertificate=true|false (BETA - default=true)
RotateKubeletServerCertificate=true|false (ALPHA - default=false)
ServiceNodeExclusion=true|false (ALPHA - default=false)
ServiceProxyAllowExternalIPs=true|false
StreamingProxyRedirects=true|false (BETA - default=true)
SupportIPVSProxyMode=true|false (ALPHA - default=false)
TaintBasedEvictions=true|false (ALPHA - default=false)
TaintNodesByCondition=true|false (ALPHA - default=false)
VolumeScheduling=true|false (ALPHA - default=false)
VolumeSubpath=true|false

--file-check-frequency duration

Duration between checking config files for new data (default 20s)

--global-housekeeping-interval duration

Interval between global housekeepings (default 1m0s)

--google-json-key string

The Google Cloud Platform Service Account JSON Key to use for authentication.

--hairpin-mode string

How should the kubelet setup hairpin NAT. This allows endpoints of a Service to loadbalance back to themselves if they should try to access their own Service. Valid values are "promiscuous-bridge", "hairpin-veth" and "none". (default "promiscuous-bridge")

--healthz-bind-address 0.0.0.0

The IP address for the healthz server to serve on (set to 0.0.0.0 for all IPv4 interfaces and '::' for all IPv6 interfaces) (default 127.0.0.1)

--healthz-port int32

The port of the localhost healthz endpoint (set to 0 to disable) (default 10248)

--host-ipc-sources stringSlice

Comma-separated list of sources from which the Kubelet allows pods to use the host ipc namespace. (default [*])

--host-network-sources stringSlice

Comma-separated list of sources from which the Kubelet allows pods to use of host network. (default [*])

--host-pid-sources stringSlice

Comma-separated list of sources from which the Kubelet allows pods to use the host pid namespace. (default [*])

--hostname-override string

If non-empty, will use this string as identification instead of the actual hostname.

--housekeeping-interval duration

Interval between container housekeepings (default 10s)

--http-check-frequency duration

Duration between checking http for new data (default 20s)

--image-gc-high-threshold int32

The percent of disk usage after which image garbage collection is always run. (default 85)

--image-gc-low-threshold int32

The percent of disk usage before which image garbage collection is never run. Lowest disk usage to garbage collect to. (default 80)

--image-pull-progress-deadline duration

If no pulling progress is made before this deadline, the image pulling will be cancelled. (default 1m0s)

--image-service-endpoint string

[Experimental] The endpoint of remote image service. If not specified, it will be the same with container-runtime-endpoint by default. Currently unix socket is supported on Linux, and tcp is supported on windows.

--init-config-dir string

The Kubelet will look in this directory for the init configuration. The path may be absolute or relative; relative paths start at the Kubelet's current working directory. Omit this argument to use the built-in default configuration values. Presently, you must also enable the KubeletConfigFile feature gate to pass this flag.

--iptables-drop-bit int32

1274

The bit of the fwmark space to mark packets for dropping. Must be within the range [0, 31]. (default 15)

--iptables-masquerade-bit int32

The bit of the fwmark space to mark packets for SNAT. Must be within the range [0, 31]. Please match this parameter with corresponding parameter in kube-proxy. (default 14)

--kube-api-burst int32

Burst to use while talking with kubernetes apiserver (default 10)

--kube-api-content-type string

Content type of requests sent to apiserver. (default "application/vnd.kubernetes.protobuf")

--kube-api-qps int32

QPS to use while talking with kubernetes apiserver (default 5)

--kube-reserved mapStringString

A set of ResourceName=ResourceQuantity (e.g. cpu=200m,memory=500Mi,ephemeral-storage=1Gi) pairs that describe resources reserved for kubernetes system components. Currently cpu, memory and local ephemeral storage for root file system are supported. See http://kubernetes.io/docs/user-guide/compute-resources for more detail. [default=none]

--kube-reserved-cgroup string

Absolute name of the top level cgroup that is used to manage kubernetes components for which compute resources were reserved via '--kube-reserved' flag. Ex. '/kube-reserved'. [default=""]

--kubeconfig string

Path to a kubeconfig file, specifying how to connect to the API server. (default "/var/lib/kubelet/kubeconfig")

--kubelet-cgroups string

Optional absolute name of cgroups to create and run the Kubelet in.

--lock-file string

The path to file for kubelet to use as a lock file.

--log-backtrace-at traceLocation

when logging hits line file:N, emit a stack trace (default :0)

--log-cadvisor-usage

Whether to log the usage of the cAdvisor container

--log-dir string

If non-empty, write log files in this directory

--log-flush-frequency duration

Maximum number of seconds between log flushes (default 5s)

--logtostderr

log to standard error instead of files (default true)

--machine-id-file string

Comma-separated list of files to check for machine-id. Use the first one that exists. (default "/etc/machine-id,/var/lib/dbus/machine-id")

--make-iptables-util-chains

If true, kubelet will ensure iptables utility rules are present on host. (default true)

--manifest-url string

URL for accessing the container manifest

--manifest-url-header --manifest-url-header 'a:hello,b:again,c:world' --manifest-url-header 'b:beautiful'

Comma-separated list of HTTP headers to use when accessing the manifest URL. Multiple headers with the same name will be added in the same order provided. This flag can be repeatedly invoked. For example: --manifest-url-header 'a:hello,b:again,c:world' --manifest-url-header 'b:beautiful'

--max-open-files int

Number of files that can be opened by Kubelet process. (default 1000000)

--max-pods int32

Number of Pods that can run on this Kubelet. (default 110)

--minimum-image-ttl-duration duration

Minimum age for an unused image before it is garbage collected.

--network-plugin string

The name of the network plugin to be invoked for various events in kubelet/pod lifecycle

--network-plugin-mtu int32

The MTU to be passed to the network plugin, to override the default. Set to 0 to use the default 1460 MTU.

--node-ip string

IP address of the node. If set, kubelet will use this IP address for the node

1276

--node-labels mapStringString

Labels to add when registering the node in the cluster.

--node-status-update-frequency duration

Specifies how often kubelet posts node status to master. Note: be cautious when changing the constant, it must work with nodeMonitorGracePeriod in nodecontroller. (default 10s)

--oom-score-adj int32

The oom-score-adj value for kubelet process. Values must be within the range [-1000, 1000] (default -999)

--pod-cidr string

The CIDR to use for pod IP addresses, only used in standalone mode.

--pod-infra-container-image string

The image whose network/ipc namespaces containers in each pod will use. (default "k8s.gcr.io/pause:3.1")

--pod-manifest-path string

Path to the directory containing pod manifest files to run, or the path to a single pod manifest file. Files starting with dots will be ignored.

--pods-per-core int32

Number of Pods per core that can run on this Kubelet. The total number of Pods on this Kubelet cannot exceed max-pods, so max-pods will be used if this calculation results in a larger number of Pods allowed on the Kubelet. A value of 0 disables this limit.

--port int32

The port for the Kubelet to serve on. (default 10250)

--protect-kernel-defaults

Default kubelet behaviour for kernel tuning. If set, kubelet errors if any of kernel tunables is different than kubelet defaults.

--provider-id string

Unique identifier for identifying the node in a machine database, i.e cloud-provider

--read-only-port int32

The read-only port for the Kubelet to serve on with no authentication/authorization (set to 0 to disable) (default 10255)

--really-crash-for-testing

If true, when panics occur crash. Intended for testing.

--register-node

Register the node with the apiserver. If --kubeconfig is not provided, this flag is irrelevant, as the Kubelet won't have an apiserver to register with. Default=true. (default true)

--register-with-taints []api.Taint

Register the node with the given list of taints (comma separated "=:"). No-op if register-node is false.

--registry-burst int32

Maximum size of bursty pulls, temporarily allows pulls to burst to this number, while still not exceeding registry-qps. Only used if --registry-qps > 0 (default 10)

--registry-qps int32

If > 0, limit registry pull QPS to this value.

--resolv-conf string

Resolver configuration file used as the basis for the container DNS resolution configuration. (default "/etc/resolv.conf")

--root-dir string

Directory path for managing kubelet files (volume mounts,etc). (default "/var/lib/kubelet")

--rotate-certificates

Auto rotate the kubelet client certificates by requesting new certificates from the kube-apiserver when the certificate expiration approaches.

--runonce

If true, exit after spawning pods from local manifests or remote urls. Exclusive with --enable-server

--runtime-cgroups string

Optional absolute name of cgroups to create and run the runtime in.

--runtime-request-timeout duration

Timeout of all runtime requests except long running request - pull, logs, exec and attach. When timeout exceeded, kubelet will cancel the request, throw out an error and retry later. (default 2m0s)

--seccomp-profile-root string

Directory path for seccomp profiles. (default "/var/lib/kubelet/seccomp")

--serialize-image-pulls

Pull images one at a time. We recommend *not* changing the default value on nodes that run docker daemon with version < 1.9 or an Aufs storage backend. Issue #10959 has more details. (default true)

--stderrthreshold severity

logs at or above this threshold go to stderr (default 2)

--storage-driver-buffer-duration duration

Writes in the storage driver will be buffered for this duration, and committed to the non memory backends as a single transaction (default 1m0s)

--storage-driver-db string

database name (default "cadvisor")

--storage-driver-host string

database host:port (default "localhost:8086")

--storage-driver-password string

database password (default "root")

--storage-driver-secure

use secure connection with database

--storage-driver-table string

table name (default "stats")

--storage-driver-user string

database username (default "root")

--streaming-connection-idle-timeout duration

Maximum time a streaming connection can be idle before the connection is automatically closed. 0 indicates no timeout. Example: '5m' (default 4h0m0s)

--sync-frequency duration

Max period between synchronizing running containers and config (default 1m0s)

--system-cgroups /

Optional absolute name of cgroups in which to place all non-kernel processes that are not already inside a cgroup under /. Empty for no container. Rolling back the flag requires a reboot.

--system-reserved mapStringString

A set of ResourceName=ResourceQuantity (e.g. cpu=200m,memory=500Mi,ephemeral-storage=1Gi) pairs that describe resources reserved for non-kubernetes

components. Currently only cpu and memory are supported. See http://kubernetes.io/docs/user-guide/compute-resources for more detail. [default=none]

--system-reserved-cgroup string

Absolute name of the top level cgroup that is used to manage non-kubernetes components for which compute resources were reserved via '--system-reserved' flag. Ex. '/system-reserved'. [default='']

--tls-cert-file string

File containing x509 Certificate used for serving HTTPS (with intermediate certs, if any, concatenated after server cert). If --tls-cert-file and --tls-private-key-file are not provided, a self-signed certificate and key are generated for the public address and saved to the directory passed to --cert-dir.

--tls-cipher-suites stringSlice

Comma-separated list of cipher suites for the server. If omitted, the default Go cipher suites will be used. Possible values: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECD

--tls-private-key-file string

File containing x509 private key matching --tls-cert-file.

-v, --v Level

log level for V logs

--version version[=true]

Print version information and quit

--vmodule moduleSpec

comma-separated list of pattern=N settings for file-filtered logging

--volume-plugin-dir string

The full path of the directory in which to search for additional third party volume plugins (default "/usr/libexec/kubernetes/kubelet-plugins/volume/exec/")

--volume-stats-agg-period duration

Specifies interval for kubelet to calculate and cache the volume disk usage for all pods and volumes.

-h, --help

help for kubelet

Edit This Page

∗ SEE ALSO

kubectl

kubectl controls the Kubernetes cluster manager

Synopsis

kubectl controls the Kubernetes cluster manager.

Find more information at: https://kubernetes.io/docs/reference/kubectl/overview/

```
kubectl [flags]
```

Options

--allow-verification-with-non-compliant-keys

Allow a SignatureVerifier to use keys which are technically non-compliant with RFC6962.

--alsologtostderr

log to standard error as well as files

--as string

Username to impersonate for the operation

--as-group stringArray

Group to impersonate for the operation, this flag can be repeated to specify multiple groups.

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--cache-dir string   Default: "/Users/zarnold/.kube/http-cache"

Default HTTP cache directory

--certificate-authority string

Path to a cert file for the certificate authority

--client-certificate string

Path to a client certificate file for TLS

--client-key string

Path to a client key file for TLS

--cloud-provider-gce-lb-src-cidrs cidrs   Default: 130.211.0.0/22,209.85.152.0/22,209.85.204.0/22,35.191.0.0/16

CIDRs opened in GCE firewall for LB traffic proxy & health checks

--cluster string

The name of the kubeconfig cluster to use

--context string

The name of the kubeconfig context to use

--default-not-ready-toleration-seconds int   Default: 300

Indicates the tolerationSeconds of the toleration for notReady:NoExecute that is added by default to every pod that does not already have such a toleration.

--default-unreachable-toleration-seconds int   Default: 300

Indicates the tolerationSeconds of the toleration for unreachable:NoExecute that is added by default to every pod that does not already have such a toleration.

-h, --help

help for kubectl

--insecure-skip-tls-verify

If true, the server's certificate will not be checked for validity. This will make your HTTPS connections insecure

--kubeconfig string

Path to the kubeconfig file to use for CLI requests.

--log-backtrace-at traceLocation   Default: :0

when logging hits line file:N, emit a stack trace

--log-dir string

If non-empty, write log files in this directory

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--logtostderr   Default: true

log to standard error instead of files

--match-server-version

Require server version to match client version

-n, --namespace string

If present, the namespace scope for this CLI request

--request-timeout string   Default: "0"

The length of time to wait before giving up on a single server request. Non-zero values should contain a corresponding time unit (e.g. 1s, 2m, 3h). A value of zero means don't timeout requests.

-s, --server string

The address and port of the Kubernetes API server

--stderrthreshold severity   Default: 2

logs at or above this threshold go to stderr

--token string

Bearer token for authentication to the API server

--user string

The name of the kubeconfig user to use

-v, --v Level

log level for V logs

--version version[=true]

Print version information and quit

--vmodule moduleSpec

comma-separated list of pattern=N settings for file-filtered logging

SEE ALSO

- kubectl alpha - Commands for features in alpha
- kubectl annotate - Update the annotations on a resource
- kubectl api-resources - Print the supported API resources on the server
- kubectl api-versions - Print the supported API versions on the server, in the form of "group/version"
- kubectl apply - Apply a configuration to a resource by filename or stdin
- kubectl attach - Attach to a running container
- kubectl auth - Inspect authorization
- kubectl autoscale - Auto-scale a Deployment, ReplicaSet, or Replication-Controller
- kubectl certificate - Modify certificate resources.
- kubectl cluster-info - Display cluster info
- kubectl completion - Output shell completion code for the specified shell (bash or zsh)
- kubectl config - Modify kubeconfig files
- kubectl convert - Convert config files between different API versions

- kubectl cordon - Mark node as unschedulable
- kubectl cp - Copy files and directories to and from containers.
- kubectl create - Create a resource from a file or from stdin.
- kubectl delete - Delete resources by filenames, stdin, resources and names, or by resources and label selector
- kubectl describe - Show details of a specific resource or group of resources
- kubectl drain - Drain node in preparation for maintenance
- kubectl edit - Edit a resource on the server
- kubectl exec - Execute a command in a container
- kubectl explain - Documentation of resources
- kubectl expose - Take a replication controller, service, deployment or pod and expose it as a new Kubernetes Service
- kubectl get - Display one or many resources
- kubectl label - Update the labels on a resource
- kubectl logs - Print the logs for a container in a pod
- kubectl options - Print the list of flags inherited by all commands
- kubectl patch - Update field(s) of a resource using strategic merge patch
- kubectl plugin - Provides utilities for interacting with plugins.
- kubectl port-forward - Forward one or more local ports to a pod
- kubectl proxy - Run a proxy to the Kubernetes API server
- kubectl replace - Replace a resource by filename or stdin
- kubectl rollout - Manage the rollout of a resource
- kubectl run - Run a particular image on the cluster
- kubectl scale - Set a new size for a Deployment, ReplicaSet, Replication Controller, or Job
- kubectl set - Set specific features on objects
- kubectl taint - Update the taints on one or more nodes
- kubectl top - Display Resource (CPU/Memory/Storage) usage.
- kubectl uncordon - Mark node as schedulable
- kubectl version - Print the client and server version information
- kubectl wait - Experimental: Wait for a specific condition on one or many resources.

Edit This Page

Overview of kubectl

Kubectl is a command line interface for running commands against Kubernetes clusters. This overview covers `kubectl` syntax, describes the command operations, and provides common examples. For details about each command, including all the supported flags and subcommands, see the kubectl reference documentation. For installation instructions see installing kubectl.

- Syntax
- Operations

- Resource types
- Output options
- Examples: Common operations
- Examples: Creating and using plugins
- What's next

Syntax

Use the following syntax to run `kubectl` commands from your terminal window:

`kubectl [command] [TYPE] [NAME] [flags]`

where `command`, `TYPE`, `NAME`, and `flags` are:

- `command`: Specifies the operation that you want to perform on one or more resources, for example `create`, `get`, `describe`, `delete`.

- `TYPE`: Specifies the resource type. Resource types are case-insensitive and you can specify the singular, plural, or abbreviated forms. For example, the following commands produce the same output:

  ```
  $ kubectl get pod pod1
  $ kubectl get pods pod1
  $ kubectl get po pod1
  ```

- `NAME`: Specifies the name of the resource. Names are case-sensitive. If the name is omitted, details for all resources are displayed, for example `$ kubectl get pods`.

When performing an operation on multiple resources, you can specify each resource by type and name or specify one or more files:

- To specify resources by type and name:

  - To group resources if they are all the same type: `TYPE1 name1 name2 name<#>`.
    Example: `$ kubectl get pod example-pod1 example-pod2`

  - To specify multiple resource types individually: `TYPE1/name1 TYPE1/name2 TYPE2/name3 TYPE<#>/name<#>`.
    Example: `$ kubectl get pod/example-pod1 replicationcontroller/example-rc1`

- To specify resources with one or more files: `-f file1 -f file2 -f file<#>`

  - Use YAML rather than JSON since YAML tends to be more user-friendly, especially for configuration files.
    Example: `$ kubectl get pod -f ./pod.yaml`

- `flags`: Specifies optional flags. For example, you can use the `-s` or `--server` flags to specify the address and port of the Kubernetes API

1285

server.

> **Caution:** Flags that you specify from the command line override
> default values and any corresponding environment variables.

If you need help, just run `kubectl help` from the terminal window.

Operations

The following table includes short descriptions and the general syntax for all of
the `kubectl` operations:

Operation	Syntax
annotate	`kubectl annotate (-f FILENAME | TYPE NAME | TYPE/NAME) KEY_1=VAL_1 ... KE`
api-versions	`kubectl api-versions [flags]`
apply	`kubectl apply -f FILENAME [flags]`
attach	`kubectl attach POD -c CONTAINER [-i] [-t] [flags]`
autoscale	`kubectl autoscale (-f FILENAME | TYPE NAME | TYPE/NAME) [--min=MINPODS] -`
cluster-info	`kubectl cluster-info [flags]`
config	`kubectl config SUBCOMMAND [flags]`
create	`kubectl create -f FILENAME [flags]`
delete	`kubectl delete (-f FILENAME | TYPE [NAME | /NAME | -l label | --all]) [`
describe	`kubectl describe (-f FILENAME | TYPE [NAME_PREFIX | /NAME | -l label]) [`
edit	`kubectl edit (-f FILENAME | TYPE NAME | TYPE/NAME) [flags]`
exec	`kubectl exec POD [-c CONTAINER] [-i] [-t] [flags] [-- COMMAND [args...]]`
explain	`kubectl explain [--include-extended-apis=true] [--recursive=false] [flags]`
expose	`kubectl expose (-f FILENAME | TYPE NAME | TYPE/NAME) [--port=port] [--pro`
get	`kubectl get (-f FILENAME | TYPE [NAME | /NAME | -l label]) [--watch] [--`
label	`kubectl label (-f FILENAME | TYPE NAME | TYPE/NAME) KEY_1=VAL_1 ... KEY_N`
logs	`kubectl logs POD [-c CONTAINER] [--follow] [flags]`
patch	`kubectl patch (-f FILENAME | TYPE NAME | TYPE/NAME) --patch PATCH [flags]`
port-forward	`kubectl port-forward POD [LOCAL_PORT:]REMOTE_PORT [...[LOCAL_PORT_N:]REMOTE`
proxy	`kubectl proxy [--port=PORT] [--www=static-dir] [--www-prefix=prefix] [--api`
replace	`kubectl replace -f FILENAME`
rolling-update	`kubectl rolling-update OLD_CONTROLLER_NAME ([NEW_CONTROLLER_NAME] --image=N`
run	`kubectl run NAME --image=image [--env="key=value"] [--port=port] [--replica`
scale	`kubectl scale (-f FILENAME | TYPE NAME | TYPE/NAME) --replicas=COUNT [--r`
stop	`kubectl stop`
version	`kubectl version [--client] [flags]`

Remember: For more about command operations, see the kubectl reference
documentation.

Resource types

The following table includes a list of all the supported resource types and their abbreviated aliases:

Resource type	Abbreviated alias
apiservices	
certificatesigningrequests	csr
clusters	
clusterrolebindings	
clusterroles	
componentstatuses	cs
configmaps	cm
controllerrevisions	
cronjobs	
customresourcedefinition	crd
daemonsets	ds
deployments	deploy
endpoints	ep
events	ev
horizontalpodautoscalers	hpa
ingresses	ing
jobs	
limitranges	limits
namespaces	ns
networkpolicies	netpol
nodes	no
persistentvolumeclaims	pvc
persistentvolumes	pv
poddisruptionbudget	pdb
podpreset	
pods	po
podsecuritypolicies	psp
podtemplates	
replicasets	rs
replicationcontrollers	rc
resourcequotas	quota
rolebindings	
roles	
secrets	
serviceaccounts	sa
services	svc
statefulsets	
storageclasses	

Output options

Use the following sections for information about how you can format or sort the output of certain commands. For details about which commands support the various output options, see the kubectl reference documentation.

Formatting output

The default output format for all `kubectl` commands is the human readable plain-text format. To output details to your terminal window in a specific format, you can add either the `-o` or `--output` flags to a supported `kubectl` command.

Syntax

`kubectl [command] [TYPE] [NAME] -o=<output_format>`

Depending on the `kubectl` operation, the following output formats are supported:

Output format	Description
`-o=custom-columns=<spec>`	Print a table using a comma separated list of custom columns.
`-o=custom-columns-file=<filename>`	Print a table using the custom columns template in the `<filename`
`-o=json`	Output a JSON formatted API object.
`-o=jsonpath=<template>`	Print the fields defined in a jsonpath expression.
`-o=jsonpath-file=<filename>`	Print the fields defined by the jsonpath expression in the `<filenam`
`-o=name`	Print only the resource name and nothing else.
`-o=wide`	Output in the plain-text format with any additional information. F
`-o=yaml`	Output a YAML formatted API object.

Example

In this example, the following command outputs the details for a single pod as a YAML formatted object:

`$ kubectl get pod web-pod-13je7 -o=yaml`

Remember: See the kubectl reference documentation for details about which output format is supported by each command.

Custom columns

To define custom columns and output only the details that you want into a table, you can use the `custom-columns` option. You can choose to define the

custom columns inline or use a template file: `-o=custom-columns=<spec>` or
`-o=custom-columns-file=<filename>`.

Examples

Inline:

```
$ kubectl get pods <pod-name> -o=custom-columns=NAME:.metadata.name,RSRC:.metadata.resourceV
```

Template file:

```
$ kubectl get pods <pod-name> -o=custom-columns-file=template.txt
```

where the `template.txt` file contains:

```
NAME            RSRC
metadata.name metadata.resourceVersion
```

The result of running either command is:

```
NAME            RSRC
submit-queue    610995
```

Server-side columns

`kubectl` supports receiving specific column information from the server about
objects. This means that for any given resource, the server will return columns
and rows relevant to that resource, for the client to print. This allows for
consistent human-readable output across clients used against the same cluster,
by having the server encapsulate the details of printing.

This feature is enabled by default in `kubectl` 1.11 and higher. To disable it,
add the `--server-print=false` flag to the `kubectl get` command.

Examples

To print information about the status of a pod, use a command like the following:

```
kubectl get pods <pod-name> --server-print=false
```

Output looks like this:

```
NAME        READY     STATUS        RESTARTS    AGE
pod-name    1/1       Running       0           1m
```

Sorting list objects

To output objects to a sorted list in your terminal window, you can add the
`--sort-by` flag to a supported `kubectl` command. Sort your objects by spec-

1289

ifying any numeric or string field with the `--sort-by` flag. To specify a field,
use a jsonpath expression.

Syntax

```
kubectl [command] [TYPE] [NAME] --sort-by=<jsonpath_exp>
```

Example

To print a list of pods sorted by name, you run:

```
$ kubectl get pods --sort-by=.metadata.name
```

Examples: Common operations

Use the following set of examples to help you familiarize yourself with running
the commonly used `kubectl` operations:

`kubectl create` - Create a resource from a file or stdin.

```
// Create a service using the definition in example-service.yaml.
$ kubectl create -f example-service.yaml
```

```
// Create a replication controller using the definition in example-controller.yaml.
$ kubectl create -f example-controller.yaml
```

```
// Create the objects that are defined in any .yaml, .yml, or .json file within the <directo
$ kubectl create -f <directory>
```

`kubectl get` - List one or more resources.

```
// List all pods in plain-text output format.
$ kubectl get pods
```

```
// List all pods in plain-text output format and includes additional information (such as no
$ kubectl get pods -o wide
```

```
// List the replication controller with the specified name in plain-text output format. Tip:
$ kubectl get replicationcontroller <rc-name>
```

```
// List all replication controllers and services together in plain-text output format.
$ kubectl get rc,services
```

```
// List all daemon sets, including uninitialized ones, in plain-text output format.
$ kubectl get ds --include-uninitialized
```

```
// List all pods running on node server01
```

```
$ kubectl get pods --field-selector=spec.nodeName=server01

// List all pods in plain-text output format, delegating the details of printing to the serv
$ kubectl get pods --experimental-server-print
```

kubectl describe - Display detailed state of one or more resources, including
the uninitialized ones by default.

```
// Display the details of the node with name <node-name>.
$ kubectl describe nodes <node-name>

// Display the details of the pod with name <pod-name>.
$ kubectl describe pods/<pod-name>

// Display the details of all the pods that are managed by the replication controller named
// Remember: Any pods that are created by the replication controller get prefixed with the r
$ kubectl describe pods <rc-name>

// Describe all pods, not including uninitialized ones
$ kubectl describe pods --include-uninitialized=false
```

> **Note:** The kubectl get command is usually used for retrieving one
> or more resources of the same resource type. It features a rich set
> of flags that allows you to customize the output format using the -o
> or --output flag, for example. You can specify the -w or --watch
> flag to start watching updates to a particular object. The kubectl
> describe command is more focused on describing the many related
> aspects of a specified resource. It may invoke several API calls to the
> API server to build a view for the user. For example, the kubectl
> describe node command retrieves not only the information about
> the node, but also a summary of the pods running on it, the events
> generated for the node etc.

kubectl delete - Delete resources either from a file, stdin, or specifying label
selectors, names, resource selectors, or resources.

```
// Delete a pod using the type and name specified in the pod.yaml file.
$ kubectl delete -f pod.yaml

// Delete all the pods and services that have the label name=<label-name>.
$ kubectl delete pods,services -l name=<label-name>

// Delete all the pods and services that have the label name=<label-name>, including uniniti
$ kubectl delete pods,services -l name=<label-name> --include-uninitialized

// Delete all pods, including uninitialized ones.
$ kubectl delete pods --all
```

kubectl exec - Execute a command against a container in a pod.

```
// Get output from running 'date' from pod <pod-name>. By default, output is from the first
$ kubectl exec <pod-name> date

// Get output from running 'date' in container <container-name> of pod <pod-name>.
$ kubectl exec <pod-name> -c <container-name> date

// Get an interactive TTY and run /bin/bash from pod <pod-name>. By default, output is from
$ kubectl exec -ti <pod-name> /bin/bash
```

kubectl logs - Print the logs for a container in a pod.

```
// Return a snapshot of the logs from pod <pod-name>.
$ kubectl logs <pod-name>

// Start streaming the logs from pod <pod-name>. This is similar to the 'tail -f' Linux comm
$ kubectl logs -f <pod-name>
```

Examples: Creating and using plugins

Use the following set of examples to help you familiarize yourself with writing
and using kubectl plugins:

```
// create a simple plugin in any language and name the resulting executable file
// so that it begins with the prefix "kubectl-"
$ cat ./kubectl-hello
#!/bin/bash

# this plugin prints the words "hello world"
echo "hello world"

// with our plugin written, let's make it executable
$ sudo chmod +x ./kubectl-hello

// and move it to a location in our PATH
$ sudo mv ./kubectl-hello /usr/local/bin

// we have now created and "installed" a kubectl plugin.
// we can begin using our plugin by invoking it from kubectl as if it were a regular command
$ kubectl hello
hello world

// we can "uninstall" a plugin, by simply removing it from our PATH
$ sudo rm /usr/local/bin/kubectl-hello
```

In order to view all of the plugins that are available to kubectl, we can use the
kubectl plugin list subcommand:

```
$ kubectl plugin list
The following kubectl-compatible plugins are available:

/usr/local/bin/kubectl-hello
/usr/local/bin/kubectl-foo
/usr/local/bin/kubectl-bar

// this command can also warn us about plugins that are
// not executable, or that are overshadowed by other
// plugins, for example
$ sudo chmod -x /usr/local/bin/kubectl-foo
$ kubectl plugin list
The following kubectl-compatible plugins are available:

/usr/local/bin/kubectl-hello
/usr/local/bin/kubectl-foo
  - warning: /usr/local/bin/kubectl-foo identified as a plugin, but it is not executable
/usr/local/bin/kubectl-bar

error: one plugin warning was found
```

We can think of plugins as a means to build more complex functionality on top
of the existing kubectl commands:

```
$ cat ./kubectl-whoami
#!/bin/bash

# this plugin makes use of the `kubectl config` command in order to output
# information about the current user, based on the currently selected context
kubectl config view --template='{{ range .contexts }}{{ if eq .name "'$(kubectl config curre
```

Running the above plugin gives us an output containing the user for the currently
selected context in our KUBECONFIG file:

```
// make the file executable
$ sudo chmod +x ./kubectl-whoami

// and move it into our PATH
$ sudo mv ./kubectl-whoami /usr/local/bin

$ kubectl whoami
Current user: plugins-user
```

To find out more about plugins, take a look at the example cli plugin.

What's next

Start using the kubectl commands.

Edit This Page

JSONPath Support

JSONPath template is composed of JSONPath expressions enclosed by {}. And we add three functions in addition to the original JSONPath syntax:

1. The `$` operator is optional since the expression always starts from the root object by default.
2. We can use `""` to quote text inside JSONPath expressions.
3. We can use `range` operator to iterate lists.
4. We can use negative slice indices to step backwards through a list. Negative indices do not "wrap around" a list. They are valid as long as `-index + listLength >= 0`.

The result object is printed as its String() function.

Given the input:

```
{
  "kind": "List",
  "items":[
    {
      "kind":"None",
      "metadata":{"name":"127.0.0.1"},
      "status":{
        "capacity":{"cpu":"4"},
        "addresses":[{"type": "LegacyHostIP", "address":"127.0.0.1"}]
      }
    },
    {
      "kind":"None",
      "metadata":{"name":"127.0.0.2"},
      "status":{
        "capacity":{"cpu":"8"},
        "addresses":[
          {"type": "LegacyHostIP", "address":"127.0.0.2"},
          {"type": "another", "address":"127.0.0.3"}
        ]
      }
    }
  ],
```

```
  "users":[
    {
      "name": "myself",
      "user": {}
    },
    {
      "name": "e2e",
      "user": {"username": "admin", "password": "secret"}
    }
  ]
}
```

Function	Description	Example
text	the plain text	kind is {.kind}
@	the current object	{@}
. or []	child operator	{.kind} or {['kind']}
..	recursive descent	{..name}
	wildcard. Get all objects	{.items[*].metadata.name}
[start:end :step]	subscript operator	{.users[0].name}
[,]	union operator	{.items[*]['metadata.name', 'status.capacity']}
?()	filter	{.users[?(@.name=="e2e")].user.password}
range, end	iterate list	{range .items[*]}[{.metadata.name}, {.status.capacity}] {end}
"	quote interpreted string	{range .items[*]}{.metadata.name}{'\t'}{end}

Below are some examples using jsonpath:

```
$ kubectl get pods -o json
$ kubectl get pods -o=jsonpath='{@}'
$ kubectl get pods -o=jsonpath='{.items[0]}'
$ kubectl get pods -o=jsonpath='{.items[0].metadata.name}'
$ kubectl get pods -o=jsonpath='{range .items[*]}{.metadata.name}{"\t"}{.status.startTime}{'
```

On Windows, you must *double* quote any JSONPath template that contains
spaces (not single quote as shown above for bash). This in turn means that
you must use a single quote or escaped double quote around any literals in the
template. For example:

```
C:\> kubectl get pods -o=jsonpath="{range .items[*]}{.metadata.name}{'\t'}{.status.startTime
C:\> kubectl get pods -o=jsonpath="{range .items[*]}{.metadata.name}{\"\t\"}{.status.startTi
```

Edit This Page

- – kubectl
    * Synopsis
    * Options
    * SEE ALSO

kubectl

kubectl controls the Kubernetes cluster manager

Synopsis

kubectl controls the Kubernetes cluster manager.

Find more information at: https://kubernetes.io/docs/reference/kubectl/overview/

```
kubectl [flags]
```

Options

--allow-verification-with-non-compliant-keys

Allow a SignatureVerifier to use keys which are technically non-compliant with RFC6962.

--alsologtostderr

log to standard error as well as files

--as string

Username to impersonate for the operation

--as-group stringArray

Group to impersonate for the operation, this flag can be repeated to specify multiple groups.

--azure-container-registry-config string

Path to the file containing Azure container registry configuration information.

--cache-dir string   Default: "/Users/zarnold/.kube/http-cache"

Default HTTP cache directory

--certificate-authority string

Path to a cert file for the certificate authority

--client-certificate string

Path to a client certificate file for TLS

--client-key string

Path to a client key file for TLS

--cloud-provider-gce-lb-src-cidrs cidrs   Default: 130.211.0.0/22,209.85.152.0/22,209.85.204.0/22,35.191.0.0/16

CIDRs opened in GCE firewall for LB traffic proxy & health checks

--cluster string

The name of the kubeconfig cluster to use

--context string

The name of the kubeconfig context to use

--default-not-ready-toleration-seconds int   Default: 300

Indicates the tolerationSeconds of the toleration for notReady:NoExecute that is added by default to every pod that does not already have such a toleration.

--default-unreachable-toleration-seconds int   Default: 300

Indicates the tolerationSeconds of the toleration for unreachable:NoExecute that is added by default to every pod that does not already have such a toleration.

-h, --help

help for kubectl

--insecure-skip-tls-verify

If true, the server's certificate will not be checked for validity. This will make your HTTPS connections insecure

--kubeconfig string

Path to the kubeconfig file to use for CLI requests.

--log-backtrace-at traceLocation   Default: :0

when logging hits line file:N, emit a stack trace

--log-dir string

If non-empty, write log files in this directory

--log-flush-frequency duration   Default: 5s

Maximum number of seconds between log flushes

--logtostderr   Default: true

log to standard error instead of files

--match-server-version

Require server version to match client version

-n, --namespace string

If present, the namespace scope for this CLI request

--request-timeout string   Default: "0"

The length of time to wait before giving up on a single server request. Non-zero values should contain a corresponding time unit (e.g. 1s, 2m, 3h). A value of zero means don't timeout requests.

-s, --server string

The address and port of the Kubernetes API server

--stderrthreshold severity   Default: 2

logs at or above this threshold go to stderr

--token string

Bearer token for authentication to the API server

--user string

The name of the kubeconfig user to use

-v, --v Level

log level for V logs

--version version[=true]

Print version information and quit

--vmodule moduleSpec

comma-separated list of pattern=N settings for file-filtered logging

SEE ALSO

- kubectl alpha - Commands for features in alpha
- kubectl annotate - Update the annotations on a resource
- kubectl api-resources - Print the supported API resources on the server
- kubectl api-versions - Print the supported API versions on the server, in the form of "group/version"
- kubectl apply - Apply a configuration to a resource by filename or stdin
- kubectl attach - Attach to a running container
- kubectl auth - Inspect authorization
- kubectl autoscale - Auto-scale a Deployment, ReplicaSet, or Replication-Controller
- kubectl certificate - Modify certificate resources.
- kubectl cluster-info - Display cluster info
- kubectl completion - Output shell completion code for the specified shell (bash or zsh)
- kubectl config - Modify kubeconfig files
- kubectl convert - Convert config files between different API versions
- kubectl cordon - Mark node as unschedulable
- kubectl cp - Copy files and directories to and from containers.

- kubectl create - Create a resource from a file or from stdin.
- kubectl delete - Delete resources by filenames, stdin, resources and names, or by resources and label selector
- kubectl describe - Show details of a specific resource or group of resources
- kubectl drain - Drain node in preparation for maintenance
- kubectl edit - Edit a resource on the server
- kubectl exec - Execute a command in a container
- kubectl explain - Documentation of resources
- kubectl expose - Take a replication controller, service, deployment or pod and expose it as a new Kubernetes Service
- kubectl get - Display one or many resources
- kubectl label - Update the labels on a resource
- kubectl logs - Print the logs for a container in a pod
- kubectl options - Print the list of flags inherited by all commands
- kubectl patch - Update field(s) of a resource using strategic merge patch
- kubectl plugin - Provides utilities for interacting with plugins.
- kubectl port-forward - Forward one or more local ports to a pod
- kubectl proxy - Run a proxy to the Kubernetes API server
- kubectl replace - Replace a resource by filename or stdin
- kubectl rollout - Manage the rollout of a resource
- kubectl run - Run a particular image on the cluster
- kubectl scale - Set a new size for a Deployment, ReplicaSet, Replication Controller, or Job
- kubectl set - Set specific features on objects
- kubectl taint - Update the taints on one or more nodes
- kubectl top - Display Resource (CPU/Memory/Storage) usage.
- kubectl uncordon - Mark node as schedulable
- kubectl version - Print the client and server version information
- kubectl wait - Experimental: Wait for a specific condition on one or many resources.

Edit This Page

kubectl Cheat Sheet

See also: Kubectl Overview and JsonPath Guide.

This page is an overview of the `kubectl` command.

- Kubectl Autocomplete
- Kubectl Context and Configuration
- Creating Objects
- Viewing, Finding Resources
- Updating Resources
- Patching Resources

kubectl - Cheat Sheet

Kubectl Autocomplete

BASH

```
source <(kubectl completion bash) # setup autocomplete in bash into the current shell, bash-
echo "source <(kubectl completion bash)" >> ~/.bashrc # add autocomplete permanently to your
```

ZSH

```
source <(kubectl completion zsh)  # setup autocomplete in zsh into the current shell
echo "if [ $commands[kubectl] ]; then source <(kubectl completion zsh); fi" >> ~/.zshrc # ad
```

Kubectl Context and Configuration

Set which Kubernetes cluster `kubectl` communicates with and modifies configuration information. See Authenticating Across Clusters with kubeconfig documentation for detailed config file information.

```
kubectl config view # Show Merged kubeconfig settings.

# use multiple kubeconfig files at the same time and view merged config
KUBECONFIG=~/.kube/config:~/.kube/kubconfig2 kubectl config view

# Get the password for the e2e user
kubectl config view -o jsonpath='{.users[?(@.name == "e2e")].user.password}'

kubectl config current-context                # Display the current-context
kubectl config use-context my-cluster-name  # set the default context to my-cluster-name

# add a new cluster to your kubeconf that supports basic auth
kubectl config set-credentials kubeuser/foo.kubernetes.com --username=kubeuser --password=ku

# set a context utilizing a specific username and namespace.
kubectl config set-context gce --user=cluster-admin --namespace=foo \
```

```
   && kubectl config use-context gce
```

Creating Objects

Kubernetes manifests can be defined in json or yaml. The file extension `.yaml`, `.yml`, and `.json` can be used.

```
kubectl create -f ./my-manifest.yaml            # create resource(s)
kubectl create -f ./my1.yaml -f ./my2.yaml      # create from multiple files
kubectl create -f ./dir                         # create resource(s) in all manifest files in
kubectl create -f https://git.io/vPieo          # create resource(s) from url
kubectl run nginx --image=nginx                 # start a single instance of nginx
kubectl explain pods,svc                        # get the documentation for pod and svc manif

# Create multiple YAML objects from stdin
cat <<EOF | kubectl create -f -
apiVersion: v1
kind: Pod
metadata:
  name: busybox-sleep
spec:
  containers:
  - name: busybox
    image: busybox
    args:
    - sleep
    - "1000000"
---
apiVersion: v1
kind: Pod
metadata:
  name: busybox-sleep-less
spec:
  containers:
  - name: busybox
    image: busybox
    args:
    - sleep
    - "1000"
EOF

# Create a secret with several keys
cat <<EOF | kubectl create -f -
apiVersion: v1
kind: Secret
```

```
metadata:
  name: mysecret
type: Opaque
data:
  password: $(echo -n "s33msi4" | base64 -w0)
  username: $(echo -n "jane" | base64 -w0)
EOF
```

Viewing, Finding Resources

```
# Get commands with basic output
kubectl get services                      # List all services in the namespace
kubectl get pods --all-namespaces         # List all pods in all namespaces
kubectl get pods -o wide                  # List all pods in the namespace, with more de
kubectl get deployment my-dep             # List a particular deployment
kubectl get pods --include-uninitialized  # List all pods in the namespace, including ur

# Describe commands with verbose output
kubectl describe nodes my-node
kubectl describe pods my-pod

kubectl get services --sort-by=.metadata.name # List Services Sorted by Name

# List pods Sorted by Restart Count
kubectl get pods --sort-by='.status.containerStatuses[0].restartCount'

# Get the version label of all pods with label app=cassandra
kubectl get pods --selector=app=cassandra rc -o \
  jsonpath='{.items[*].metadata.labels.version}'

# Get all running pods in the namespace
kubectl get pods --field-selector=status.phase=Running

# Get ExternalIPs of all nodes
kubectl get nodes -o jsonpath='{.items[*].status.addresses[?(@.type=="ExternalIP")].address]

# List Names of Pods that belong to Particular RC
# "jq" command useful for transformations that are too complex for jsonpath, it can be found
sel=${$(kubectl get rc my-rc --output=json | jq -j '.spec.selector | to_entries | .[] | "\(.
echo $(kubectl get pods --selector=$sel --output=jsonpath={.items..metadata.name})

# Check which nodes are ready
JSONPATH='{range .items[*]}{@.metadata.name}:{range @.status.conditions[*]}{@.type}={@.statu
 && kubectl get nodes -o jsonpath="$JSONPATH" | grep "Ready=True"
```

```
# List all Secrets currently in use by a pod
kubectl get pods -o json | jq '.items[].spec.containers[].env[]?.valueFrom.secretKeyRef.name

# List Events sorted by timestamp
kubectl get events --sort-by=.metadata.creationTimestamp
```

Updating Resources

```
kubectl rolling-update frontend-v1 -f frontend-v2.json          # Rolling update pods of fr
kubectl rolling-update frontend-v1 frontend-v2 --image=image:v2  # Change the name of the re
kubectl rolling-update frontend --image=image:v2                 # Update the pods image of
kubectl rolling-update frontend-v1 frontend-v2 --rollback        # Abort existing rollout in
cat pod.json | kubectl replace -f -                              # Replace a pod based on th

# Force replace, delete and then re-create the resource. Will cause a service outage.
kubectl replace --force -f ./pod.json

# Create a service for a replicated nginx, which serves on port 80 and connects to the conta
kubectl expose rc nginx --port=80 --target-port=8000

# Update a single-container pod's image version (tag) to v4
kubectl get pod mypod -o yaml | sed 's/\(image: myimage\):.*$/\1:v4/' | kubectl replace -f -

kubectl label pods my-pod new-label=awesome                # Add a Label
kubectl annotate pods my-pod icon-url=http://goo.gl/XXBTWq # Add an annotation
kubectl autoscale deployment foo --min=2 --max=10          # Auto scale a deployment '
```

Patching Resources

```
kubectl patch node k8s-node-1 -p '{"spec":{"unschedulable":true}}' # Partially update a node

# Update a container's image; spec.containers[*].name is required because it's a merge key
kubectl patch pod valid-pod -p '{"spec":{"containers":[{"name":"kubernetes-serve-hostname",'

# Update a container's image using a json patch with positional arrays
kubectl patch pod valid-pod --type='json' -p='[{"op": "replace", "path": "/spec/containers/0

# Disable a deployment livenessProbe using a json patch with positional arrays
kubectl patch deployment valid-deployment  --type json   -p='[{"op": "remove", "path": "/spe

# Add a new element to a positional array
kubectl patch sa default --type='json' -p='[{"op": "add", "path": "/secrets/1", "value": {"n
```

Editing Resources

The edit any API resource in an editor.

```
kubectl edit svc/docker-registry                     # Edit the service named docker-regist
KUBE_EDITOR="nano" kubectl edit svc/docker-registry   # Use an alternative editor
```

Scaling Resources

```
kubectl scale --replicas=3 rs/foo                                   # Scale a replicaset named
kubectl scale --replicas=3 -f foo.yaml                              # Scale a resource specifi
kubectl scale --current-replicas=2 --replicas=3 deployment/mysql    # If the deployment named
kubectl scale --replicas=5 rc/foo rc/bar rc/baz                     # Scale multiple replicati
```

Deleting Resources

```
kubectl delete -f ./pod.json                                       # Delete a pod usi
kubectl delete pod,service baz foo                                 # Delete pods and
kubectl delete pods,services -l name=myLabel                       # Delete pods and
kubectl delete pods,services -l name=myLabel --include-uninitialized   # Delete pods and
kubectl -n my-ns delete po,svc --all                               # Delete all pods
```

Interacting with running Pods

```
kubectl logs my-pod                                # dump pod logs (stdout)
kubectl logs my-pod --previous                     # dump pod logs (stdout) for a previous
kubectl logs my-pod -c my-container                # dump pod container logs (stdout, multi
kubectl logs my-pod -c my-container --previous      # dump pod container logs (stdout, multi
kubectl logs -f my-pod                             # stream pod logs (stdout)
kubectl logs -f my-pod -c my-container             # stream pod container logs (stdout, mul
kubectl run -i --tty busybox --image=busybox -- sh # Run pod as interactive shell
kubectl attach my-pod -i                           # Attach to Running Container
kubectl port-forward my-pod 5000:6000              # Listen on port 5000 on the local machi
kubectl exec my-pod -- ls /                        # Run command in existing pod (1 contain
kubectl exec my-pod -c my-container -- ls /        # Run command in existing pod (multi-con
kubectl top pod POD_NAME --containers              # Show metrics for a given pod and its c
```

Interacting with Nodes and Cluster

```
kubectl cordon my-node                                           # Mark my-node as unsc
kubectl drain my-node                                            # Drain my-node in pre
kubectl uncordon my-node                                         # Mark my-node as sche
kubectl top node my-node                                         # Show metrics for a g
```

1304

```
kubectl cluster-info                                          # Display addresses of
kubectl cluster-info dump                                     # Dump current cluster
kubectl cluster-info dump --output-directory=/path/to/cluster-state  # Dump current cluster

# If a taint with that key and effect already exists, its value is replaced as specified.
kubectl taint nodes foo dedicated=special-user:NoSchedule
```

Resource types

List all supported resource types along with their shortnames, API group,
whether they are namespaced, and Kind:

```
kubectl api-resources
```

Other operations for exploring API resources:

```
kubectl api-resources --namespaced=true        # All namespaced resources
kubectl api-resources --namespaced=false       # All non-namespaced resources
kubectl api-resources -o name                  # All resources with simple output (just the re
kubectl api-resources -o wide                  # All resources with expanded (aka "wide") outp
kubectl api-resources --verbs=list,get         # All resources that support the "list" and "ge
kubectl api-resources --api-group=extensions   # All resources in the "extensions" API group
```

Formatting output

To output details to your terminal window in a specific format, you can add
either the `-o` or `--output` flags to a supported `kubectl` command.

Output format	Description
`-o=custom-columns=<spec>`	Print a table using a comma separated list of custom columns
`-o=custom-columns-file=<filename>`	Print a table using the custom columns template in the `<filename`
`-o=json`	Output a JSON formatted API object
`-o=jsonpath=<template>`	Print the fields defined in a jsonpath expression
`-o=jsonpath-file=<filename>`	Print the fields defined by the jsonpath expression in the `<filenam`
`-o=name`	Print only the resource name and nothing else
`-o=wide`	Output in the plain-text format with any additional information, a
`-o=yaml`	Output a YAML formatted API object

Kubectl output verbosity and debugging

Kubectl verbosity is controlled with the `-v` or `--v` flags followed by an integer
representing the log level. General Kubernetes logging conventions and the
associated log levels are described here.

Verbosity	Description
`--v=0`	Generally useful for this to ALWAYS be visible to an operator.
`--v=1`	A reasonable default log level if you don't want verbosity.
`--v=2`	Useful steady state information about the service and important log messages that may correlate
`--v=3`	Extended information about changes.
`--v=4`	Debug level verbosity.
`--v=6`	Display requested resources.
`--v=7`	Display HTTP request headers.
`--v=8`	Display HTTP request contents.
`--v=9`	Display HTTP request contents without truncation of contents.

What's next

- Learn more about Overview of kubectl.

- See kubectl options.

- Also kubectl Usage Conventions to understand how to use it in reusable scripts.

- See more community kubectl cheatsheets.

Edit This Page

kubectl Commands

kubectl Command Reference

Edit This Page

kubectl Usage Conventions

Recommended usage conventions for `kubectl`.

- Using `kubectl` in Reusable Scripts
- Best Practices

Using `kubectl` in Reusable Scripts

For a stable output in a script:

- Request one of the machine-oriented output forms, such as `-o name`, `-o json`, `-o yaml`, `-o go-template`, or `-o jsonpath`.

1306

- Fully-qualify the version. For example, `jobs.v1.batch/myjob`. This will ensure that kubectl does not use its default version that can change over time.
- Specify the `--generator` flag to pin to a specific behavior when you use generator-based commands such as `kubectl run` or `kubectl expose`.
- Don't rely on context, preferences, or other implicit states.

Best Practices

`kubectl run`

For `kubectl run` to satisfy infrastructure as code:

- Tag the image with a version-specific tag and don't move that tag to a new version. For example, use `:v1234`, `v1.2.3`, `r03062016-1-4`, rather than `:latest` (For more information, see Best Practices for Configuration).
- Capture the parameters in a checked-in script, or at least use `--record` to annotate the created objects with the command line for an image that is lightly parameterized.
- Check in the script for an image that is heavily parameterized.
- Switch to configuration files checked into source control for features that are needed, but not expressible via `kubectl run` flags.
- Pin to a specific generator version, such as `kubectl run --generator=deployment/v1beta1`.

Generators

You can create the following resources using `kubectl run` with the `--generator` flag:

Resource	kubectl command
Pod	`kubectl run --generator=run-pod/v1`
Replication controller	`kubectl run --generator=run/v1`
Deployment	`kubectl run --generator=extensions/v1beta1`
-for an endpoint (default)	`kubectl run --generator=deployment/v1beta1`
Deployment	`kubectl run --generator=apps/v1beta1`
-for an endpoint (recommended)	`kubectl run --generator=deployment/apps.v1beta1`
Job	`kubectl run --generator=job/v1`
CronJob	`kubectl run --generator=batch/v1beta1`
-for an endpoint (default)	`kubectl run --generator=cronjob/v1beta1`
CronJob	`kubectl run --generator=batch/v2alpha1`
-for an endpoint (deprecated)	`kubectl run --generator=cronjob/v2alpha1`

If you do not specify a generator flag, other flags prompt you to use a specific generator. The following table lists the flags that force you to use specific

1307

generators, depending on the version of the cluster:

Generated Resource	Cluster v1.4 and later	Cluster v1.3	Cluster v1.2
Pod	`--restart=Never`	`--restart=Never`	`--generator=run-pod/v1`
Replication Controller	`--generator=run/v1`	`--generator=run/v1`	`--generator=run/v1`
Deployment	`--restart=Always`	`--restart=Always`	`--restart=Always`
Job	`--restart=OnFailure`	`--restart=OnFailure`	`--restart=OnFailure` OR `--res`
Cron Job	`--schedule=<cron>`	N/A	N/A

> **Note:** These flags use a default generator only when you have not specified any flag. This means that when you combine `--generator` with other flags the generator that you specified later does not change. For example, in a cluster v1.4, if you initially specify `--restart=Always`, a Deployment is created; if you later specify `--restart=Always` and `--generator=run/v1`, a Replication Controller is created. This enables you to pin to a specific behavior with the generator, even when the default generator is changed later.

The flags set the generator in the following order: first the `--schedule` flag, then the `--restart` policy flag, and finally the `--generator` flag.

To check the final resource that was created, use the `--dry-run` flag, which provides the object to be submitted to the cluster.

kubectl apply

- You can use `kubectl apply` to create or update resources. However, to update a resource you should have created the resource by using `kubectl apply` or `kubectl create --save-config`. For more information about using kubectl apply to update resources, see Managing Resources.

Edit This Page

kubectl for Docker Users

You can use the Kubernetes command line tool kubectl to interact with the API Server. Using kubectl is straightforward if you are familiar with the Docker command line tool. However, there are a few differences between the docker commands and the kubectl commands. The following sections show a docker sub-command and describe the equivalent kubectl command.

- docker run
- docker ps
- docker attach

1308

- docker exec
- docker logs
- docker stop and docker rm
- docker login
- docker version
- docker info

docker run

To run an nginx Deployment and expose the Deployment, see kubectl run.

docker:

```
$ docker run -d --restart=always -e DOMAIN=cluster --name nginx-app -p 80:80 nginx
55c103fa129692154a7652490236fee9be47d70a8dd562281ae7d2f9a339a6db
```

```
$ docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS
55c103fa1296        nginx               "nginx -g 'daemon of…"   9 seconds ago       Up 9 se
```

kubectl:

```
# start the pod running nginx
$ kubectl run --image=nginx nginx-app --port=80 --env="DOMAIN=cluster"
deployment "nginx-app" created
```

> **Note:** kubectl commands print the type and name of the resource
> created or mutated, which can then be used in subsequent commands.
> You can expose a new Service after a Deployment is created.

```
# expose a port through with a service
$ kubectl expose deployment nginx-app --port=80 --name=nginx-http
service "nginx-http" exposed
```

By using kubectl, you can create a Deployment to ensure that N pods are running nginx, where N is the number of replicas stated in the spec and defaults to 1. You can also create a service with a selector that matches the pod labels. For more information, see Use a Service to Access an Application in a Cluster.

By default images run in the background, similar to `docker run -d ...`. To run things in the foreground, use:

```
kubectl run [-i] [--tty] --attach <name> --image=<image>
```

Unlike `docker run ...`, if you specify `--attach`, then you attach `stdin`, `stdout` and `stderr`. You cannot control which streams are attached (`docker -a ...`). To detach from the container, you can type the escape sequence Ctrl+P followed by Ctrl+Q.

1309

Because the kubectl run command starts a Deployment for the container, the Deployment restarts if you terminate the attached process by using Ctrl+C, unlike `docker run -it`. To destroy the Deployment and its pods you need to run `kubectl delete deployment <name>`.

docker ps

To list what is currently running, see kubectl get.

docker:

```
$ docker ps -a
CONTAINER ID        IMAGE             COMMAND              CREATED              STATUS
14636241935f        ubuntu:16.04      "echo test"          5 seconds ago        Exited
55c103fa1296        nginx             "nginx -g 'daemon of…"  About a minute ago  Up Abo
```

kubectl:

```
$ kubectl get po -a
NAME                        READY   STATUS      RESTARTS   AGE
nginx-app-8df569cb7-4gd89   1/1     Running     0          3m
ubuntu                      0/1     Completed   0          20s
```

docker attach

To attach a process that is already running in a container, see kubectl attach.

docker:

```
$ docker ps
CONTAINER ID        IMAGE             COMMAND              CREATED              STATUS
55c103fa1296        nginx             "nginx -g 'daemon of…"  5 minutes ago       Up 5 mi

$ docker attach 55c103fa1296
...
```

kubectl:

```
$ kubectl get pods
NAME               READY   STATUS    RESTARTS   AGE
nginx-app-5jyvm    1/1     Running   0          10m

$ kubectl attach -it nginx-app-5jyvm
...
```

To detach from the container, you can type the escape sequence Ctrl+P followed by Ctrl+Q.

docker exec

To execute a command in a container, see kubectl exec.

docker:

```
$ docker ps
CONTAINER ID        IMAGE              COMMAND                 CREATED         STATUS
55c103fa1296        nginx              "nginx -g 'daemon of…"  6 minutes ago   Up 6 mi

$ docker exec 55c103fa1296 cat /etc/hostname
55c103fa1296
```

kubectl:

```
$ kubectl get po
NAME              READY     STATUS    RESTARTS   AGE
nginx-app-5jyvm   1/1       Running   0          10m

$ kubectl exec nginx-app-5jyvm -- cat /etc/hostname
nginx-app-5jyvm
```

To use interactive commands.

docker:

```
$ docker exec -ti 55c103fa1296 /bin/sh
# exit
```

kubectl:

```
$ kubectl exec -ti nginx-app-5jyvm -- /bin/sh
# exit
```

For more information, see Get a Shell to a Running Container.

docker logs

To follow stdout/stderr of a process that is running, see kubectl logs.

docker:

```
$ docker logs -f a9e
192.168.9.1 - - [14/Jul/2015:01:04:02 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.35.0" "-"
192.168.9.1 - - [14/Jul/2015:01:04:03 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.35.0" "-"
```

kubectl:

```
$ kubectl logs -f nginx-app-zibvs
10.240.63.110 - - [14/Jul/2015:01:09:01 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.26.0" "-
10.240.63.110 - - [14/Jul/2015:01:09:02 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.26.0" "-
```

There is a slight difference between pods and containers; by default pods do not terminate if their processes exit. Instead the pods restart the process. This is similar to the docker run option `--restart=always` with one major difference. In docker, the output for each invocation of the process is concatenated, but for Kubernetes, each invocation is separate. To see the output from a previous run in Kubernetes, do this:

```
$ kubectl logs --previous nginx-app-zibvs
10.240.63.110 - - [14/Jul/2015:01:09:01 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.26.0" "-
10.240.63.110 - - [14/Jul/2015:01:09:02 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.26.0" "-
```

For more information, see Logging Architecture.

docker stop and docker rm

To stop and delete a running process, see kubectl delete.

docker:

```
$ docker ps
CONTAINER ID        IMAGE              COMMAND               CREATED        STATUS
a9ec34d98787        nginx              "nginx -g 'daemon of" 22 hours ago   Up 22 hou

$ docker stop a9ec34d98787
a9ec34d98787

$ docker rm a9ec34d98787
a9ec34d98787
```

kubectl:

```
$ kubectl get deployment nginx-app
NAME        DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
nginx-app   1         1         1            1           2m

$ kubectl get po -l run=nginx-app
NAME                        READY     STATUS    RESTARTS   AGE
nginx-app-2883164633-aklf7  1/1       Running   0          2m

$ kubectl delete deployment nginx-app
deployment "nginx-app" deleted

$ kubectl get po -l run=nginx-app
# Return nothing
```

> **Note:** When you use kubectl, you don't delete the pod directly. You have to first delete the Deployment that owns the pod. If you delete the pod directly, the Deployment recreates the pod.

docker login

There is no direct analog of `docker login` in kubectl. If you are interested in using Kubernetes with a private registry, see Using a Private Registry.

docker version

To get the version of client and server, see kubectl version.

docker:

```
$ docker version
Client version: 1.7.0
Client API version: 1.19
Go version (client): go1.4.2
Git commit (client): 0baf609
OS/Arch (client): linux/amd64
Server version: 1.7.0
Server API version: 1.19
Go version (server): go1.4.2
Git commit (server): 0baf609
OS/Arch (server): linux/amd64
```

kubectl:

```
$ kubectl version
Client Version: version.Info{Major:"1", Minor:"6", GitVersion:"v1.6.9+a3d1dfa6f4335", GitCom
Server Version: version.Info{Major:"1", Minor:"6", GitVersion:"v1.6.9+a3d1dfa6f4335", GitCom
```

docker info

To get miscellaneous information about the environment and configuration, see kubectl cluster-info.

docker:

```
$ docker info
Containers: 40
Images: 168
Storage Driver: aufs
 Root Dir: /usr/local/google/docker/aufs
 Backing Filesystem: extfs
 Dirs: 248
 Dirperm1 Supported: false
Execution Driver: native-0.2
Logging Driver: json-file
Kernel Version: 3.13.0-53-generic
```

```
Operating System: Ubuntu 14.04.2 LTS
CPUs: 12
Total Memory: 31.32 GiB
Name: k8s-is-fun.mtv.corp.google.com
ID: ADUV:GCYR:B3VJ:HMPO:LNPQ:KD5S:YKFQ:76VN:IANZ:7TFV:ZBF4:BYJO
WARNING: No swap limit support
```

kubectl:

```
$ kubectl cluster-info
Kubernetes master is running at https://108.59.85.141
KubeDNS is running at https://108.59.85.141/api/v1/namespaces/kube-system/services/kube-dns/
kubernetes-dashboard is running at https://108.59.85.141/api/v1/namespaces/kube-system/servi
Grafana is running at https://108.59.85.141/api/v1/namespaces/kube-system/services/monitorin
Heapster is running at https://108.59.85.141/api/v1/namespaces/kube-system/services/monitori
InfluxDB is running at https://108.59.85.141/api/v1/namespaces/kube-system/services/monitori
```

Edit This Page

Tools

Kubernetes contains several built-in tools to help you work with the Kubernetes
system.

- Kubectl
- Kubeadm
- Kubefed
- Minikube
- Dashboard
- Helm
- Kompose

Kubectl

`kubectl` is the command line tool for Kubernetes. It controls the Kubernetes
cluster manager.

Kubeadm

`kubeadm` is the command line tool for easily provisioning a secure Kubernetes
cluster on top of physical or cloud servers or virtual machines (currently in
alpha).

Kubefed

`kubefed` is the command line tool to help you administrate your federated clusters.

Minikube

`minikube` is a tool that makes it easy to run a single-node Kubernetes cluster locally on your workstation for development and testing purposes.

Dashboard

`Dashboard`, the web-based user interface of Kubernetes, allows you to deploy containerized applications to a Kubernetes cluster, troubleshoot them, and manage the cluster and its resources itself.

Helm

`Kubernetes Helm` is a tool for managing packages of pre-configured Kubernetes resources, aka Kubernetes charts.

Use Helm to:

- Find and use popular software packaged as Kubernetes charts
- Share your own applications as Kubernetes charts
- Create reproducible builds of your Kubernetes applications
- Intelligently manage your Kubernetes manifest files
- Manage releases of Helm packages

Kompose

`Kompose` is a tool to help Docker Compose users move to Kubernetes.

Use Kompose to:

- Translate a Docker Compose file into Kubernetes objects
- Go from local Docker development to managing your application via Kubernetes
- Convert v1 or v2 Docker Compose `yaml` files or Distributed Application Bundles

1315