NETWORK

SERVICE

5

„Connecting Pods, Wherever They Are.“

A Service is an abstraction that defines a logical set of Pods and a policy by which to access them. It provides stable IP addresses and DNS names, allowing you to expose an application running on a set of Pods to other applications or external users. Services can route traffic to Pods across multiple nodes.

WORKLOAD

DAEMONSET

35

„One Pod Per Node, Always.“

A DaemonSet ensures that a copy of a specific Pod is running on each node in the cluster. It's commonly used for deploying system-level services like logging or monitoring agents across all nodes. When new nodes are added, the DaemonSet automatically deploys the Pod to them.

ROLE BASED ACCESS CONTROL

ROLE

434

„Scoped Permissions, Focused Control.“

A Role defines permissions within a specific namespace, controlling access to Kubernetes resources. It allows you to set granular permissions, ensuring that users or applications can only perform the actions they need. Roles are ideal for managing security within a single namespace.

ROLE BASED ACCESS CONTROL

CLUSTERROLE

∞

„Cluster-Wide Permissions, Global Control.“

A ClusterRole is similar to a Role, but its permissions apply across the entire cluster, not just a single namespace. It's used to grant access to cluster-wide resources or to apply consistent permissions across multiple namespaces. ClusterRoles are essential for managing large, multi-tenant clusters.

CONFIGMAP

5

CONFIGURATION

„Configuration at Your Fingertips.“

A ConfigMap stores key-value pairs that Pods can use for configuration data. It decouples environment-specific configurations from container images, making it easier to manage and update settings without rebuilding images. ConfigMaps are ideal for keeping configuration data separate from application code.

PERSISTENT-VOLUMECLAIM

35

STORAGE

„Claim Your Storage, Persist Your Data.“

A PersistentVolumeClaim (PVC) is a request for storage by a user. It abstracts storage details and connects your Pods to PersistentVolumes, which provide the physical storage. PVCs ensure that your data remains available even if Pods are rescheduled or deleted.

NODE

MISCELLANEOUS

„The Backbone of Your Cluster.“

A Node is a physical or virtual machine that runs your applications and workloads in Kubernetes. It's the basic building block of a cluster, providing the CPU, memory, and network resources necessary to run your Pods. Nodes are managed by the control plane, which assigns workloads and handles scheduling.

NODE FAILURE

∞

EVENT CARD

„Neunmalkluges Zitat mit Bezug zur Karte von einer fiktiven Figur.“

Auswirkungen:

Ziehe 2 Karten, nimm 3 Gold, lege alles ab, lauf weg …

NETWORK

INGRESS

5

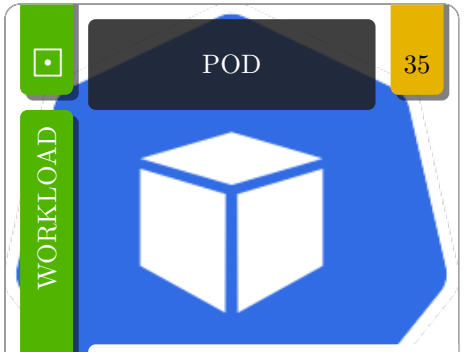
„Your Gateway to the Cluster.“

An Ingress is an API object that manages external access to services within a cluster, typically HTTP or HTTPS. It provides a way to route traffic based on rules, such as URL paths, to the appropriate services. Ingress helps you expose multiple services under a single IP address, simplifying external access management.

WORKLOAD

POD

35



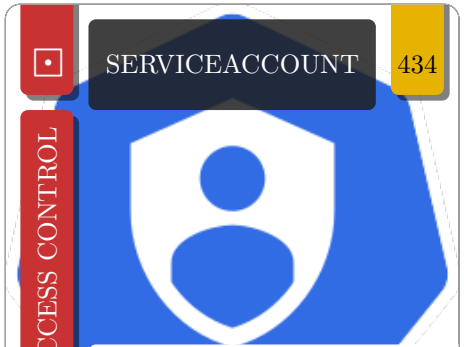
„The Smallest Deployable Unit.“

A Pod is the smallest and simplest Kubernetes object, representing a single instance of a running process in your cluster. It can contain one or more containers that share the same network namespace and storage. Pods are the fundamental building blocks for deploying applications in Kubernetes.

ROLE BASED ACCESS CONTROL

SERVICEACCOUNT

434



„Identity for Your Pods.“

A ServiceAccount provides an identity for processes that run in a Pod, allowing them to interact with the Kubernetes API. It grants permissions and tokens that control what the Pod can do within the cluster. ServiceAccounts are essential for managing secure and controlled access for applications.

MISCELLANEOUS

CUSTOMRESOURCE-DEFINITION

∞

„Extend Kubernetes, Your Way.“

A CustomResourceDefinition (CRD) allows you to create custom resources that extend Kubernetes' capabilities beyond its built-in objects. CRDs enable you to define and manage application-specific configurations or behaviors. They are key to building and scaling custom solutions on top of Kubernetes.

CONFIGURATION

SECRET 5

„Keep It Safe, Keep It Secret.“

A Secret is used to store and manage sensitive information, such as passwords, tokens, or keys, securely in your cluster. It decouples sensitive data from application code, ensuring that credentials and other secrets are not exposed in plain text. Secrets help maintain security best practices in Kubernetes.

STORAGE

STORAGECLASS 35

„Define Your Storage Strategy.“

A StorageClass provides a way to describe the classesöf storage available in a Kubernetes cluster. It abstracts storage provisioning, allowing PersistentVolumeClaims to automatically request specific types of storage (e.g., SSDs, NFS). StorageClasses enable flexible and automated storage management.

MISCELLANEOUS

NAMESPACE

„Organize and Isolate Your Resources.“

A Namespace is a way to divide cluster resources between multiple users or teams, providing isolation and resource scoping. It helps manage environments (like dev, test, prod) within the same cluster and allows for better organization and access control. Namespaces are essential for multi-tenant or complex deployments.

EVENT CARD

CVE DISCLOSED ∞

„Neunmalkluges Zitat mit Bezug zur Karte von einer fiktiven Figur.“

Auswirkungen:

Ziehe 2 Karten, nimm 3 Gold, lege alles ab, lauf weg …

NETWORK

INGRESS-CONTROLLER

5

„Traffic Control at the Edge.“

An IngressController is a component that implements the rules defined by an Ingress resource. It processes incoming HTTP/HTTPS requests and routes them to the appropriate Services in the cluster. IngressControllers are essential for managing external traffic and ensuring it reaches the correct endpoints.

WORKLOAD

REPLICASET

35

„Keep Your Pods Running.“

A ReplicaSet ensures that a specified number of identical Pods are always running in the cluster. It automatically replaces Pods that fail or are deleted, maintaining the desired state. ReplicaSets are crucial for ensuring high availability and scaling of your applications.

ROLE BASED ACCESS CONTROL

ROLEBINDING

434

„Linking Roles to Users.“

A RoleBinding grants specific permissions to a user, group, or ServiceAccount within a particular namespace by associating them with a Role. It's how you apply the access rules defined in a Role to actual users or services. RoleBindings help enforce security and access controls in a namespace.

ROLE BASED ACCESS CONTROL

CLUSTERROLE-BINDING

∞

„Cluster-Wide Access Control.“

A ClusterRoleBinding grants cluster-wide permissions to a user, group, or ServiceAccount by associating them with a ClusterRole. It allows you to apply access rules across all namespaces in the cluster. ClusterRoleBindings are essential for managing security and permissions on a global scale.

WORKLOAD

JOB

5

„Run to Completion.“

A Job creates one or more Pods that run to completion, ensuring that a specific task is executed a defined number of times. Once the Pods complete their task, the Job is considered finished. Jobs are ideal for batch processing or tasks that need to run once or a few times.

STORAGE

PERSISTENT-VOLUME

35

„Provisioned Storage for Your Cluster.“

A PersistentVolume (PV) is a piece of storage in the cluster that has been provisioned by an administrator or dynamically by a StorageClass. It is used by PersistentVolumeClaims to persist data beyond the life of individual Pods. PVs provide durable storage that remains available even when Pods are deleted.

NETWORK

NETWORKPOLICY

„Control Traffic, Secure Your Cluster.“

A NetworkPolicy is a set of rules that define how Pods can communicate with each other and with external endpoints. It controls traffic at the network level, specifying which connections are allowed or denied. NetworkPolicies are vital for securing communication between services and managing network segmentation.

EVENT CARD

POD RESTART

∞

„Neunmalkluges Zitat mit Bezug zur Karte von einer fiktiven Figur.“

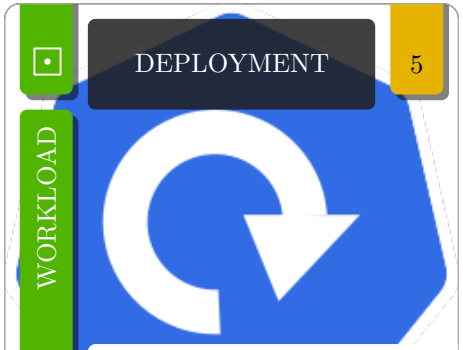
Auswirkungen:

Ziehe 2 Karten, nimm 3 Gold, lege alles ab, lauf weg …

WORKLOAD

DEPLOYMENT

5



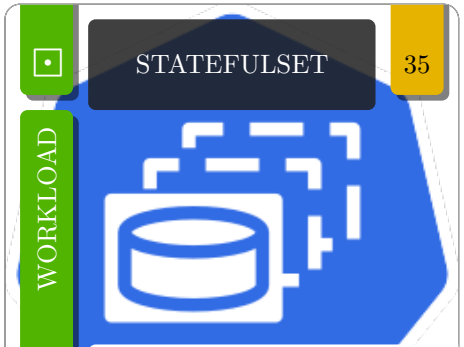
„Manage and Scale Your Pods.“

A Deployment automates the creation, updating, and scaling of Pods in a ReplicaSet. It ensures that your application runs consistently by rolling out updates and scaling up or down as needed. Deployments are essential for managing the lifecycle of stateless applications in Kubernetes.

WORKLOAD

STATEFULSET

35



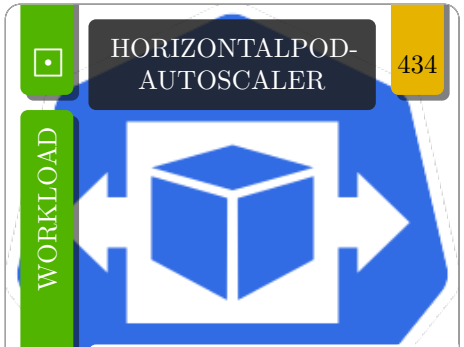
„Persistent Identity, Stable Storage.“

A StatefulSet manages the deployment and scaling of Pods with unique identities and stable network storage. It's used for stateful applications, where each Pod must retain its state across restarts. StatefulSets ensure that Pods are consistently ordered and maintain stable names.

WORKLOAD

HORIZONTALPOD-AUTOSCALER

434



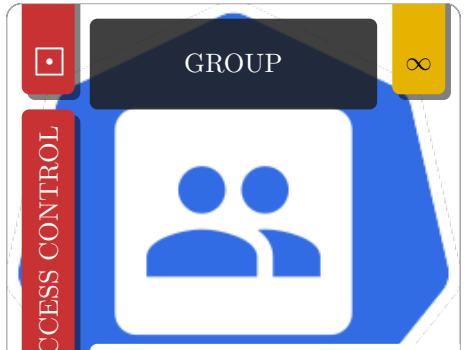
„Scale with Demand.“

A HorizontalPodAutoscaler automatically adjusts the number of Pods in a deployment, ReplicaSet, or StatefulSet based on observed CPU usage or other select metrics. It helps ensure your applications can handle varying loads by scaling resources up or down as needed.

ROLE BASED ACCESS CONTROL

GROUP

∞



„Organize Users, Simplify Access.“

A Group is a collection of users in Kubernetes that can be assigned roles and permissions collectively. Groups simplify access control management by allowing administrators to apply policies to multiple users at once. They are essential for managing permissions in larger teams or organizations.

WORKLOAD

CRONJOB

5

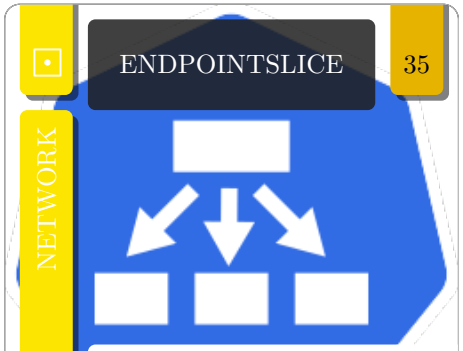
„Scheduled Tasks, Automated.“

A CronJob creates Jobs on a time-based schedule, allowing you to run tasks at specific intervals. It's ideal for recurring tasks like backups, reports, or maintenance scripts. CronJobs automate routine operations, ensuring they run regularly without manual intervention.

NETWORK

ENDPOINTSLICE

35

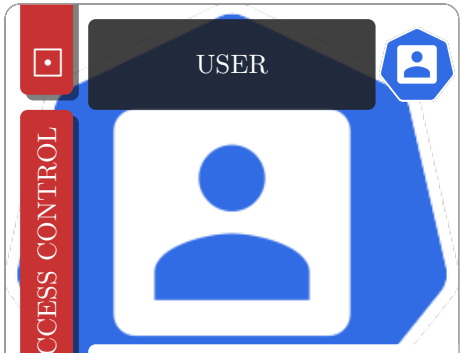


„Efficient Service Discovery.“

An EndpointSlice provides a scalable way to track network endpoints, improving the efficiency of service discovery within large clusters. It breaks down the list of endpoints into smaller slices, making it easier to manage and scale services. EndpointSlices enhance the performance of networking in Kubernetes.

ROLE BASED ACCESS CONTROL

USER



„Access Control Starts Here.“

A User represents an individual or a service that interacts with the Kubernetes API. Users are authenticated to determine what actions they can perform within the cluster. Proper management of users is crucial for securing your Kubernetes environment.

MISCELLANEOUS

CUSTOMRESOURCE

∞

„Tailored to Your Needs.“

A CustomResource extends Kubernetes by adding your own object types to the API, allowing you to manage application-specific configurations or processes. It works alongside CustomResourceDefinitions to let you create and control resources that Kubernetes doesn't provide out of the box. CustomResources enable powerful customization and automation.