## [COMPANY LOGO]

Sample RFI / RFP for Kubernetes & Cluster Management Software & Services

# Table of Contents

[TBD after content complete]

# Purpose of this Document

[This section can be removed prior to RFP distribution]

The purpose of this document is to assist companies and organizations with the creation of a request for information (RFI) or a request for proposal (RFP) for Kubernetes & Cluster management (KCM) software and services. It includes 40+ anonymized questions from real RFIs and RFPs related to Kubernetes management and may be freely used in the creation of future RFIs and RFPs.

# Important Considerations for Vendor Selection

Kubernetes & cluster management (KCM) is not a single activity, but a series of operational steps performed over time, involving the coordination of multiple disciplines across IT including development, operations and support.

[Please add any background and/or perspectives that would be useful for vendors to know when responding to this RFI/RFP]

# Section A: Company Profile

[Please provide the following information about the company issuing the RFI/RFP].

## Company Background

[Please describe the background of the company who is requesting proposals for Kubernetes & cluster management software and services].

## Project Overview and Objectives

The purpose of this RFI/RFP is to gather technical, delivery, and pricing information for Kubernetes & cluster management software and services. Specifically, [COMPANY NAME] is looking to acquire KCM software and services for the purposes of…[X, Y, Z].

## Infrastructure, Application & Cluster Information

[Please describe your current and future infrastructure (e.g., public clouds, on-premises, edge, etc.), the types of applications that require Kubernetes management, the number of applications and clusters that are currently supported and the volumes of which that are expected to be supported over the next 3 to 5 years].

## Current Application Deployment and Cluster Management Process

[Please describe the current application deployment and cluster management process employed by your corporation. Be as specific as possible and outline any existing internal standards for technologies and services within the Kubernetes ecosystem. Use the following table to summarize]:

|  |  |  |
| --- | --- | --- |
| **Technology Function** | **Existing Solution** | **Future Solution** |
| CI/CD | E.g., Jenkins | E.g., Same or Open |
| Registries |  |  |
| In-Memory Database |  |  |
| Persistent Storage |  |  |
| Networking |  |  |
| Security/Shared Secrets |  |  |
| Logging |  |  |
| Monitoring |  |  |
| [Additional…] |  |  |

# Section B: Schedule & Submission Instructions

The timeline of events for the RFI/RFP process is as follows:

## Schedule of Events

Please detail in the following table the anticipated schedule of events:

|  |  |
| --- | --- |
| *Task* | *Date (5pm ET)* |
| RFP distribution | XX/XX/XX |
| Deadline for vendors questions | XX/XX/XX |
| Answers to vendor questions | XX/XX/XX |
| Deadline for RFP submission | XX/XX/XX |
| Vendor notification of short-listed vendors | XX/XX/XX |
| Vendor presentations | XX/XX/XX |
| Vendor evaluations | XX/XX/XX |
| Vendor selection | XX/XX/XX |
| Project commencement | XX/XX/XX |
| Project completion | XX/XX/XX |

## RFP Cost

All costs incurred in the preparation and submission of responses to the RFI/RFP shall be the responsibility of the vendor.

## Late Proposals

Proposals received after the due date will not be considered. Regardless of the method used for delivery, vendors shall be wholly responsible for the timely delivery of submitted proposals.

## Proposal Delivery

Each submitted proposal shall consist of one (1) electronic copy using the following format(s): Microsoft Word, Microsoft Excel, and/or Adobe PDF and be submitted via email. Clearly label and index proposals with appropriate section and sub-section numbers as referred to herein. Number each page individually and provide a table of contents. All vendors submitting proposals must agree to Terms and Conditions in Section I. Please send all questions and final proposal to:

*[Contact Name] [Contact Email] [COMPANY NAME]*

## Selection Process

[Please describe any important details of the above Schedule of Events and outline the decision-making process for the purchase of KCM solution and services].

# Section C: Vendor Profile

Please provide the following information about your company and its products and services.

|  |  |
| --- | --- |
| Requirement | Vendor Response |
| Please list the contact information (name, address, phone, etc.) of the vendor location that would support this solution |  |
| How many years has your company been in business and how long has your product been on the market? |  |
| Describe the company vision and future direction for your company’s products and services |  |
| Describe your product road map and how it reflects the needs of your customers |  |
| Describe the company’s approach to product development and process for product enhancements |  |
| What CNCF accreditations or certifications does your company have? |  |
| Are you a member of and do you participate in any of the industry standards organizations or committees? If so, describe your role and responsibilities |  |
| Please classify your company as one or more of the following: Provider of Open Source Software, Provider of Commercial Software, Provider of Cloud-based Solution, Provider of Professional Services |  |
| Do you have partnerships with other vendors or service providers? If so, with which companies? Please provide a description of those partnerships |  |
| If any of your services are sub-contracted to another party, provide name, contact information, and description of each service each sub-contractor performs and their responsibilities. |  |

# Section D: Functional Requirements

For each requirement, indicate if the requirement is supported directly by the proposed solution(s). If more information or clarification is required enter that information in the Vendor Response column.

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Requirement** | **Supported? (Yes / No / Partially)** | **Vendor Response** |
|  | **KCM Core Functions** |  |  |
| Application Dashboards | Ready to use, detailed application dashboards that are critical for customer application operations teams for a bird's eye view of the health, usage and performance of their applications deployed to 1,000s of clusters. |  |  |
| Operational Dashboards | Ready to use, detailed operational dashboards that are critical for company's operations teams for a bird's eye view of the health, usage and performance of the clusters deployed across multiple customers. |  |  |
| Programmatic Access to Dashboard Data | All the data available via the Application and Operational Dashboards should be accessible to the company programmatically via APIs |  |  |
| Rapid Cluster Bring-up & Deploy Across Infrastructure | Company requires the ability to configure and bring-up clusters in any infrastructure in any combination including: On-premises (private cloud including bare metal, VMWare and Openstack), Public cloud (e.g., AWS, Azure, etc. across any region) and at Edge |  |  |
| Native Kubernetes | Company requires usage of the native Kubernetes distribution for each public cloud used (e.g., use of Amazon EKS when managing cluster on Amazon AWS). |  |  |
| In-Cluster Autoscaling | Company desires configurable horizontal (in-cluster) auto-scaling based on default and custom metrics |  |  |
| Operations Console | A dedicated console designed for the company's Operations Team to manage and support clusters deployed across the end customer's network. |  |  |
| Remote Debugging and Diagnostics | Company's IT Operations team should have access to built in remote debugging and diagnostics tools to address issues on 1,000s of remote clusters |  |  |
| Health and Capacity Monitoring | The Operations Console should provide real time visibility and access to the health and capacity utilization & monitoring of the managed clusters. |  |  |
| Programmatic Access | The controller should provide a rich set of REST APIs that can be used by the company to programmatically manage the controller and retrieve business critical information. |  |  |
| Audit Trail | All actions performed by the company's operations team should be recorded and accessible via an easy to use Audit Trail |  |  |
| Flexible Cluster Scaling Approaches | The managed clusters should support both manual and auto scaling so that addition capacity can be made available to customer applications when required |  |  |
| Application Ready Clusters | The managed clusters should be deployed with critical 3rd party components that are required for customer applications. For example, Prometheus for monitoring, Fluentd for Log Aggregation etc. |  |  |
| Importing Clusters | Company requires ability to import existing clusters into solution. |  |  |
| Deployment Flavors | The company should be able to support multiple deployment flavors for customer applications  - Edge: Small Footprint devices on the network edge such as MEC etc  - On-Premises: uCPE type devices deployed on-premises  - Cloud: Deployments on company's datacenter/cloud environments |  |  |
| Support for Helm and YAML | Companies requires full support for Helm charts and YAML defined objects |  |  |
| Hitless K8s & Cluster Upgrades | The controller should provide the means to upgrade k8s across the deployed fleet with zero impact to the applications |  |  |
| On Demand Cluster Patching | The company should be able to rapidly patch and update 1,000s of remote clusters when Kubernetes CVEs are reported. This is critical to ensure that customers are provided with a secure operating environment for their applications |  |  |
| Application Health Tracking | Company requires the platform tracks and monitors the health status of each deployed container replica globally across multi-cloud environments. |  |  |
| Rollbacks | Company requires support for both manual and automated rollbacks. DevOps teams can configure automatic rollbacks if the upgrade process fails for some reason. |  |  |
| Projects | Company requires ability to create and manage dedicated isolation boundaries or "Projects" which can have dedicated users, groups and resources (clusters, namespaces and integrations). Users assigned to specific projects will only have access/visibility into resources in their projects. |  |  |
| Cluster Blueprints | Company requires fleet of Kubernetes clusters need to ensure that clusters are standardized and compliant to those standards by defining and enforcing a certain baseline set of software components as required for the application profile. |  |  |
|  | **Security** |  |  |
| Roll-based Access Control (RBAC) | Users of the platform can be assigned roles that allow them to only perform specific operations |  |  |
| Single Sign-on (SSO) | Access to the Ops Console (Cluster Operations) and Application Console (App Operations) should provide the means for users to access via Single Sign On (SSO) using SAML etc. The Ops Console and the App Console will need to be configured to use different Identity Providers for Single Sign On. |  |  |
| Secured Controller Access (No SSH) | Clusters will be deployed in a customer's private network with the controller operating outside the customer's private network. The controller should not require the customer to make changes to their corporate firewall configurations to allow inbound network connectivity from the controller to the managed clusters. Instead, a dial out model should be supported by the managed clusters which will establish a long-lived control channel to the controller |  |  |
| Kubectl Access Control | Access to Kubectl should be controlled (via SSO and/or RBAC) and every action logged for audit and compliance purposes |  |  |
| Full Auditing | Company should have access to a rich audit trail which will track and report all activity performed by users |  |  |
| Multi-Factor Authentication (MFA) | Company should be able to strongly authenticate users using best of breed MFA authenticators |  |  |
| Secrets Management | All sensitive data in the platform should be encrypted using a hardware backed root of trust. Secrets that customer applications require are delivered encrypted to managed clusters and are decrypted/stored in non-persistent storage as it is made available to the application across 1,000s of locations |  |  |
| Namespace Support | Support for multiple namespaces ensuring logical isolation between different applications on the same cluster |  |  |
| Default TLS | Customer applications operating on the managed clusters provided with the option to leverage the built in API Gateway (Layer 7 Ingress) that is pre-configured for TLS 1.2 support with secure cipher suites |  |  |
| On-Demand Cluster Patching | The company should be able to rapidly patch and update 1,000s of remote clusters when CVEs are reported. This is critical to ensure that customers are provided with a secure operating environment for their applications |  |  |
| Log Aggregation | Company requires log management targets such as Elasticsearch and AWS S3. |  |  |
|  | **Alerting & Notifications** |  |  |
| Incident Management and Reporting | Company requires continuous monitoring of both clusters and applications deployed. When a critical issue is detected, the company requires automatically generated alerts to notify operations teams via a variety of notification channels. |  |  |
| Cluster Alerts | Alerts should be automatically generated by the KCM solution as it observes critical health related issues with the managed cluster. |  |  |
| Workload Alerts | Alerts should be automatically generated by the KCM as it observes critical health related issues with the workload's pods and services, for example, if there is insufficient capacity on one of the clusters to deploy the workload. |  |  |
| Notifications | The controller should provide the means to send notifications (email etc.) when managed clusters have operational issues. For example, hardware failure |  |  |
|  | **Application Deployment (CI/CD)** |  |  |
| Support for Continuous Integration (CI) | Company requires integration with CI tools such as Jenkins, CircleCI, Gitlab and Bamboo and end-to-end automation for Kubernetes cluster bring-up, containerized application deployment, infrastructure lifecycle, and more. |  |  |
| Support for Continuous Deployment (CD) | Company requires support for deployment pipelines for containerized applications and associated infrastructure as well as declarative, GitOps-based continuous delivery platform for containerized applications. |  |  |
|  | **Storage and Disaster Recovery** |  |  |
| Networked storage | For on-prem clusters, the platform should provide a turnkey and managed integration with networked storage for Kubernetes workloads to request PVCs |  |  |
| Managed Backup and Restore | The solution should support integrated capability for policy driven backup and restore capabilities for Disaster Recovery |  |  |
|  | **Kubernetes Ecosystem Integrations** |  |  |
| Container Registry Integrations | KCM should provide turnkey integrations with container registry platforms such as AWS Elastic Container Registry (ECR), Google Container Registry (GCR), JFrog Artifactory and others. |  |  |
| Secrets Management Integrations | KCM should provide turnkey integrations with crypto/secrets repositories such as Vault, thereby automating the end-to-end management and lifecycle of secrets across Kubernetes clusters deployed in the cloud or on premises. |  |  |
| SSO Integrations | Company requires integrations with SAML v2.0, Okta, PingOne and AzureAD to ensure users are provided seamless and secure access to their clusters |  |  |
| Managed Ingress Controller | KCM should provide turnkey integrations with Ingress Controllers (such as NGINX) |  |  |
|  | **Developer Productivity** |  |  |
| Developer Sandboxes | The platform should allow the company to build and operate a sandbox network of managed clusters that can be used to help their prospective customers perform trials and test drive the platform. |  |  |
| Integrated Debugging and Troubleshooting Capabilities | The platform should provide integrated and interactive debugging and troubleshooting capabilities for developers and operations teams to quickly diagnose and troubleshoot issues, correct them and make updates |  |  |
|  | **Customer Support & Professional Services** |  |  |
| Custom Engineering Services | Company should have access to certified Kubernetes administrators and developers that are available to assist company in configurations and integrations |  |  |
| Customer Support | Company should have enterprise-grade 24x7 support across multiple severity levels defined SLAs and communication channels (e.g., email, Slack, phone) |  |  |

# Section E: Architectural/Technical Requirements

|  |  |
| --- | --- |
| Architecture / Technical Approach | Vendor Response |
| Please detail the technical architecture of your solution. Explain why it is unique. Also, attach a separate diagram depicting this architecture. |  |
| Is your solution a self-contained solution or does the solution require additional licenses and software from third parties? Please describe. |  |
| Does your solution require additional hardware from third parties? Please describe. |  |
| Compared to your competitors, describe the key differentiators of your technical architecture |  |
| Describe how scalable your solution is – how does the solution handle hundreds of clusters? |  |
| Describe your application's ability to operate in a high availability data center |  |
| Describe any key technology differentiators (any leading-edge technologies?) that set your application apart from your competitor’s solutions. |  |

# Section F: Total Cost of Ownership

Please describe how much time and resources your solutions require to a) install and b) operate over time.

|  |  |
| --- | --- |
| TCO Components | Vendor Response |
| Please detail the amount of time typically required to install/bring-up your KCM solution. Please include the necessary hardware resources, expertise required and site specific customer examples that can be referenced. |  |
| Please detail the amount of time typically required to configure and integrate your KCM solution with our Kubernetes ecosystem vendors. Please include the necessary hardware resources, expertise required and site specific customer examples that can be referenced. |  |
| Please detail the number and expertise of resources required to manage your KCM solution over 3-5 years and site specific customer examples that can be referenced. |  |

Section G: Pricing

Please describe how your solution(s) are licensed and priced.

|  |  |
| --- | --- |
| Pricing Components | Vendor Response |
| How is your KCM solution licensed? Is it open source, commercial software or a cloud-based solution? |  |
| What is the cost for maintenance and support? Please detail available support packages. |  |
| Are training services available? Please list available services and cost. |  |
| Are professional services available? Please list available services and cost. |  |

# Section H: Customer References

Please provide four customer references that [COMPANY NAME] may contact that have used the solution you are proposing in production for at least 3 months:

|  |  |
| --- | --- |
| Reference 1 |  |
| Company Name |  |
| Contact Name |  |
| Contact Phone |  |
| Contact Email |  |
| Company Address |  |
| Description of Solution Provided |  |
| Benefits of Solution Provided |  |

|  |  |
| --- | --- |
| Reference 2 |  |
| Company Name |  |
| Contact Name |  |
| Contact Phone |  |
| Contact Email |  |
| Company Address |  |
| Description of Solution Provided |  |
| Benefits of Solution Provided |  |

|  |  |
| --- | --- |
| Reference 3 |  |
| Company Name |  |
| Contact Name |  |
| Contact Phone |  |
| Contact Email |  |
| Company Address |  |
| Description of Solution Provided |  |
| Benefits of Solution Provided |  |

# Section I: Terms and Conditions

[Please describe the appropriate terms and conditions the vendor must agree to for this project including confidentiality, insurance, compliance with applicable laws and indemnity clauses].