NetApp Instaclustr

MANAGED PLATFORM

Managed Platform Subscription: Apache Kafka®

Versions

The versions detailed at **https://www.instaclustr.com/support/documentation/useful-information/lifecycle-status-of-application-versions/** as GENERALLY AVAILABLE, DEPRECATED, CLOSED, LEGACY SUPPORT, or otherwise mutually agreed between the parties.

Cloud Provider/s

- Amazon Web Services (AWS)
- Google Cloud Provider (GCP)
- Azure

Services Provided

NetApp will provide the Customer with a 24x7 managed platform on supported public cloud infrastructure for the open source technologies detailed above and related add-on technologies and services that form part of NetApp Instaclustr's standard product catalogue as at the date of execution of this SOW.

Under the managed platform, NetApp shall be responsible for ensuring Customer's open source technology clusters (and add-on services) are operating effectively without impacting Customer's service (in consideration of the limitations of Customer's data model and use case), which generally includes:

- **24x7 Support**
  NetApp will provide a 24x7 support capability for responding to incidents related to Customer's open source nodes (and related technologies) in the managed platform scope set out in this Agreement.
- **Monitoring and Alerting on the Open Source Nodes**
  NetApp will monitor performance and availability of Customer's open source nodes. Alerts are sent to NetApp Instaclustr's 24x7 support team, who will investigate and action alerts in accordance with NetApp Instaclustr's Incident Severity Levels as defined in **Service Support**. Monitoring metrics can be accessed on the Managed Platform dashboard and also through an API. Where NetApp identifies issues caused by Customer's use of the cluster NetApp will provide guidance on solutions.

- **Backups and Snapshots**
  NetApp takes daily backups of ZooKeeper/KRaft data (topics and other configuration). Should Customer require a backup of data written to Kafka, Customer will be responsible for configuring and operating a Kafka consumer to maintain that back up outside of Customer's managed cluster.
- **Updates and Patch Management**
  NetApp will update operating systems, product software and NetApp's software as required, generally on a quarterly basis, or as/if when issues are identified (such as a critical security vulnerability is released).
- **Health Checks and Repairs**
  NetApp will perform daily cluster health checks.
- **Dashboard and API With Key Metrics of the Cluster**
  NetApp will provide Customer with access to live and historical performance and capacity metrics at the per node and at table level via its managed platform dashboard and API.
- **Service Level Management and Reporting**
  NetApp will manage and monitor the Service on an ongoing basis and provide a mechanism for Customer to verify that SLAs are being met (see **Service Levels**).
- **Capacity Management**
  NetApp will assist Customer in managing capacity of Customer's open source clusters through constant monitoring and reporting on cluster performance and health. Customer shall be entirely responsible for approval of capacity increases, however NetApp may temporarily add capacity to your cluster without prior permission where there is an imminent risk of cluster stability issues. NetApp will support Customer with this by advising when the appropriate time is to upscale or downscale the cluster for predetermined events. Customer can initiate via the managed platform or via a support channel a request to upscale or downscale the cluster at any time by either adding additional nodes or increasing the size (capacity) of existing nodes depending upon the product types used to implement Customer's clusters in the managed platform.

Customer will not install any additional software on managed nodes. Customer will have access to the cluster via the standard open source technology (and related technology) APIs to create tables, insert and update data or run jobs. Customer will not install any additional software components within the managed platform.

Open Source Software

Customer acknowledges and agrees to NetApp's use of open source software under a variety of licenses in the provision of the managed platform and that Customer is not required to directly license any open source software to use our managed platform. The open source software NetApp use includes the following permissive open source software:

- Apache Cassandra® (under the Apache 2.0 license)
- Apache Kafka® (under the Apache 2.0 license)
- Cadence® (MIT)
- ClickHouse® (under the Apache 2.0 license)
- Docker (under the Apache 2.0 license)
- Debian GNU/Linux (under GNU General Public License v2 and compatible licences)
- OpenSearch® (under the Apache 2.0 license)
- PostgreSQL® (under the PostgreSQL License)
- A number of enabling packages including Java

Required Third Party Services

Zendesk: NetApp uses Zendesk as its support ticketing system. Customer will be required to establish a Zendesk user account (no additional fees apply).

Service Support

Support Summary

The specific support capabilities and service levels associated with each level of support are described in the following table. In addition to what is listed there, all support tiers include:

- **24x7x365 Expert Support**
  NetApp provide around the clock expert support in English with initial response time as defined in the table below for customers contacting us via our self-service portal **support.instaclustr.com** (our preferred method) or emailing us at **support@instaclustr.com**. You can also use the live chat at **support.instaclustr.com** to ask for assistance, but please note that our live chat is only monitored 24 hours per day on workdays. We may be able to provide support in other languages; please contact us to find out more.
- **NetApp Instaclustr Console and API Access**
  Customers may securely manage their NetApp Instaclustr services and resources through the NetApp Instaclustr console and API. Customers can view detailed live and historical performance metrics, change firewall rules, expand a cluster, and add and delete clusters.
- **Technical Documentation**
  NetApp provides access to technical documentation and guides to assist customers in maximizing the value of their NetApp Instaclustr service. Technical documentation and guides are published and available through our support portal.
- **Security Reviews and Fixes**
  In addition to performing security reviews of NetApp Instaclustr features before they are implemented, we perform regular scans and tests of the NetApp environment. Any issues that arise from the scans are resolved as soon as practical. More detail on our security program can be found here: **https://www.instaclustr.com/support/security/**
- **Baseline Maintenance**
  NetApp ensures our clusters are running a recent, stable version of the core technology (Cassandra, OpenSearch, Kafka, etc.) and underlying operating system, with the latest version of our monitoring software. NetApp will advise of any upgrade to the version before changing the existing configuration. For application versions which are in **General Availability or Deprecated lifecycle states**, customers may request that NetApp defer a minor version upgrade by up to three months of the proposed date. Note that for “Non-Production” tier support, we replace development class clusters without attempting to recover the existing cluster which may result in data loss.

- **Disaster Recovery and Backup** (as applicable to the relevant service)
  The way NetApp provide disaster recovery and data backups for the various offerings differs, as listed below:
  - **Apache Cassandra**
    Snapshot backups are taken once daily for all Cassandra clusters by default and retained for 7 days. Other optional backups options are provided to customers, such as the ability to trigger manual backups. More information is available **here**.
  - **Apache Kafka**
    NetApp do not provide any backup services for Kafka, aside for backing up ZooKeeper data directory once daily, for clusters running in ZooKeeper mode and KRaft data directory once daily, for clusters running in KRaft mode. Kafka's architecture inherently allows for replication between nodes.
  - **Cadence**
    NetApp do not carry out any backups for Cadence itself. However, for customers using Advanced Visibility, any backup settings configured for their Cassandra, Kafka and OpenSearch clusters apply.
  - **Clickhouse**
    ClickHouse clusters are fully backedup every 6 days, and incrementally every 6 hours (for Production tier clusters) or 24 hours (for Non-Production tier clusters). Backup's are retained for 7 days and only one copy of replicated data is backedup
  - **OpenSearch**
    Snapshot backups are triggered once every hour by default and retained for 7 days.
    Information on snapshot backups for OpenSearch clusters can be found **here**.
  - **PostgreSQL**
    Full daily backups are taken by default and retained for 7 days. In addition, WAL (Walk Ahead Log) archiving is also carried out by default. Information on backups for PostgreSQL clusters can be found **here**.

Ticket Severity Levels

Support tickets are assigned a severity level that helps us prioritize issues for remediation. Urgent issues are worked 24x7 until they are resolved. High tickets are worked continuously with updates provided every 4-6 hours until they are resolved, or severity reduced. Normal and Low priority issues are worked during the working hours of the assigned Support team member.

Severity Level	Classification	Description
1	URGENT	• Total cluster outage or an outage having a significant impact on a customer's business. • An event causing significant degradation of a cluster's service with a significant impact on customer's business. • An event identified as a significant and immediate risk of causing a total cluster outage or significant degradation in service. • A vulnerability that is currently impacting the confidentiality, integrity or availability of customer data. • An unmitigated vulnerability with an identified exploit that would impact the confidentiality, integrity, or availability of customer data. • Incidents impacting clusters with non-production SLA tier will not be classified Urgent.
2	HIGH	• An event causing significant reduced availability of NetApp management features but not impacting customer cluster functionality. • Intermittent (but not persistent or current) significant degradation of cluster service. • A vulnerability, without an identified exploit, that materially increases the risk of impact to the confidentiality, integrity, or availability of customer data. • Proposed maintenance that, if not performed in a timely manner, will cause degradation of a customer's service. • Incidents impacting clusters with non-production SLA tier will not be classified High.

Severity Level	Classification	Description
3	NORMAL	• An incident with effects that are inconvenient though not impacting a customer’s business. • Normal is the maximum priority that will be assigned to clusters with a non-production SLA tier.
4	LOW	• Requests for information or planned changes. • Incidents or events not covered in any of the aforementioned severity levels.

Support Service Details

Support Service	Non-Production	Production - Base	Production - Premium
Definition	Applicable for all Non-Production node size clusters.	Applicable for all production node size clusters. [1]	Optional 20% uplift for customers with 0-100MU. By negotiation for 200+ MU
Initial response time	Best Effort	20 Minutes	10 Minutes
Health and performance monitoring [2]	Reduced	✓	✓
Extended maintenance [3]		✓	✓
Named contacts [4]	1	3	25
Direct access to assigned account executive [5]			✓
Enhanced Service Level Agreement [6]			✓

Support Service Details

1. **Upgrading to Premium Support Tiers**
   Qualified customers wishing to upgrade to the Premium support tier can be accommodated under certain conditions. Please reach out to your customer success representative to find out how.

2. **Health and Performance Monitoring**
   We actively monitor health and performance benchmarks for all our clusters to provide early detection and remediation of problems with a cluster. Where issues are identified which affect customer applications, we will notify customers through the relevant **account support contact**.

3. **Extended Maintenance**
   Extended Maintenance includes our pre-emptive intervention services to ensure clusters are running within expected limits. We allow time for manual intervention to ensure operations such as node clean-up are successful. We also provide initial assessment of and recommended resolution of high latency, high disk usage, and high CPU Usage events.

4. **Named Contacts**
   Named contacts are the primary point of contact registered with the NetApp Instaclustr support team. They have the right to raise issues within the NetApp ticket management system. The NetApp Instaclustr Support team notifies the support contact address or emergency support contact address (as appropriate) nominated in the NetApp Instaclustr console via email where a maintenance issue is identified and for resolution of support tickets.

5. **Direct Access to Assigned Account Executive**
   Premium support customers will have direct contact details for their NetApp Instaclustr account executive during business hours to escalate support issues and raise service concerns.

6. **Enhanced Service Level Agreement**
   Customers running production clusters, are eligible for Enterprise or Critical (where available) SLAs.

Support Exclusions

The following types of activities are excluded:

- Application architecture, design and implementation
- Open source technology training
- Attendance at the Customer site
- Activities or products that are listed under NetApp Instaclustr's consulting services including, but not limited to, broader advice on open source technology strategies and implementations

Additional Support

Services falling outside included support scope may be provided under a "fee for service" basis. If you have a request which does not fall under the defined scope of support as described above, please contact NetApp Instaclustr support or your customer success representative to discuss your requirement.

Services provided under this arrangement include, but are not limited to:

- Data model design and review focused on your application's requirements;
- Cluster reconfiguration;
- Specific cluster performance tuning;
- Requests for data loading in lower environments;
- BCP/DR simulations; and
- Actions from us to bring your cluster back from a catastrophic failure (not caused by our advice or actions), including:
  - Actions required due to exhausted disk space;
  - Actions required to recover from accidental deletion of data by you; and
  - Cluster recovery due to inappropriate data models or configurations.

Conditions of Running in Your Account

When running in Customer's account, Customer will have significant access to change configuration. It is a condition of NetApp Instaclustr's SLAs and support for Customer's cluster that Customer does not make any changes to any object created by NetApp Instaclustr's provisioning system without first agreeing those changes with NetApp.

NetApp will agree to any reasonable requested changes that do not pose a risk to the security or reliability of Customer's cluster or NetApp Instaclustr's management systems. Some changes may result in additional charges if they will increase the management load for Customer's cluster.

Any issues caused by unauthorized changes will not be subject to SLAs and NetApp may directly charge for support time required to resolve such issues.

Customer's Responsibilities

Maintaining the health of your cluster(s) is a cooperative effort between our customers and NetApp. Your obligations in this cooperative effort are:

1. Maintain node disk usage below requirements for the managed application (see SLA document for details);

2. Action reasonable requests from NetApp Instaclustr support to prevent issues arising and troubleshoot existing issues;

3. Use our self-service portal **support.instaclustr.com** (our preferred method) or email us at **support@instaclustr.com** to raise support requests;

4. Ensure that **support@instaclustr.com** is whitelisted in your email service;

5. Choose a secure password for your NetApp Instaclustr account that is commensurate with the sensitivity and value of your data;

6. Ensure that the logical security within your cluster (e.g., authentication, encryption) is commensurate with the sensitivity and value of your data; and

7. Where you have specific requirements for backup, security or operations, verify with NetApp Instaclustr support that our offerings meet your requirements.

8. Plan for significant changes on operational load or data volumes in your cluster and provision capacity in anticipation of those loads.

9. Remove all sensitive information or data from any logs, query results, code snippets, screen shares, or any other correspondence before sending to NetApp via support channels.

Support is not provided to customers with accounts over 30 days in arrears.

Responsibility Matrix

# NetApp Instaclustr Consulting can assist, on an additional paid basis, with items that are outside the scope of support or where a solution tailored to the customer's use case is required.

Process/ Task/ Responsibility	NetApp Instaclustr		Customer
	Managed Service	Consulting Service #	
Data Model, Topology and Data Management			
Design topic configuration		X	X
Design, create and manage topics			X
Topic design review, suggestions & recommendations		X	
Insert and delete data			X
Determine cluster topology and replication for application availability and performance requirements		X	X
Define topic retention and related requirements for the application		X	X
Ensure brokers are placed in appropriate racks based on cloud provider topology	X		
Define and set appropriate topic replication factor for application availability requirements			X
Determine and set topic compaction settings		X	X
Identify and explain performance problems caused by topic configuration	X		
Resolve performance problems caused by topic configuration		X	X
Cluster reconfiguration, including altering broker configuration files and topology	X		
Reassign partitions after cluster topology changes	X		
Specific application and cluster performance testing		X	X
Actions required due to exhausted disk space after warning	X		

Process/ Task/ Responsibility	NetApp Instaclustr		Customer
	Managed Service	Consulting Service #	
Cluster recovery due to inappropriate topic configuration or application usage		X	X
Cluster management			
Provide initial assessment of, and recommended resolution of, high latency, high disk usage and high CPU Usage events	X		
Provide detailed assessment of, and recommended resolution of, high latency, high disk usage and high CPU Usage events		X	
Monitor broker disk usage	X		
Monitor cluster latency and availability. Take action to remain within SLA	X		
Maintain broker disk usage under 70%			X
Action reasonable requests from NetApp Instaclustr support to prevent issues arising			X
Deploy and manage producers, consumers, Kafka Streams and Kafka Connect (if used)			X
Capacity Planning			
Define growth expectations, latency thresholds for the cluster			X
Plan for significant changes on operational load or data volumes in your cluster and provision capacity in anticipation of those loads			X
Backup and recovery Note: in line with recommended operational practice, we do not perform backups of Kafka clusters			
Maintain ability to recreate cluster configuration (topics, etc)			X
Work with customer to simulate disaster recovery exercise	X		

Process/ Task/ Responsibility	NetApp Instaclustr		Customer
	Managed Service	Consulting Service #	
Cluster Security			
Chose a secure password for your NetApp Instaclustr account that is commensurate with the sensitivity and value of your data			X
Ensure that the logical security within your cluster (e.g. authentication, encryption) is commensurate with the sensitivity and value of your data			X
Design cluster roles and permissions			X
Create / Initialize cluster roles and permissions			X
Manage cluster administrators and service users			X
Log customer activity in Kafka cluster			X
Log NetApp Instaclustr activity in Kafka cluster (including ssh access)	X		
Retain exclusive operating system root privileges and ssh access	X		
Maintain NetApp Instaclustr superuser account in Kafka	X		
Monitor and detect malware in NetApp Instaclustr-managed instances	X		
Incident Resolution			
Provide 24x7 support for underlying broker instances in line with support level SLA	X		
Provide 24x7 support for Kafka in line with support level SLA	X		
Assess impact of the incident to customer business as per severity levels defined in the support policy	X		
Notify the customer on detection of an incident that may have a customer-visible impact, and provide updates on progress and resolution	X		

Process/ Task/ Responsibility	NetApp Instaclustr		Customer
	Managed Service	Consulting Service #	
Create patches or workarounds for Apache Kafka bugs impacting customers (patches will be submitted back to project)	X		
Produce post mortem incident reports for Severity 1 incidents as required	X		
Participate in customer RCAs or incident reviews as required	X		
General			
Where you have specific requirements for backup, security or Kafka operations, verify NetApp Instaclustr offerings meet your requirements			X

Note:

- For PCI enabled clusters, please refer to the following document for additional responsibilities specific to PCI enabled clusters: **https://www.instaclustr.com/support/documentation/useful-information/pci-compliance/**
- For RIYOA-Specific Cloud environments, please refer to the following document for additional responsibilities: **Generic RIYOA**

NetApp® Instaclustr specializes in open source technologies for enterprises. Our managed platform streamlines data infrastructure management, backed by experts who ensure ongoing performance, scalability, and optimization. This enables companies to focus on building cutting edge applications at lower costs.

NetApp Instaclustr

info@instaclustr.com | www.instaclustr.com