NetApp® Instaclustr Services Specific Terms
January 2025

These Service Specific Terms ("Service Specific Terms") for **NetApp® Instaclustr** Support Service ("Instaclustr Support Service") and Platform Service ("Instaclustr Platform Service") are part of the NetApp Cloud Services-Terms of Service ("Terms"). Capitalized terms used, but not defined in these Service Specific Terms, will have the meaning assigned to them in the Terms.

1. Service Level Agreement (Instaclustr Support Services)

If the Service does not achieve the service levels described in this Service Level Agreement (SLA), then you may be eligible for a service credit.

We reserve the right to change the terms of this SLA or discontinue the SLA at our discretion. We will honor the SLA in effect at the outset of your subscription for the duration of your initial Subscription Term. However, if you renew your subscription, the version of this SLA that is in effect the time of renewal will apply throughout your renewal term.

Availability Service Level

NetApp will use commercially reasonable efforts to make support available 24 hours a day, seven days a week, during any monthly billing cycle.

Response Time Service Level

NetApp will use commercially reasonable efforts to respond to support requests no later than 20 minutes from which the support request is received from an authorized customer support contact by NetApp via one of the support channels until acknowledgement by a NetApp Technical Operations Engineer to the Customer and incident resolution commenced according to the defined incident severities.

Service Credits

For each breach of the response time SLA beyond the second in any month, 10% of the monthly contract support subscription fees as a service credit to a maximum of 50% of the monthly contracted support subscription. The service credit will apply to future use of the Instaclustr Support Services and will be deducted from your next billing cycle/invoice,

2. Service Level Agreement (Instaclustr Platform Services)

If the Service does not achieve the service levels described in this Service Level Agreement (SLA), then you may be eligible for a service credit.

We reserve the right to change the terms of this SLA or discontinue the SLA at our discretion. We will honor the SLA in effect at the outset of your subscription for the duration of your initial Subscription Term. However, if you renew your subscription, the version of this SLA that is in effect the time of renewal will apply throughout your renewal term.

The SLA is tiered based on the technology, size, number and/or class of the cluster that the Customer is running. The tiers recognize that larger clusters can support more consistent levels of performance and availability and is as follows:

Instaclustr Platform Services supporting Apache Cassandra®

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability[4] (99.9% target) ○ No latency[3] SLAs	○ Minimum replication of 2 on all topics ○ Add capacity or adjust retention settings when requested by the NetApp Instaclustr

		product team to maintain disk usage in normal operations as less than 80% o Comply with reasonable requests from NetApp to modify application for best practice Cassandra usage
Small (5 or less production nodes)	o 99.95% availability for LOCAL_QUORUM o No latency SLAs o 20% monthly fees at risk in total; 10% credit for each breach	o Minimum replication factor of 3 on all keyspaces (please ensure that cluster is initially configured with target RF of 3) o Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% o Comply with reasonable requests to modify the application for best practice Cassandra usage
Enterprise (6+ production nodes)	o 99.99% availability for LOCAL_QUORUM consistency operations o 99% of read/write transactions to NetApp-maintained table in the cluster within specified latency threshold[3] o 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	o Minimum replication factor of 3 on all keyspaces (please ensure that cluster is initially configured with target RF of 3) o Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% o Comply with reasonable requests to modify the application for best practice Cassandra usage
Critical (12+ production nodes)	o 100% availability for LOCAL_QUORUM consistency operations o Custom latency SLA negotiable (or use medium SLA)[3] o 100% of monthly fees at risk in total; 30% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	o Minimum replication factor of 5 on all keyspaces (please ensure that cluster is initially configured with target RF of 5) o Separate testing and production clusters o Customer notifies that they wish to receive this SLA, commissions NetApp to review their application for best practice alignment and actions finding from that review. o NetApp review prior to deploying changes that may impact latency SLA o Add capacity or remove data when requested by the NetApp Instaclustr product team to maintain disk usage in normal operations at less than 70% o Comply with reasonable requests to modify the application for best practice Cassandra usage

**For Enterprise and Critical level Cassandra clusters, we also provide Recovery Point Objective SLA: The native replication of data in Cassandra means restoration of data from backups is rarely required. However, we will maintain backups to allow restoration of data with less than 24 hours data loss for standard backups and less than 5 minutes data loss for our Continuous Back-ups option. Should we fail to meet this recovery point objective, you will be eligible for SLA credits at 100% of monthly fees for the relevant cluster. If you have undertaken to restore testing of your cluster in the last 6 months (using our automated restore functionality) and can demonstrate that data loss during an emergency restore is outside target RPO and your verification testing, then you will be eligible for SLA credits at 500% of monthly fees.

Instaclustr Platform Services supporting Debezium® Change Data Capture Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	o No guaranteed availability[4] (99.9% target) o No latency[3] SLAs	o Add capacity when requested by NetApp to maintain disk usage in normal operations as less than 70%

		○ Comply with reasonable requests from NetApp to modify the application for best practice Debezium usage
Enterprise (3+ production nodes)	○ 99.95% availability for get data into Kafka within <5 minutes ○ 10% monthly fees at risk in total; 5% credit for each breach	○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application for best practice Debezium usage

**Service Level Objective is for delivery of at least 1 replica to Debezium. Duplicate writes may be delivered.

<u>Instaclustr Platform Services supporting Apache Kafka® Services</u>

Tier[1]	Service Standards[2]	Customer Requirements
Starter[11,18] (Developer nodes)	○ No guaranteed availability[4] (99.9% target) ○ No latency [3] SLAs	○ Minimum replication of 2 on all topics ○ Add capacity or adjust retention settings when requested by the NetApp Instaclustr product team to maintain disk usage in normal operations as less than 80% ○ Comply with reasonable requests to modify application for best practice Kafka usage
Small[17] (5 or less production nodes)	○ 99.95% availability for writes with 2 replica consistency requirement and all reads ○ No latency SLAs ○ 20% monthly fees at risk in total; 10% credit for each breach ○ PrivateLink availability of 99.99%	○ Minimum replication of 3 on all topics ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations as less than 80% ○ Comply with reasonable requests to modify application for best practice Kafka usage
Enterprise[17] (6+ production nodes)	○ 99.99% availability for writes with 2 replica consistency requirement and all reads ○ Availability SLA is increased to 99.999% when dedicated ZooKeeper/KRaft nodes are used ○ 99% of read/write transactions to NetApp-maintained topic in the cluster within specified latency threshold[3] ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA ○ PrivateLink availability of 99.99%	○ Minimum replication factor of 3 on all topics ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 80% ○ Comply with reasonable requests to modify the application for best practice Kafka usage
Critical[17] (12+ production nodes)	○ 99.999% availability for writes with 2 replica consistency requirement and all reads ○ 99% of read/write transactions to NetApp-maintained topic in the cluster within specified latency threshold[3] ○ 100% of monthly fees at risk in total; 30% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA ○ PrivateLink availability of 99.99%	○ Minimum replication factor of 3 on all topics ○ Separate testing and production clusters ○ Must use dedicated ZooKeeper/KRaft nodes for production ○ Customer notifies that they wish to receive this SLA, commissions NetApp to review their application for best practice alignment and actions findings from that review ○ NetApp review prior to deploying changes that may impact latency SLA ○ Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 80%

		○ Comply with reasonable requests to modify application for best practice Kafka usage

Instaclustr Platform Services supporting Kafka® Connect Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter[11] (Developer nodes)	○ No guaranteed availability[8] (99.9% target)	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Kafka Connect usage
Production Nodes	○ 99.99% availability[8] to NetApp maintained synthetic transaction connector ○ 20% monthly fees at risk in total; 10% credit for each breach	○ Minimum of 3 nodes ○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Kafka Connect usage

Instaclustr Platform Services supporting Redis® Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Redis usage
Enterprise (6+ production nodes)	○ 99.99% availability[9] to NetApp maintained synthetic transaction ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ The number of Redis Replica Nodes is greater than or equal to the number of Redis Master Nodes ○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Redis usage

Instaclustr Platform Services supporting Valkey™ Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Valkey usage
Enterprise (6+ production nodes)	○ 99.99% availability[9] to NetApp maintained synthetic transaction ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ The number of Valkey Replica Nodes is greater than or equal to the number of Valkey Master Nodes ○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice Valkey usage

Instaclustr Platform Services supporting Apache ZooKeeper™ Services

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests to modify the application for best practice ZooKeeper usage

Enterprise (3+ production nodes)	○ 99.99% availability[10] ○ No latency[3] SLAs ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Add capacity as reasonably requested by the NetApp Instaclustr product team to manage operational loads. ○ Comply with reasonable to modify the application for best practice ZooKeeper usage

Instaclustr Platform Services supporting PostgreSQL® Services

Tier	Service Standards	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (targeting 99.95%[12]) ○ No latency SLAs	○ Add capacity as reasonably requested by NetApp to manage operational loads. ○ Configure cluster replication and query settings which are appropriate for their data loss tolerance[13] ○ Comply with reasonable requests from the NetApp Instaclustr product team to modify the application for best practice PostgreSQL usage ○ Add capacity or remove data when requested to maintain disk usage in normal operations at less than 70%
Enterprise (2+ production nodes, or 3+ if utilizing synchronous mode strict)	○ 99.99%[12] availability for read and write operations ○ 99.9%[3] of read/write transactions to NetApp-maintained table in the cluster within specified latency threshold ○ 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	○ Add capacity as reasonably requested by NetApp to manage operational loads ○ Comply with reasonable requests from the NetApp Instaclustr product team to modify the application for best practice PostgreSQL usage ○ Configure cluster replication and query settings which are appropriate for their data loss tolerance[13] ○ Add capacity or remove data when requested to maintain disk usage in normal operations at less than 70%

**Availability uptime is not inclusive of one 60-minute scheduled maintenance window per month. During the maintenance window database connectivity may be interrupted for short periods during switchover to secondary nodes. Customers will be notified of scheduled maintenance at least 7 days in advance.

Instaclustr Platform Services supporting OpenSearch Services[14]

Tier[1]	Service Standards[2]	Customer Requirements
Starter (Developer nodes)	○ No guaranteed availability (99.9% target) ○ No latency[3] SLAs	○ Minimum of one replica shard on all indices ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify application and index settings for best practice OpenSearch usage
Small (5 or less production nodes)	○ 99.95% availability[15] for search and index operations, where wait_for_active_shards is 2 or less. ○ No latency SLAs ○ 20% monthly fees at risk in total; 10% credit for each breach	○ Minimum of 2 replica shards on all indices ○ Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 70% ○ Comply with reasonable requests to modify the application and index settings for best practice OpenSearch usage

Enterprise (6+ production nodes)	o 99.99% availability[15] for search and index operations, where wait_for_active_shards is 2 or less o 95% of index/search operations to NetApp-maintained Index in the cluster within specified latency threshold[3] o 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing breach of latency SLA	o Minimum of 2 replica shards on all indices o Use dedicated masters o Add capacity or adjust retention settings when requested by NetApp to maintain disk usage in normal operations at less than 70% o Comply with reasonable requests to modify the application and index settings for best practice OpenSearch usage
Critical (12+ production nodes)	o 99.999% availability[15] for search and index operations, where wait_for_active_shards is 2 or less o 99% of index/search operations to NetApp-maintained index in the cluster within specified latency threshold[3] o 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing a breach of latency SLA	o Minimum of 2 replica shards on all indices o Use dedicated masters o Separate testing and production clusters o Customer notifies that they wish to receive this SLA, commissions NetApp to review their application and index settings for best practice alignment and actions findings from that review o NetApp Instaclustr product team review prior to deploying changes that may impact latency SLA o Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% o Comply with reasonable requests to modify the application for best practice OpenSearch usage

Instaclustr Platform Services supporting Cadence Services

Tier	Service Standards	Customer Requirements
Starter (Developer Size Nodes)	o No guaranteed availability (99.9% target) o No latency SLAs	o Add capacity as reasonably requested by NetApp to manage operational loads o Comply with reasonable requests to modify the application for best practice Cadence usage. o Comply with requirements for Starter level SLAs for dependency services (Cassandra, Kafka, OpenSearch)
Production (3+ Production size nodes for each of Cadence and its dependency service clusters)	o 99.95% availability as measured by NetApp Instaclustr synthetic transaction monitoring o 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA and 10% credit for each incident causing a breach of latency SLA	o Add capacity as reasonably requested by NetApp to manage operational loads o Comply with reasonable requests to modify the application for best practice Cadence usage o Comply with requirements for at least Small level SLAs for dependency services (Cassandra, Kafka, OpenSearch)

Instaclustr Platform Services supporting ClickHouse® Services

Tier	**Service Standards**	**Customer Requirements**
Starter (Developer Nodes)	• No guaranteed availability[4] (99.5% target)	• Comply with reasonable requests to modify the application for best practice ClickHouse usage,

Production – Small (production nodes)	• 99.95% guaranteed availability[4] as measured by NetApp Instaclustr synthetic transaction monitoring • 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA.	• At least 2 replicas per shard per cluster. • Minimum of 3 nodes per cluster • Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% • Comply with reasonable requests to modify the application for best practice ClickHouse usage.
Production – Enterprise (production nodes)	• 99.99% guaranteed availability[4] as measured by NetApp Instaclustr synthetic transaction monitoring • 30% of monthly fees at risk in total; 15% credit for each incident causing breach of availability SLA.	• At least 3 replicas per shard per cluster. • All clusters must use dedicated ClickHouse Keeper nodes. • Add capacity or remove data when requested by NetApp to maintain disk usage in normal operations at less than 70% • Comply with reasonable requests to modify the application for best practice ClickHouse usage.

Claims Process

If at any time during your Subscription Term, you determine that you are not receiving the Availability Service Level, contact support@instaclustr.com and include the following information in your email:

- Calculated Downtime
- Description in incident of issue
- Cluster ID of impacted cluster(s)

[1] SLA tier is per-cluster and based on the number of nodes in the cluster. Customer credits are calculated based on the fees payable for the cluster or clusters impacted by the incident. SLAs credits apply to production clusters only.

[2] Service levels are measured on a monthly basis based on NetApp Instaclustr's monitoring systems. All service levels exclude outages caused by non-availability of service at the underlying cloud provide region level or availability zone level in regions which only support two availability zones.

[3] Latency is measured at a minimum rate of one read/write pair per node per 20 second period. Latency SLA excludes incidents where the cause is determined to be changes to a customer's application or unusually high loads on the cluster.

[4] Availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one read/write pair per node per 20 second period. A cluster is considered to be unavailable where read/write operations fail for a majority of nodes in the cluster in a given check-in period.

[5] Where a customer meets requirements for a tier based on cluster size but does not meet other requirements for a tier, the highest level of SLA where all requirements are met will apply.

[6] All SLAs exclude issues caused by customer actions including but not limited to attempting to operate a cluster beyond available processing or storage capacity.

[7] SLA credits must be claimed by customers within 14 days of the end of the relevant calendar month.

[8] For Kafka Connect, availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one Connector read or write operation per cluster per 20 second period. Excludes issues caused by BYO Kafka Connect Connectors due to the potential impact of user code on the availability of these environments.

[9] For Valkey, availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one read or write operation per cluster per 20 second period. Excludes latency issues caused by the use of integrated Lua scripting (EVAL and EVALSHA). Excludes issues caused by customers executing commands marked as "dangerous" by the Valkey project (turning on authentication will restrict access to these commands). Details of these commands can be found here.

[10] For ZooKeeper, availability is measured by establishing a connection with the ZooKeeper server on each node using a local ZooKeeper client, on a per node per 20 second basis.

[11] For preview versions of Kafka and Kafka Connect, only their respective "Starter" tier SLAs are valid. Production usage may be brought under an agreed SLA for the GA version after joint testing. Please contact us if you wish to discuss this option.

[12] PostgreSQL availability is measured by NetApp Instaclustr's synthetic monitoring at a minimum rate of one read/write pair per node per 20 second period. A cluster is considered to be unavailable where read/write operations fail for all nodes in the cluster in a given check-in period. PostgreSQL SLAs exclude issues caused by customer actions including but not limited to; attempting to operate a cluster beyond available processing or storage capacity, modifications to application configuration, or customer initiated reloads or resizes. PostgreSQL uptime is not inclusive of one 30-minute scheduled maintenance window per month. Customers will be notified

of scheduled maintenance at least 7 days in advance, and the NetApp Instaclustr product team will make all reasonable attempts to minimize the impact to your availability.

[13] Client PostgreSQL applications should be configured in order to maintain high availability and reestablish connections in the event of a master replica failure. For more information see Replication and High Availability

[14] OpenSearch SLAs also apply to legacy OpenDistro for Elasticsearch clusters.

[15] The KNN plugin will use additional off heap memory. The default cache and selected node size may be inappropriate depending on the specific use of the plugin combined with other OpenSearch activities. This may result in cluster instability and customers need to be aware this could impact high availability of the cluster.

[16] Clusters created as “Bundled Use Only” are covered by SLAs only when used purely as a supporting service for another NetApp Instaclustr offering (i.e., no direct access).

[17] Enterprise Add-ons for Kafka (Schema Registry, REST Proxy, Karapace Schema Registry and Karapace REST Proxy) are excluded from availability and latency SLAs.

[18] For preview versions of Enterprise Features for Kafka, only the “Starter” tier SLAs are valid. Production usage may be brought under an agreed SLA for the GA version after joint testing. Please contact us if you wish to discuss this option.

3. Open-Source Software

In the event NetApp distributes or otherwise provides for Customer any software for which the original source code is made freely available to the public under a designated open source license which permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form (“Open Source Software”) to Customer in furtherance of the delivery of the services associated with this Order Form, then such Open Source Software is subject to the terms of the applicable open source license. To the extent there is a conflict between the terms and conditions of this Order Form and the terms and conditions of the applicable open-source licensee, the terms and conditions of the open-source license will prevail.

Bug fixes, patches and features developed for Open-Source Software (Open-Source Contribution), because of the services associated with this Order Form, may be released by NetApp to the Apache Software Foundation project or other relevant open-source project at any time (a “Open-Source Software Contribution”). The parties agree that, despite any other provision in the Order Form, neither NetApp nor Customer has any right (including IP Rights), title or interest in the Open-Source Contribution.

4. Service Use for Processing Personal Information

If personal information has not been specified in the Order Form, Customer will not use the Services for the storage and processing of personal information without NetApp’s consent.

If personal information has been specified in the Order Form. NetApp acknowledges that Customer will use of the Services for the storage and processing of personal information. Where personal information is stored in the Services NetApp recommends:

- Using application encryption (as appropriate) for all personal information before storage in the Services;
- Enabling Customer to Server encryption when provisioning clusters;
- For clusters running in AWS, enabling EBS encryption within the Services when provisioning clusters;
- Meeting NetApp’s published baseline security control requirements for NetApp Instaclustr services applicable to Customers;
- Meeting all Customer security responsibilities as described in the Agreement; and
- Implementing any additional security controls as are reasonably recommended by NetApp.

Customer must provide NetApp, at reasonable periods, information regarding the total number of personal records stored within the Services to enable NetApp to meet its security, insurance, and other compliance requirements.

In order to provide you with the most effective response, information submitted to NetApp via email or our support portal may be sent to any or all members of our support team, in Australia, UK, Europe, India and the US. As such, NetApp requires that you ensure that information that is considered Personal Information, Health Information, or PCI related data is NOT submitted to NetApp via email, our support portal or any chat interface. The only approved mechanism for submitting such data, is directly to a managed cluster.

NetApp will manage Customer's clusters and information as stated in NetApp's SOC-2 accreditation. NetApp will not be liable to Customer for any data breach arising from Customer's failure to implement any of the above recommendations.

5. **PCI Compliance**. If Customer wishes to run a cluster in PCI mode, Customer must comply with the requirements as set out in the PCI Responsibilities Document available at https://www.instaclustr.com/support/documentation/useful-information/pci-compliance/

6. **Security Incident reporting**
Any incident suspected in Customer Facing Infrastructure must be reported to **support@instaclustr.com**, which will instigate the Major Incident Management process.
For the purposes of this procedure, Customer Facing Infrastructure means any customer managed environment, regardless of whether it is Run In Instaclustr's Account, Run in Your Own Account, or Run In Customer Managed Infrastructure / On-Premise. It also includes support only customers, where we support the infrastructure that is the subject of the incident.

7. **Customer Responsibilities—Baseline Security Controls**
At a minimum, we require you to implement and monitor the following aspects of the security of your account and cluster. You are responsible for:
    a. Configuring firewall rules via the NetApp Instaclustr Console.
    b. Configuring encryption between the client and the cluster.
    c. Approving user access to the cluster.
    d. Removing user access to the cluster on a timely basis.
    e. Providing accurate, current, and complete information in their communications with NetApp.
    f. Reading release notes published on the website www.instaclustr.com.
    g. Determining the authentication method to the console from those supported by NetApp (i.e. password rules or two-factor authentication).
    h. Cluster capacity planning and cross data center performance considerations.
    i. Defining and configuring the number of nodes and hence the layers of redundancy required.
    j. Adding, managing and removing the data stored on the NetApp Instaclustr platform.

8. **Data Protection.** NetApp will maintain commercially reasonable administrative, physical and technical safeguards to protect the security, confidentiality and integrity of Customer's Data. All NetApp Instaclustr services rely on Office365 and Zendesk for customer interactions. NetApp has reviewed and are satisfied that these services meet a reasonable level of security for information typically provided to our technical support team. Customer should review the security practices of Office365 and Zendesk to confirm that Customer is satisfied that the level of protection is appropriate for any data Customer is considering submitting to NetApp. The links to their security practices are provided below:
Microsoft Office365 Security
Zendesk Security

9. **Managed Services**
    (a) **Data Protection.** Cluster safeguards include the ability to enable encryption of Customer's Data at rest and in transmission to Your Environment (using TLS or similar technologies) over the Internet, except for any Third-Party Services that does not support encryption, which Customer may link to through the Services at Customer's election. Some NetApp Instaclustr instances do not support encryption. This is clear in the NetApp Instaclustr console on cluster creation, and Customer is responsible for ensuring that the protection required for Customer's Data is appropriately enabled.

    (b) **Data Center Environment and Physical Security.** The Sub-processors which are utilized by NetApp, as per Customer's instructions, for hosting services in connection with NetApp's provision of the NetApp Instaclustr Service employ their own security measures. Customer is responsible for verifying that the measures of Customer's chosen provider are appropriate for Customer's use case. NetApp review each supported providers SOC2 report and are satisfied that they meet an appropriate level of protection for both NetApp and NetApp's Customer's Data. NetApp recommends that Customer obtains and review the SOC2 report of the underlying Cloud Provider(s) that Customer is considering. Where Services are within the scope of NetApp security accreditations, NetApp will review at least the SOC2 report of the service at least once per year. Any issues will be assessed in accordance with NetApp's vulnerability assessment process.