instaclustr
by NetApp

PCI Responsibilities

Updated: July 2024

Introduction

Instaclustr has achieved PCI Compliance for specific services in specific configurations. This document outlines the configurations that are covered by our PCI Compliance claims, an overview of our controls, and requirements for any customer wishing to run an Instaclustr cluster in PCI mode.

PCI Configurations

The following configurations are covered by our PCI scope:

1. Apache Cassandra®, Apache Kafka®, OpenSearch®, Redis™, and Cadence® are able to be provisioned in a PCI Configuration.
    a. Cadence PCI clusters must be provisioned and maintained with dedicated underlying services (Cassandra, Kafka, and OpenSearch) that are also PCI compliant
2. Only clusters in Amazon Web Services (AWS) and Google Cloud Platform (GCP) are supported at this time.
3. Both Run In Instaclustr's Account (RIIA) and Run In Your Own Account (RIYOA) are within Instaclustr's PCI boundary.
4. PCI clusters are restricted to TLS 1.2.
5. Instaclustr's PCI accreditation covers Instaclustr services only and requires that our customers implement certain measures as detailed in the PCI Responsibilities Matrix.

Account Definitions

Cluster User:

This refers to an account to log into the cluster

- Instaclustr creates a default cluster user for each cluster. Although cluster users can possess various permission levels, the default user essentially functions as a super user, with the ability to perform all application-specific operations.

Instaclustr Account:
This refers to the console account that maintains ownership over clusters and various other settings, such as billing.

Instaclustr User:
This term describes an individual who can log into the console and may have access to any number of accounts, from none to many.

Provider Account:
The account that we provision into in the cloud provider's system.

Service Users:
Service Users are a type of user specifically designed for system access to Instaclustr APIs and the Terraform Provider.

Core Customer Responsibilities

1. Customers have PCI compliant account settings enabled and have the PCI add-on enabled for each applicable cluster.
2. Customers must ensure **Primary Account Numbers** (PAN) are encrypted before submission to the Instaclustr service.
3. Customers must not provide PAN data to Instaclustr via any method other than direct submission to a cluster.
4. Customers must accept maintenance windows required to apply patches and other fixes within mandated timeframes. Wherever possible, these patches will be applied without service downtime.
5. Customers are responsible for configuring firewall rules in the Instaclustr console, ensuring clusters are accessible only from pre-identified, controlled IP ranges.
6. Firewall rules must exclusively be configured through the Instaclustr console.

PCI Responsibilities Matrix:

Run In Instaclustr Account (RIIA)

The following matrix provides an overview of activities undertaken by Instaclustr and identifies requirements that our customers must fulfil to ensure full PCI compliance of selected Instaclustr Services. It supports our customers in their own PCI compliance activities.

PCI Section	Requirement	Instaclustr	Customer
1	Install and maintain a firewall configuration to protect cardholder data	• Design, document, and implement firewall configuration for Instaclustr management network • Design, document, and implement firewall configurations for customer cluster • Monitor firewall rules for conformance with design • Maintain network diagrams for Instaclustr management networks • Maintain templates for customer clusters • Ensure that management connections do not allow access from wireless and untrusted networks and the Internet • Ensure that no mobile devices can access the Instaclustr production environment	• Provision application in AWS or GCP • Design, document, and implement firewall configurations for application (including firewall rules in the Instaclustr console) (PCI 1.1.2) • Create and maintain a DMZ between Instaclustr cluster and untrusted and wireless networks (PCI 1.3.1, 1.3.2) • Ensure that Firewall rules do not allow direct public access from the internet. (PCI 1.4.1) • Ensure that personal firewalls are installed in accordance with PCI 1.5.1 • Maintain all documentation related to firewall rule decisions
2	Do not use vendor-supplied defaults for system passwords and other security parameters	• Ensure that default passwords are not used in the Instaclustr network • Design and implement hardening standards throughout the Instaclustr network	• Ensure that default passwords are not used in the customer network (PCI 2.2.2)

PCI Section	Requirement	Instaclustr	Customer
2 (continued)		• Implement VPN and SSH for all communications to the Instaclustr production networks	
3	Protect stored cardholder data	• Instaclustr does not make any claims with respect to this PCI section	• Ensure that all PANs are encrypted prior to being stored or processed by an Instaclustr service • Ensure that PAN is only submitted directly to a cluster. Specifically, customers will not email or submit to the Instaclustr support portal • Ensure that all aspects of this family are addressed within the context of the above requirements (PCI 3) For Kafka Customers using Karapace Schema Registry (that is also used by the Cassandra Debezium connector): • Please note that the PCI certification for Karapace Schema Registry covers metadata only, therefore no sensitive data should be included in the schema.

PCI Section	Requirement	Instaclustr	Customer
4	Encrypt transmission of cardholder data across open, public networks	• Instaclustr does not have access to Cardholder data (CHD) in an unencrypted format • Instaclustr has implemented data spill procedures for the case that CHD is unintentionally provided in an unencrypted format	• Ensure that all PANs are encrypted prior to being stored or processed by an Instaclustr service • Ensure that PAN is only submitted directly to a cluster. Specifically, customers will not email or submit PAN to the Instaclustr support portal • Ensure that all aspects of this family are addressed within the context of the above requirements (PCI 4)
5	Protect all systems against malware and regularly update anti-virus software or programs	• Instaclustr implemented appropriate antimalware measures for the Instaclustr environment	• No actions required for Instaclustr clusters
6	Develop and maintain secure systems and applications	• Instaclustr maintains a documented responsibility matrix for assigned roles and responsibilities. Assigned individuals have a comprehensive understanding of their roles and responsibilities. • Instaclustr has integrated finding and addressing vulnerabilities into our build and release process • The Instaclustr release process does not move software from the preproduction environment into the production environment	• As per 6.1.2, customers are responsible for ensuring documentation and assigning roles and responsibilities. Roles and responsibilities must be understood by the assigned personnel. • Customers must ensure that their cluster and schema designs do not allow development, test, and/or custom application accounts, user IDs, and passwords to be used in their production environment (PCI 6.5.6)

PCI Section	Requirement	Instaclustr	Customer
6 (continued)		• Instaclustr reviews all custom code for security vulnerabilities • Instaclustr has implemented change control measures to meet PCI 6.5.1 • Instaclustr trains developers in secure coding techniques and develops applications based on security coding guidelines • Instaclustr has implemented appropriate defences for our customer console • Instaclustr has implemented appropriate security policies and operational procedures	• Customers must ensure that live PANs are not used in clusters designated for testing or development (PCI 6.5.5)
7	Restrict access to cardholder data by business need to know	• Instaclustr has implemented access control procedures for Instaclustr access to customer and management environments • Instaclustr provides a single cluster administrator user via the Console, with permissions to create and manage users within the customer environment	• Customers must design an appropriate Instaclustr account and role scheme to limit access to their clusters to only those individuals whose job requires such access • Customers are responsible for managing users that are granted management access to clusters through the Instaclustr console

PCI Section	Requirement	Instaclustr	Customer
8	Identify and authenticate access to system components	**Users in the Instaclustr Console and Support Portal:** • Instaclustr has implemented access control systems for Instaclustr access to customer and management environments that are compliant with PCI section 8 • 8.3.10.1, 8.4.2 Insatclustr enforces MFA and rotation of the password once in every 90 days. **For Customer Accounts:** • Instaclustr accounts without Single Sign-On (SSO) enabled are compliant with PCI section 8. It is the customers' responsibility to ensure their SSO-enabled Instaclustr users are in compliance with this section. • When a customer opts to enable SSO on their account: ▪ Owner users are complaint with PCI section 8 ▪ It's the customers' responsibility to ensure that "non-owner" users comply with PCI sect. 8	• Customers must design an appropriate account and role scheme to limit access to their clusters to only those individuals whose job requires such access **Accounts in the Instaclustr Console and Support Portal:** • If a customer chooses to enable SSO user authentication through a custom Identity Provider for their Instaclustr account, they are then responsible for implementing the following requirements in their IdP: ▪ 8.2.5 Immediately revoke access for any terminated users ▪ 8.2.6 Remove/disable inactive user accounts within 90 days ▪ 8.3.4 Limit repeated access attempts by locking out the user ID after not more than 6 attempts Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

PCI Section	Requirement	Instaclustr	Customer
8 (continued)		▪ If Kibana is enabled on a customer's OpenSearch cluster, then Kibana user authentication/ authorization is enforced via the customer's OpenID Connect compliant 3rd party identity provider. (Note: OpenSearch dashboards as the Kibana equivalent for OpenSearch clusters) **Users in Instaclustr Clusters:** • Cluster users, which are unique within each cluster, are categorized as Service Accounts. These service cluster users are not required to meet the criteria laid out in PCI Requirements 8.2.6, 8.2.7, 8.3.4, 8.2.8, 8.3, and 8.4.	▪ 8.3.3 Verify user identity before modifying any authentication credential ▪ 8.3.6 Passwords must require a minimum length of at least 12 characters and contain both numeric and alphabetic characters ▪ 8.3.9 Change user passwords/passphrases at least every 90 days ▪ 8.3.7 Do not allow an individual to submit a new password/phrase that is the same as any of the last 4 passwords/ phrases he or she has used. ▪ 8.4 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication • If a customer chooses to link their Instaclustr account with users using unmanaged SSO Instaclustr users, then they are responsible for the following requirements on each user's IdP: 8.3.4, 8.3.3, 8.3.6, 8.3.9, 8.3.7, 8.4. Customers should check whether the proposed IdP can meet these requirements before allowing non-managed IdPs to provide authentication services.

PCI Section	Requirement	Instaclustr	Customer
8 (continued)			**Users in Instaclustr Clusters:** • Customers should note that Cluster users are considered System Accounts for the purposes of PCI, and are not subject to the usual limitations under PCI section 8, e.g. there are no technically enforced minimum password requirements • Customers must implement appropriate procedures to manage service users • If Kibana is enabled on a customer OpenSearch cluster, the following PCI requirements must be met by the customer via their OpenID Connect compliant 3rd party identity provider: ▪ 8.2.5 Immediately revoke access for any terminated users ▪ 8.2.6 Remove/disable inactive user accounts within 90 days ▪ 8.3.4 Limit repeated access attempts by locking out the user ID after not more than 6 attempts ▪ 8.3.4 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID ▪ 8.3.3 Verify user identity before modifying any authentication credential

PCI Section	Requirement	Instaclustr	Customer
8 (continued)			▪ 8.3.6 Passwords must require a minimum length of at least 12 characters and contain both numeric and alphabetic characters ▪ 8.3.9 Change user passwords/passphrases at least every 90 days ▪ 8.3.7. Do not allow an individual to submit a new password/phrase that is the same as any of the last 4 passwords/phrases he or she has used ▪ 8.4.1 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication **For Customers with Cadence PCI:** **The Cadence Web application does not support authentication and authorization**. Within PCI-compliant clusters, the Cadence Web application is only accessible from a customer's private network. Instaclustr users are not able or permitted to access the Web application. It is the customer's responsibility to manage access to Cadence Web using network layer controls.

PCI Section	Requirement	Instaclustr	Customer
9	Restrict physical access to cardholder data	• As a cloud-based service, Instaclustr requires all Primary Account Numbers (PANs) to be encrypted before they are processed or stored in a cluster. Most requirements are therefore met by AWS or GCP for physical protection of encrypted PAN, or the customer for their own environments • Instaclustr has implemented compliance visitor processes for offices that usually host technical operations staff	• Customers should review all of Section 9 with respect to access to PAN using AWS or GCP PCI ROCs as an input
10	Track and monitor all access to network resources and cardholder data	• Instaclustr has implemented logging for Instaclustr administrator actions	• Customers must implement logging in their application to track their access to their cluster (PCI 10.2.1)
11	Regularly test security systems and processes	• Instaclustr performs appropriate internal, external, and ASV scans of Instaclustr management infrastructure and customer environments • Instaclustr engages with independent penetration testers who conduct testing in line with industry accepted standards • Vulnerabilities are managed as part of our development and release process, regardless of how Instaclustr becomes aware of them	• No action required for Instaclustr clusters

PCI Section	Requirement	Instaclustr	Customer
11 (continued)		• All Instaclustr customer environments are implemented in separate VPCs, distinct from the management environment VPC, thus ensuring appropriate segmentation. This holds true for all platforms, including AWS and GCP • Instaclustr uses intrusion detection systems and process whitelisting to ensure that the Technical Operations team is alerted to potential compromises • Instaclustr has deployed a change detection system across critical files • Instaclustr has implemented a process to deal with alerts from monitoring systems	

PCI Section	Requirement	Instaclustr	Customer
12	Maintain a policy that addresses information security for all personnel	• Instaclustr has established and published a Security policy. The security policy is maintained and disseminated • Instaclustr has implemented a risk management process • Instaclustr has developed acceptable usage policies • The security policy defines responsibilities, and assigns security management to the Instaclustr Director of Information Security • Instaclustr has a formal security training program • Instaclustr implemented a process to manage service providers with potential access to encrypted PAN • Instaclustr has implemented an IR plan with respect to potential PAN data spills	Customers should email support@instaclustr.com to report any suspected security breach

PCI Responsibilities Matrix:
Run In Your Own Account (RIYOA)

PCI Section	Requirement	Instaclustr	Customer
1	Install and maintain a firewall configuration to protect cardholder data	• Design, document, and implement firewall configuration for Instaclustr management network • Design, document, and implement firewall configurations for customer cluster • Monitor firewall rules for conformance with design • Maintain network diagrams for Instaclustr management networks • Maintain template diagrams for customer clusters • Ensure that management connections do not allow access from wireless and untrusted networks and the Internet • Ensure that no mobile devices can access the Instaclustr production environment	• Customers must not make any changes to security groups directly. All changes must be made using the Instaclustr console • Provision application in AWS or GCP • Design, document, and implement firewall configurations for application (including firewall rules in the Instaclustr console) (PCI 1.1.2) • Create and maintain a DMZ between Instaclustr cluster, and untrusted and wireless networks (PCI 1.3.1, 1.3.2) • Ensure that firewall rules do not allow direct public access from the internet (PCI 1.4.1) • Ensure that personal firewalls are installed in accordance with PCI 1.5.1 • Maintain all documentation related to firewall rule decisions

PCI Section	Requirement	Instaclustr	Customer
2	Do not use vendor-supplied defaults for system passwords and other security parameters	• Ensure that default passwords are not used in the Instaclustr network • Design and implement hardening standards throughout the Instaclustr network • Implement VPN and SSH for all communications to the Instaclustr production networks	• Ensure that default passwords are not used in the customer network (PCI 2.2.2) • Ensure that accounts in your cloud account are compliant with PCI section 2
3	Protect stored cardholder data	• Instaclustr does not make any claims with respect to this PCI family	• Ensure that all Primary Account Numbers (PANs) are encrypted prior to being stored or processed by an Instaclustr service • Ensure that PAN is only submitted directly to a cluster. Specifically, customers will not email or submit CHD to the Instaclustr support portal • Ensure that all aspects of this family are addressed within the context of the above requirements (PCI 3) For Kafka Customers using Karapace Schema Registry that is also used by the Cassandra Debezium connector): • Please note that the PCI certification for Karapace Schema Registry covers metadata only, therefore no sensitive data should be included in the schema. .

PCI Section	Requirement	Instaclustr	Customer
4	Encrypt transmission of cardholder data across open, public networks	• Instaclustr does not have access to PAN in an unencrypted format • Instaclustr has implemented data spill procedures for the case that PAN is unintentionally provided in an unencrypted format	• Ensure that all PANs are encrypted prior to being stored or processed by an Instaclustr service • Ensure that PAN is only submitted directly to a cluster. Specifically, customers will not email or submit PAN to the Instaclustr support portal • Ensure that all aspects of this family are addressed within the context of the above requirements (PCI 4)
5	Protect all systems against malware and regularly update anti-virus software or programs	• Instaclustr implemented appropriate antimalware measures for the Instaclustr environment	• No actions required for Instaclustr clusters
6	Develop and maintain secure systems and applications	• Instaclustr maintains a documented responsibility matrix for assigned roles and responsibilities. Assigned individuals have a comprehensive understanding of their roles and responsibilities. (6.1.2) • Instaclustr has integrated finding and addressing vulnerabilities into our build and release process • The Instaclustr release process does not move software from the preproduction environment into the production environment	• As per 6.1.2, customers are responsible for ensuring documentation and assigning roles and responsibilities. Roles and responsibilities must be understood by the assigned personnel. • Customers must ensure that their cluster and schema designs do not allow development, test, and/or custom application accounts, user IDs, and passwords to be used in their production environment (PCI 6.5.6)

PCI Section	Requirement	Instaclustr	Customer
6 (continued		• Instaclustr reviews all custom code for security vulnerabilities • Instaclustr has implemented change control measures to meet PCI 6.5.1 • Instaclustr trains developers in secure coding techniques and develops applications based on security coding guidelines • Instaclustr has implemented appropriate defences for our customer console • Instaclustr has implemented appropriate security policies and operational procedures	• Customers must ensure that live PANs are not used in clusters designated for testing or development (PCI 6.5.5)

PCI Section	Requirement	Instaclustr	Customer
7	Restrict access to cardholder data by business need to know	• Instaclustr has implemented access control procedures for Instaclustr access to customer and management environments • Instaclustr provides a single cluster administrator account via the console, with permissions to create and manage users within the customer environment	• Customers must design an appropriate account and role scheme to limit access to their clusters and cloud accounts to only those individuals whose job requires such access • Customers are responsible for managing users that are granted management access to clusters through the Instaclustr console
8	Identify and authenticate access to system components	**Users in the Instaclustr Console and Support Portal:** • Instaclustr has implemented access control systems for Instaclustr access to customer and management environments that are compliant with PCI section 8 **For Customer Accounts:** • Instaclustr accounts without Single Sign-On (SSO) enabled are compliant with PCI section 8. It's the customers' responsibility to ensure their SSO-enabled Instaclustr users are in compliance with this section • 8.3.10.1,8.4.2 Instaclustr enforces MFA and rotation of the password once in every 90 days.	• Customers must design an appropriate account and role scheme to limit access to their clusters to only those individuals whose job requires such access **Customer Cloud Provider Accounts:** • Customers must design and implement appropriate identification and authentication controls in their provider accounts • Customers must not add new instances or services into their cluster VPC **Accounts in the Instaclustr Console and Support Portal:** • If a customer chooses to enable SSO on their account, they are then responsible for implementing the following requirements in their IdP: ▪ 8.2.5 Immediately revoke access for any terminated users

PCI Section	Requirement	Instaclustr	Customer
8 (continued)		• When a customer opts to enable SSO on their account: ▪ "Owner" users comply with PCI section 8 ▪ It's the customers' responsibility to ensure that "non-owner" users comply with PCI sect. 8 **Users in Instaclustr Clusters:** Cluster users, which are unique within each cluster, are categorized as Service Accounts. These service cluster users are not required to meet the criteria laid out in PCI Requirements 8.2.6, 8.2.7, 8.3.4, 8.3.4, 8.2.8, 8.2, and 8.4.1. If a customer decides to link their Instaclustr account with users using unmanaged Single Sign-On (SSO) user accounts, they assume responsibility for ensuring the following requirements on each user's Identity Provider (IdP): 8.3.4, 8.3.4, 8.3.3, 8.3.6, 8.3.9, 8.3.7, 8.4.1. Prior to permitting non-managed IdPs to provide authentication services, customers should verify whether the proposed IdP can fulfil these requirements	▪ 8.2.6 Remove/disable inactive user accounts within 90 days ▪ 8.3.4 Limit repeated access attempts by locking out the user ID after not more than 6 attempts ▪ 8.3.4 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID ▪ 8.3.3 Verify user identity before modifying any authentication credential ▪ 8.3.6 Passwords must require a minimum length of at least 12 characters and contain both numeric and alphabetic characters ▪ 8.3.9 Change user passwords/passphrases at least every 90 days ▪ 8.3.7 Do not allow an individual to submit a new password/phrase that is the same as any of the last 4 passwords / phrases he/she has used ▪ 8.4.1 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication

PCI Section	Requirement	Instaclustr	Customer
8 (continued)			**Users in Instaclustr Clusters:** • Customers should note that cluster users are considered System Accounts for the purposes of PCI, and are not subject to the usual limitations under PCI section 8, e.g. there are no technically enforced minimum password requirements. • Customers must implement appropriate procedures to manage service users • If Kibana is enabled on a customer OpenSearch cluster, the following PCI requirements must be met by the customer via their OpenID Connect compliant 3rd party identity provider: ▪ 8.2.5 Immediately revoke access for any terminated users ▪ 8.2.6 Remove/disable inactive user accounts within 90 days ▪ 8.3.4 Limit repeated access attempts by locking out the user ID after not more than 6 attempts ▪ 8.3.4 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID ▪ 8.3.3 Verify user identity before modifying any authentication credential

PCI Section	Requirement	Instaclustr	Customer
8 (continued)			▪ 8.3.6 Passwords must require a minimum length of at least 12 characters and contain both numeric and alphabetic characters ▪ 8.3.9 Change user passwords/ passphrases at least every 90 days ▪ 8.3.7 Do not allow an individual to submit a new password/phrase that is the same as any of the last 4 passwords/phrases he or she has used ▪ 8.4.1 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. **For Customers with Cadence PCI:** **The Cadence Web application does not support authentication and authorization**. Within PCI-compliant clusters, the Cadence Web application is only accessible from a customer's private network. Instaclustr users are not able or permitted to access the Web application. It is the customer's responsibility to manage access to Cadence Web using network layer controls.

PCI Section	Requirement	Instaclustr	Customer
9	Restrict physical access to cardholder data	• As a cloud-based service, Instaclustr requires all PANs to be encrypted before they are processed or stored in a cluster. Most requirements are therefore met by AWS or GCP for physical protection of encrypted PAN, or the customer for their own environments. Instaclustr has implemented compliance visitor processes for offices that usually host Technical Operations staff	• Customers should review all of Section 9 with respect to access to PAN using AWS or GCP PCI ROCs as an input
10	Track and monitor all access to network resources and cardholder data	• Instaclustr has implemented logging for Instaclustr administrator actions	• Customers must implement logging in their application to track their access to their cluster (PCI 10.2.1)

PCI Section	Requirement	Instaclustr	Customer
11	Regularly test security systems and processes	• Instaclustr performs appropriate internal, external, and ASV scans of Instaclustr management infrastructure and customer environments • Instaclustr engages with independent penetration testers who conduct testing in line with industry accepted standards • Vulnerabilities are managed as part of our development and release process regardless of how Instaclustr becomes aware of them • All Instaclustr customer environments are implemented in separate Virtual Private Clouds (VPCs), distinct from the management environment VPC, thus ensuring appropriate segmentation. This holds true for all platforms, including AWS and GCP Instaclustr uses Intrusion detection systems and process whitelisting to ensure that the Technical Operations team is alerted to potential compromises • Instaclustr has deployed a change detection system across critical files • Instaclustr has implemented a process to deal with alerts from monitoring systems	• No actions required for Instaclustr clusters

PCI Section	Requirement	Instaclustr	Customer
12	Maintain a policy that addresses information security for all personnel	• Instaclustr has established and published a Security policy. The security policy is maintained and disseminated • Instaclustr has implemented a risk management process • Instaclustr has developed acceptable usage policies • The security policy defines responsibilities, and assigns security management to the Instaclustr Director of Information Security • Instaclustr has a formal security training program • Instaclustr implemented a process to manage service providers with potential access to encrypted PAN • Instaclustr has implemented an IR plan with respect to potential PAN data spills	• Customers should email support@instaclustr.com to report any suspected security breach • Customers must design and implement appropriate security controls for their cloud account

6-09jul24