instaclustr

PCI Responsibilities

Updated: 11 November, 2020

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. Cassandra and Kafka are able to be provisioned in a PCI Configuration.
2. Only clusters in AWS are supported at this time.
3. Both Run In Instaclustr's Account (RIIA) and Run In Your Own Account (RIYOA) are within our 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 some aspects to ensure compliance of our service.

Core Customer Responsibilities

1. Customers must opt-in to receive PCI accredited clusters.
2. Customers must encrypt CHD prior to it being submitted to the Instaclustr service.
3. Customers must not provide CHD 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 time frames. Wherever possible, these patches will be applied without service downtime.
5. Customers must ensure that firewall rules are configured in the Instaclustr console such that clusters are only accessible from known, controlled IP ranges.
6. Customers must only configure firewall rules 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 • Design, document, and implement firewall configurations for application (including firewall rules in the Instaclustr console) (PCI 1.1) • Create and maintain a DMZ between Instaclustr cluster and untrusted and wireless networks (PCI 1.2) • Ensure that Firewall rules do not allow direct public access from the internet. (PCI 1.3) • Ensure that personal firewalls are installed in accordance with PCI 1.4 • 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 2.1)

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 family	• Ensure that all CHD is encrypted prior to being stored or processed by an Instaclustr service • Ensure that CHD 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)
4	Encrypt transmission of cardholder data across open, public networks	• Instaclustr does not have access to 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 CHD is encrypted prior to being stored or processed by an Instaclustr service • Ensure that CHD 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 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

PCI Section	Requirement	Instaclustr	Customer
6	Develop and maintain secure systems and applications	• 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 • Instaclustr reviews all custom code for security vulnerabilities • Instaclustr has implemented change control measures to meet PCI 6.4 • 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 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 6.3.1, 6.4.4 • Customers must ensure that live PANs are not used in clusters designated for testing or development (PCI 6.4.3)
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	• Customers must design an appropriate account and role scheme to limit access to their clusters to only those individuals whose job requires such access

PCI Section	Requirement	Instaclustr	Customer
7 (continued)		• Instaclustr provides a single cluster administrator account via the Console, with permissions to create and manage users within the customer environment	• 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	• Instaclustr has implemented access control systems for Instaclustr access to customer and management environments that are compliant with PCI section 8 • For Customer accounts: ▪ Accounts without SSO enabled for the Instaclustr Console are compliant with PCI section 8 ▪ If a customer chooses to enable SSO on their account, ◆ Owner users are compliant with PCI section 8 ◆ Customers are responsible for ensuring non-owner users are compliant with PCI section 8 • Customer cluster accounts (Service Accounts) are unique within a cluster. Service accounts are not required to meet, and do not meet, the PCI Requirements 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.3	• Customers must design an appropriate account and role scheme to limit access to their clusters to only those individuals whose job requires such access • Customers should note that cluster accounts 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 accounts • If a customer chooses to enable SSO on their account, they are then responsible for implementing the following requirements in their IdP : ▪ 8.1.3 Immediately revoke access for any terminated users. ▪ 8.1.4 Remove/disable inactive user accounts within 90 days

PCI Section	Requirement	Instaclustr	Customer
8 (continued)			▪ 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts ▪ 8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID ▪ 8.2.2 Verify user identity before modifying any authentication credential ▪ 8.2.3 Passwords must require a minimum length of at least seven characters and contain both numeric and alphabetic characters ▪ 8.2.4 Change user passwords/passphrases at least every 90 days ▪ 8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. ▪ 8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication

PCI Section	Requirement	Instaclustr	Customer
9	Restrict physical access to cardholder data	• Instaclustr is cloud based, and all CHD is required to be encrypted prior to being processed or stored in a cluster. Most requirements are therefore met by AWS for physical protection of encrypted CHD, 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 CHD using AWS PCI ROCs as an input
10	Track and monitor all access to metwork 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 Section 10
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	• No actions required for Instaclustr clusters

PCI Section	Requirement	Instaclustr	Customer
11 (continued)		implemented in separate VPCs, and a separate VPC to the management environment, ensuring appropriate segmentation • 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	
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 VP Security Risk and Compliance • Instaclustr has a formal security training program • Instaclustr implemented a process to manage service providers with potential access to encrypted CHD	Customers should email support@instaclustr.com to report any suspected security breach

PCI Section	Requirement	Instaclustr	Customer
12 (continued)		- Instaclustr has implemented an IR plan with respect to potential CHD data spills	

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 - Design, document, and implement firewall configurations for application (including firewall rules in the Instaclustr console) (PCI 1.1) - Create and maintain a DMZ between Instaclustr cluster, and untrusted and wireless networks (PCI 1.2) - Ensure that firewall rules do not allow direct public access from the internet (PCI 1.3) - Ensure that personal firewalls are installed in accordance with PCI 1.4 - 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 2.1) • 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 CHD is encrypted prior to being stored or processed by an Instaclustr service • Ensure that CHD 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)
4	Encrypt transmission of cardholder data across open, public networks	• Instaclustr does not have access to 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 CHD is encrypted prior to being stored or processed by an Instaclustr service • Ensure that CHD 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 4)

PCI Section	Requirement	Instaclustr	Customer
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 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 • Instaclustr reviews all custom code for security vulnerabilities • Instaclustr has implemented change control measures to meet PCI 6.4 • 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 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 6.3.1, 6.4.4) • Customers must ensure that live PANs are not used in clusters designated for testing or development (PCI 6.4.3)

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	• Instaclustr has implemented access control systems for Instaclustr access to customer and management environments that are compliant with PCI section 8 • For Customer accounts: ▪ Customer accounts without SSO enabled for the Instaclustr Console are compliant with PCI section 8 ▪ If a customer chooses to enable SSO on their account ♦ Owner users are compliant with PCI section 8. ♦ Customers are responsible for ensuring non-owner users are compliant with PCI section 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 • Customers should note that cluster accounts 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 accounts • Customers must design and implement appropriate identification and authentication controls in their cloud accounts • Customers must not add new instances or services into their cluster VPC

PCI Section	Requirement	Instaclustr	Customer
8 (continued)		- Customer cluster accounts (Service Accounts) are unique within a cluster. Service accounts are not required to meet, and do not meet, the PCI Requirements 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.3	- If a customer chooses to enable SSO on their account, they are then responsible for implementing the following requirements in their IdP : ▪ 8.1.3 Immediately revoke access for any terminated users. ▪ 8.1.4 Remove/disable inactive user accounts within 90 days ▪ 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts. ▪ 8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. ▪ 8.2.2 Verify user identity before modifying any authentication credential. ▪ 8.2.3 Passwords must require a minimum length of at least seven characters and contain both numeric and alphabetic characters. ▪ 8.2.4 Change user passwords/phrases at least every 90 days ▪ 8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four pass-

PCI Section	Requirement	Instaclustr	Customer
8 (continued)			words/phrases he or she has used - 8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.
9	Restrict physical access to cardholder data	- Instaclustr is cloud based, and all CHD is required to be encrypted prior to being processed or stored in a cluster. Most requirements are therefore met by AWS for physical protection of encrypted CHD, 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 CHD using AWS 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 Section 10
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	- No actions required for Instaclustr clusters

PCI Section	Requirement	Instaclustr	Customer
11 (continued)		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 VPCs, and a separate VPC to the management environment, ensuring appropriate segmentation • 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	
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-	• Customers should email support@instaclustr.com to report any suspected security breach • Customers must design and implement appropriate security controls for their cloud account

PCI Section	Requirement	Instaclustr	Customer
12 (continued)		management to the VP Security Risk and Compliance • Instaclustr has a formal security training program • Instaclustr implemented a process to manage service providers with potential access to encrypted CHD • Instaclustr has implemented an IR plan with respect to potential CHD data spills	