- CDE systems that process, store, or transmit CHD
- Systems that support CDE systems and components through controlled access
- Out-of-scope systems that are isolated from all CDE systems and components

As it defines the CDE's scope, this material may be essential in the proper understanding of the Oracle PCA X9-2 software-defined network (SDN) and microsegmentation implementation, which is a fundamental best practice of PCI DSS design. When properly implemented and tested, segmentation may be useful for reducing the scope of a PCI DSS assessment; however, PCI SSC guidance states that "implementing segmentation is no replacement for a holistic approach to securing an organization's infrastructure," (PCI SSC, 2017). Many CHD breaches have been linked to out-of-scope systems where the attacker uses the out-of-scope system to gain leverage and pivot on the payment entity's network until an access point to the CDE can be found.

## Service providers, designated entities, and shared PCI DSS responsibility

PCI DSS makes provisions for payment industry entities to use service providers to store, process, or transmit CHD on behalf of the payment entity or to manage components such as routers, firewalls, databases, physical security, or servers. CHD security is impacted in the course of providing services to payment industry entities, and, therefore, such service providers are responsible for compliance with PCI DSS. This is also true of shared service providers who provide services to multiple payment entities. Requirements under section 12.8 of PCI DSS 3.2.1 are focused on managing "service providers with whom CHD is shared, or that could affect the security of CHD" (PCI DSS 3.2.1 Standard). Service provider requirements in addition to PCI DSS requirements are listed in Appendix A1 of PCI DSS 3.2.1. This white paper and the accompanying workbook may be useful for service providers using or planning to use ***Oracle PCA X9-2*** as a platform for delivering services where CHD is stored, processed, or transmitted.

This white paper and the supplemental workbook may also be useful where a designated entity's ***Oracle PCA X9-2*** instances are involved with the storage, processing, or transmission of CHD. Designated entities constitute an additional category of entity for which PCI DSS 3.2.1 is applicable. A designated entity may be any payment entity, including merchants or service providers, that a payment brand or acquirer determines requires additional supplemental validation of existing PCI DSS requirements. Examples of designated entities include those storing, processing, or transmitting large volumes of CHD; those providing aggregation points for CHD; or those who have suffered significant or repeated CHD breaches. Additional requirements for designated entities are found in Appendix A3 of PCI DSS 3.2.1.

## PCI DSS qualified security assessors

This white paper and supporting materials may be useful to assist a PCI DSS QSA in evaluating an implementation of ***Oracle PCA X9-2*** during assessment activities that contribute to their Report on Compliance (ROC) or their Self-Assessment Questionnaire (SAQ). In the supplemental controls workbook of this report, Coalfire aligns the technical controls referenced in PCI DSS 3.2.1 with findings for how ***Oracle PCA X9-2*** provides controls that can meet those requirements. Additionally, a designation of origination of control is provided with commentary on how the systems integrator would implement appropriate controls. Where applicable, Coalfire references the additional implementation steps documented in this PAG to be performed by the customer when deploying and supporting a PCI DSS compliance program. Other products have been used in conjunction with the built-in ***Oracle PCA X9-2*** resources to meet the PCI DSS requirements fully, and Coalfire notes those products, such as customer edge firewalls to secure the boundary between the untrusted network (internet) and the internal, trusted networks, where applicable.

The guidance in this white paper and supporting materials are intended to provide Coalfire's opinion and are not meant to supplant or compromise the independent judgment required to perform PCI DSS assessments. The PCI SSC Code of Professional Responsibility requires QSA companies and employees to "adhere to high standards of ethical and professional conduct" (PCI Security Standards Council, LLC, 2014). Coalfire supports and upholds independent QSA judgments that might differ from this opinion.

### Objectives of this white paper

This white paper's primary objective is to render an opinion on ***Oracle PCA X9-2's*** suitability to assist merchants with meeting the requirements of PCI DSS 3.2.1 using a particular use case detailed below and in the subsequent sections. The following process is intended to illustrate Coalfire's findings and satisfy these objectives:

- Choose a likely and relevant use case for an ***Oracle PCA X9-2*** payment card infrastructure.
- Show a possible configuration used for many likely merchant and processor scenarios.
- Analyze ***Oracle PCA X9-2's*** platform and features using practices identical to an actual payment card assessment and guidance provided in QSA reactions.
- Evaluate the key features of ***Oracle PCA X9-2*** per control for their ability to support the requirements.
- Make relevant observations and recommendations about each control family and the suggested implementation approaches for ***Oracle PCA X9-2*** features to support meeting the objectives of these controls.
- State Coalfire's opinion.

This white paper also contains a representative overview of many aspects of the PCI DSS process and practices. This white paper's secondary objective is to inform a newcomer to PCI DSS 3.2.1 about a technical approach to using hyperconverged infrastructure to construct an infrastructure architecture able to host a compliant payment card workload.

Since the ***Oracle PCA X9-2*** platform's review was not being conducted on an actual payment card entity running a real-world merchant or service provider workload, Coalfire focused on the technical controls for PCI DSS 3.2.1. Coalfire did not review organizational processes, training, procedures, written supporting materials, or other non-technical controls called for in PCI DSS 3.2.1. The customer is responsible for PCI DSS processes, such as organizational, procedural, and training controls, that pertain to implementation by a real payment card entity.

Coalfire uses the term "notional" to denote the presence of such non-technical controls that may be required to support or enable the technical controls that Coalfire is evaluating. For example, PCI DSS 3.2.1 controls used to "build and maintain a secure network and systems" and "1.1 Establish and implement firewall and router configuration standards that include the following: 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations…" (PCI DSS, 2018) are notional. These requirements underpin technical controls such as 1.1.1.c and 1.1.2.a.

# Oracle PCA X9-2

Oracle PCA X9-2 is engineered to deliver a comprehensive suite of cloud infrastructure services within the secure environment of a customer's on-premises network. The system integrates all required hardware and software components and has been tested, configured, and tuned for optimal performance by Oracle engineers. It is a flexible, general-purpose, infrastructure-as-a-service (IaaS) solution that supports a wide variety of workloads. Oracle PCA X9-2's pluggable platform provides a foundation to layer platform-as-a-service (PaaS) and software-as-a-service (SaaS) solutions on top of the infrastructure.

This release of Oracle PCA X9-2 provides application programming interface (API) compatibility with Oracle's public cloud solution, Oracle Cloud Infrastructure (OCI). Customer's access the core IaaS services using the same methods, tools, and interfaces as OCI. An installation of Oracle PCA X9-2 represents a customer region. Workloads are portable between a customer's private and public cloud environments, but the private cloud is disconnected from OCI and, thus, runs its own control plane components in order to host its set of compatible services.

As an engineered system, Oracle PCA X9-2 complies with the highest business continuity and serviceability requirements. It has the capability to monitor all components, detect potential problems, send out alerts, and automatically log a service request. Subsequent troubleshooting and repair can be performed without affecting the uptime of the environment.

System upgrades are designed for minimum disruption and maximum availability. Health checks are performed before an upgrade to ensure that all components are in an acceptable state. The upgrade process is modular and allows components, such as firmware, operating systems, containerized services, or the system's main database, to be upgraded individually or as an integrated multi-component workflow.

## Oracle PCA X9-2 architecture

Customer access to the typical Oracle PCA X9-2 deployment is provided through an external-facing network and an internal management network. This supports better separation of back-end system administration and overall network administration duties.

Figure 1, below, depicts the system architecture of Oracle PCA X9-2, including internal components and external access points.

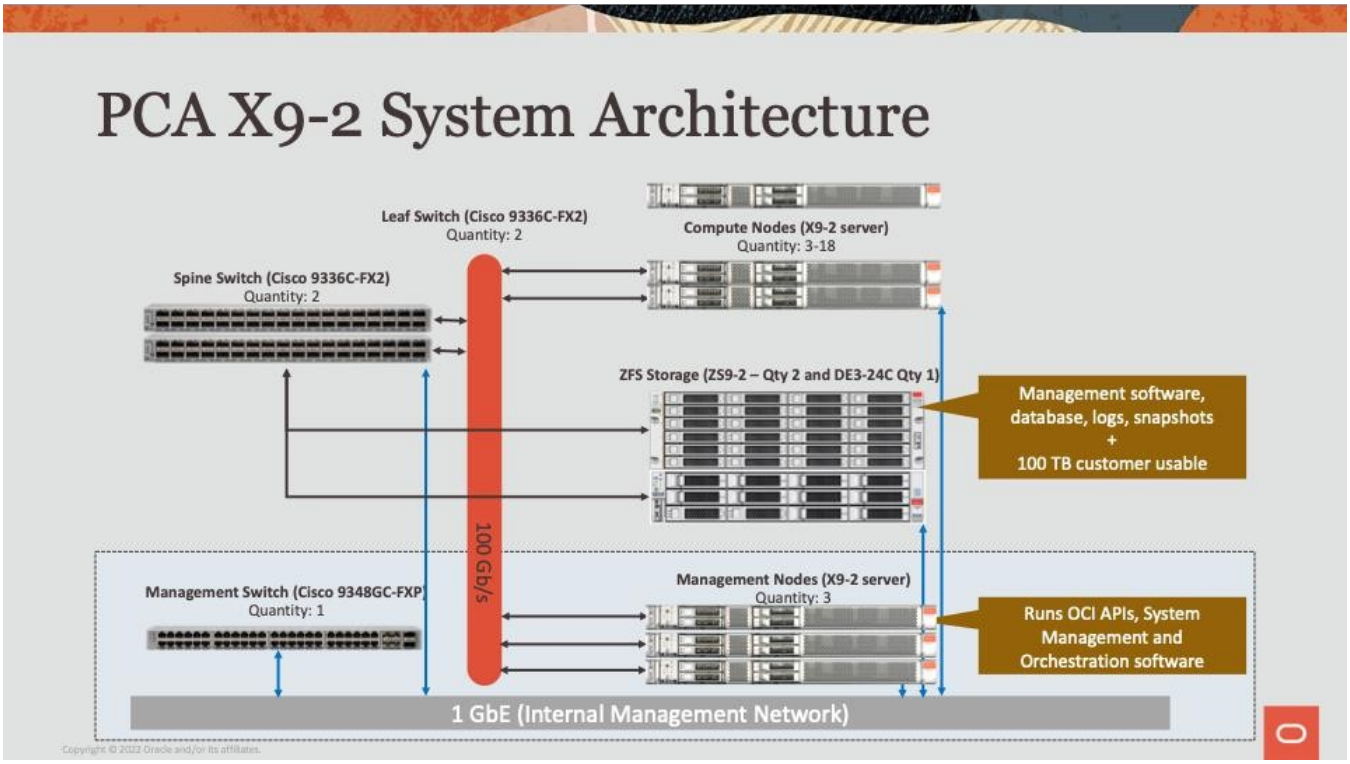


*Figure 1: Oracle PCA X9-2 System Architecture*

## Oracle PCA X9-2 components

The following components are specific to ***Oracle PCA X9-2:***

### Hardware components

- **Oracle server management nodes**:

  The management nodes, running the controller software, provide a foundation for the collection of services responsible for operating and administering Oracle PCA X9-2. Responsibilities of the management cluster include monitoring and maintaining the system hardware, ensuring system availability, upgrading software and firmware, backing up and restoring the appliance, and managing disaster recovery. The part of the system where the appliance infrastructure is controlled is called the Service Enclave, which runs on the management node cluster and can be accessed through the Service Command Line Interface (CLI) or the Service Web UI. Access is closely monitored and restricted to privileged administrators.

  There are three management nodes installed in rack units 5, 6, and 7 that form a cluster for high availability. All servers are capable of running the same controller software and system-level services and have equal access to the system configuration. All three servers manage the system as a fully active cluster.

- **Oracle server compute nodes**:

  The compute nodes in Oracle PCA X9-2 are part of the hardware layer and provide the processing power and memory capacity to host compute instances. Management of the hardware layer is provided by the platform and services layer of the appliance.

  The minimum configuration of the base rack contains three compute nodes but it can be expanded, three nodes at a time, to up to 18 compute nodes, if a customer chooses to use all of the flex bay space for compute nodes. The system can support up to 20 compute nodes total, with two slots reserved for spares that can be requested through an exception process.

- **Oracle ZFS Storage Appliance (ZS9-2)**:

  The Oracle ZFS Storage Appliance is crucial in providing storage space for the Oracle PCA X9-2 software. This component consists of two controller servers installed at the bottom of an appliance rack and disk shelf and fulfills the role of “system disk” for the entire appliance.

- **Oracle Storage Drive Enclosure**:

  The Private Cloud Appliance software automatically adds new storage capacity to the corresponding high-capacity or high-performance storage pools. Customers can optionally increase the storage by adding disk shelves to a system flex bay. The available storage options for expansion are the Oracle Storage Drive Enclosure DE3-24C and the Oracle Storage Drive Enclosure DE3-24P.

- **Cisco 9336CC 100GbE Switch:**

  Appliance data connectivity is built on redundant 100 Gigabit switches in a two-layer design similar to a leaf-spine topology. The leaf switches interconnect the rack hardware components, while the spine switches form the backbone of the network and provide a path for external traffic. Each leaf switch is connected to all the spine switches, which are also interconnected. The main benefits of this topology are extensibility and path optimization. An Oracle PCA X9-2 rack contains two leaf and two spine switches.

- **Cisco 9348GC Management Switch:**

  The device management network provides internal access to the management interfaces of all appliance components. Customers can temporarily connect to the management switch via workstation or a permanent

bastion host via port 2 of the management switch. The management switch provides ethernet connections to Oracle PCA X9-2 hardware components for Integrated Lights Out Manager (ILOM) and management interfaces.

**Software Components**

- **Service Enclave:**

  Because Oracle PCA X9-2 is operationally disconnected from OCI, it needs a control plane of its own, specific to the design and scale of the appliance. The Service Enclave (SE) is the part of the system where the appliance infrastructure is controlled. Access is closely monitored and restricted to privileged administrators. It runs on a cluster of three management nodes.

  Functionality provided by the SE includes hardware and capacity management, service delivery, monitoring, and tools for service and support. An Oracle PCA X9-2 CLI and browser access is provided to customer administrators to manage the Oracle PCA X9-2 system. Services provided by the SE include hardware and system management, monitoring, logging, load balancing, firewalls, load balancers, and identity and access management (IAM).

- **Compute Enclave:**

  The Compute Enclave is where workloads are created, configured, and hosted. The CE provides access to IaaS cloud services via the OCI cloud CLI and a browser user interface. Users of the CE have permissions to create and manage cloud resources, typically based on group membership. The principal building blocks at the users' disposal are compute instances and associated network and storage resources.

  Compute instances are created from a compute image, which contains a pre-installed operating system and optional additional software. Compute instances have a particular shape, which is a template of virtual hardware resources, such as CPUs and memory. A minimal compute instance needs a boot volume and a connection to a virtual cloud network (VCN). As customers continue to build the virtual infrastructure for their workload, they will likely add more compute instances, assign private and public network interfaces, or set up NFS shares or object storage buckets.

# Scope and approach for review

The Oracle PCA X9-2 platform may be used in a variety of likely PCI DSS scenarios. Coalfire Opinion Series PAGs benefit from the careful selection of possible and impactful use cases, highlighting critical areas within a product to evaluate potential for PCI DSS compliance.

## Coalfire evaluation methodology

Coalfire began by examining the PCI DSS 3.2.1 requirements and identifying them as either organizational (non-technical) or technical. A requirement was determined as either procedural or technical based on a review of the requirement's narrative, testing procedures, and guidance.

Organizational requirements include documented policies, procedures, and standards that were not considered directly applicable to the technical solution. Examples of these non-technical requirements include maintaining facility visitor logs, verifying an individual's identity before granting physical or logical access, performing periodic physical asset inventories, generating network drawings of CHD flow diagrams, and other elements that ***Oracle PCA X9-2*** cannot satisfy.

Once identified, technical requirements were then assessed to determine applicability to ***Oracle PCA X9-2*** for the selected use case. If the achievement of the required objectives was more likely to be met using an external and non-adjacent mechanism, the requirement was determined to be notional to the ***Oracle PCA X9-2*** platform and excluded from the use

case. Examples of PCI DSS-related components that Coalfire considered notional and not natively supplied by ***Oracle PCA X9-2*** included external encryption key management solutions, wireless networking, technical or physical access controls, anti-malware solutions, file integrity monitoring (FIM), external firewalls, network switches, network intrusion detection and prevention systems (IDS/IPS).

# Evaluation of PCI DSS controls and scoring system

Coalfire evaluated PCI DSS 3.2.1 requirements classifying them as either organizational or technical. Procedural or technical requirements were based on requirement narratives, testing procedures, and guidance.

Where the requirement was determined as applicable, Coalfire assessed the capability of Oracle PCA X9-2 to address the requirement. In keeping with the desire to present the information compactly, Coalfire used Harvey Balls (https://en.wikipedia.org/wiki/Harvey_Balls) to assign each applicable requirement a qualitative category of capability, including whether the solution had a fractional capacity to support a percentage of the controls.

The table below is a key for the scoring given to each requirement in the scoring tables below:

| Symbol | Description | Definition |
|---|---|---|
| 4 | Solid | >75% Supported |
| 3 | Three-fourths | >50% - 75% |
| 6 | Half | >25% - 50% |
| 1 | One-quarter | >0% - 25% |
| 0 | Empty | Impedes Support |
| | Blank | Not Applicable (N/A) |
| n̲ | n-bar | Notional Control |

*Table 2: Key for Score and Other Symbols*

## Summary of overall PCI DSS 3.2.1 scoring

The information presented in this section (Table 3) represents an aggregate score of the ***Oracle PCA X9-2*** platform based on a composite of the scores provided in the individual requirement scoring tables included in the sections that follow. Coalfire's scoring system summarizes Coalfire's findings for PCI DSS control applicability by representing the number of technical controls and notional controls met for the PCI DSS requirement. The column marked Controls (TC, #, n̲) reflects the total number of controls (TC) for that requirement, the technical control count (#) potentially applicable to ***Oracle PCA X9-2*** support, and the notional controls (n̲) that would be required and supplied by a system outside of ***Oracle PCA X9-2*** (and therefore be entirely the customer's responsibility). Any customer responsibilities for the elements of the platform are detailed in their respective section.

In this overall scoring representation, Coalfire has included all requirements, including a non-applicable control, Requirement 9, which pertains to physical access. Requirement 9 comprises customer and non-***Oracle PCA X9-2*** responsibilities for housing the ***Oracle PCA X9-2*** systems in secure and monitored facilities and for ensuring that the staff supporting those systems have undergone background checks, are trained, and have designated roles.

In subsequent scoring tables, any non-applicable requirements, such as Requirement 9, are omitted for clarity.

| PCI Req | PCI DSS Requirements and Security | Controls (TC, #, n) | Score |
|---|---|---|---|
| | **Build and Maintain a Secure Network and Systems** | | |
| 1 | Install and maintain a firewall configuration to protect CHD. | 19, 8, 7n | 4 |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters. | 12, 7, 5n | 4 |
| | **Protect CHD** | | |
| 3 | Protect stored CHD. | 21, 0, 11n | n |
| 4 | Encrypt transmission of CHD across open, public networks. | 4, 0, 1n | n |
| | **Maintain a Vulnerability Management Program** | | |
| 5 | Protect all systems against malware and regularly update antivirus software or programs. | 6, 0, 5n | n |
| 6 | Develop and maintain secure systems and applications. | 28, 2, 26n | 4 |
| | **Implement Strong Access Control Measures** | | |
| 7 | Restrict access to CHD by business need to know. | 8, 5, 3n | 4 |
| 8 | Identify and authenticate access to system components. | 23, 14, 5n | 4 |
| 9 | Restrict physical access to CHD. | 22, 0, 22n | n |
| | **Regularly Monitor and Test Networks** | | |
| 10 | Track and monitor all access to network resources and CHD. | 29, 25, 4n | 4 |
| 11 | Regularly test security systems and processes. | 17, 0, 14n | n |
| | **Maintain an Information Security Policy** | | |
| 12 | Maintain a policy that addresses information security for all personnel. | 41, 0, 40n | n |

*Table 3: PCI DSS 3.2.1 Overall Oracle PCA X9-2 Scoring*

# Oracle PCA X9-2 applicability to PCI DSS 3.2.1

This section details Coalfire's compliance findings for elements of the ***Oracle PCA X9-2*** platform, along with the corresponding customer requirements and responsibilities for those elements, as reviewed in Coalfire's analysis of the suggested use case.

It is essential to understand that platforms and suite technologies do not themselves provide a CDE application base (i.e., software that performs the storage, processing, or transmission of CHD), but can support CDE application software as the term platform implies. Coalfire's review of ***Oracle PCA X9-2*** applicability to PCI DSS is based on the platform's capacity to either provide compliance with the specific PCI DSS control or directly support the actual application code via technical means and other necessary elements of architecture for payment card processing.

## Oracle PCA X9-2 Platform

### Requirement 1: Install and maintain a firewall configuration to protect CHD

Firewalls are devices that control the computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The CDE is an example of a more sensitive area within an entity's trusted network.

Typically, compliance with this requirement is met by placing appliances such as Oracle PCA X9-2 behind firewall(s) deployed in the on-premises infrastructure. As Oracle PCA X9-2 must be deployed within a PCI DSS-compliant environment, this requirement will not generally apply directly to the appliance.

However, there may be situations in which segmentation is created within the appliance to:

- Reduce the CDE scope
- Segment public-facing systems and internal systems
- Segment testing, development, and production environments

For those situations in which segmentation is used, the ability of Oracle PCA X9-2 to support security lists and Network Security Groups (NSGs) to isolate cloud resources can be leveraged. It is important to note that the validity of any segmentation must be validated by technical review and penetration testing in order to meet PCI DSS compliance.

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| **1** | **Install and maintain a firewall configuration to protect CHD.** | | |
| 1.1.4 | Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone. | Oracle PCA X9-2 security lists and NSGs can be leveraged to restrict public and private subnets to comply with this requirement. | 4 |
| 1.2.1 | Restrict inbound and outbound traffic to that which is necessary for the CDE, and specifically deny all other traffic. | Oracle PCA X9-2 security lists and NSGs can be leveraged for compliance with this requirement. All other traffic is implicitly denied. | 4 |
| 1.3.1 | Implement a DMZ to limit inbound traffic to only system components that provide | Oracle PCA X9-2 security lists and NSGs can be leveraged to restrict public and private subnets to the internet gateway to support compliance with this | 1 |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| | authorized publicly accessible services, protocols, and ports. | requirement. On-premises requires configuration to allow public route access to the internet gateway. | |
| 1.3.2 | Limit inbound internet traffic to IP addresses within the DMZ. | Oracle PCA X9-2 public subnets can be restricted via security lists and NSGs for ingress traffic from the internet gateway for compliance with this requirement. | 4 |
| 1.3.4 | Do not allow unauthorized outbound traffic from the CDE to the internet. | Oracle PCA X9-2 leverages security lists and NSGs for restricting outbound traffic from public and private subnets for compliance with this requirement. | 4 |
| 1.3.5 | Permit only “established” connections into the network. | Oracle PCA X9-2 Security List rules can be defined as stateful or stateless. | 4 |
| 1.3.6 | Place system components that store CHD (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | Segmentation of cloud resources can be created within the Oracle PCA X9-2, segregated with security lists and NSGs, to facilitate compliance with this requirement. | 4 |
| 1.3.7 | 1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.<br><br>Note: Methods to obscure IP addressing may include, but are not limited to:<br>• Network Address Translation (NAT)<br>• Placing servers containing CHD behind proxy servers/firewalls,<br>• Removal or filtering of route advertisements for private networks that employ registered addressing,<br>• Internal use of RFC1918 address space instead of registered addresses. | Oracle PCA X9-2 leverages NAT to prevent disclosure of private IP addresses and routing information to unauthorized parties. | 4 |

*Table 4: **Oracle PCA X9-2** Platform PCI DSS 3.2.1 Requirement 1 Scoring*

## Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Oracle PCA X9-2 facilitates the initial setup of accounts and credentials via the Service Web UI and an Initial Installation Checklist. Additionally, Oracle PCA X9-2 supports Aqua’s Kube-Bench for testing the control plane and/or data against the industry-accepted Center for Internet Security (CIS) system hardening standards to identify and remediate configuration drift on clusters. Any administrative access to Oracle PCA X9-2 is through SSH or SSL encrypted channels.

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| **2** | **Do not use vendor-supplied defaults for system passwords and other security parameters.** | | |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.<br>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc. | Oracle PCA X9-2 prevents vendor defaults via the Initial Installation Checklist, the Service Web UI/CLI, and the initial configuration wizard.<br>In addition, Oracle PCA X9-2 supports Aqua's Kube-Bench for testing clusters against CIS standards to identify and remediate configuration drift. | 4 |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.<br>Sources of industry-accepted system hardening standards may include, but are not limited to:<br>• CIS<br>• International Organization for Standardization (ISO)<br>• SysAdmin Audit Network Security (SANS) Institute<br>• National Institute of Standards Technology (NIST) | Oracle PCA X9-2 supports industry-accepted standards by supporting tools like Aqua's Kube-Bench, which tests clusters against CIS standards to identify and remediate configuration drift. | 4 |
| 2.2.1 | Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)<br>**Note**: Where virtualization technologies are in use, implement only one primary function per virtual system component. | Oracle PCA X9-2 supports the implementation of one primary function per virtual instance and container. | 3 |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | Only those services and protocols necessary for management of the Oracle PCA X9-2 environment are enabled.<br>Management of services and protocols are implemented through NSGs and security lists. | 4 |
| 2.2.4 | Configure system security parameters to prevent misuse. | Oracle PCA X9-2 prevents misuse of security parameters via the initial configuration wizard and Initial Installation Checklist accessed by the Service Web UI/CLI. | 4 |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| 2.3 | Encrypt all non-console administrative access using strong cryptography.<br>**Note**: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. | Administrative access to the Oracle PCA X9-2 is conducted through SSH and TLS encrypted channels. | 4 |
| 2.4 | Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of the components function/use. | The Oracle PCA X9-2 Service console, monitoring dashboard, and Admin CLI support querying inventory elements for critical hardware and software from the inventory database. | 3 |

*Table 5: **Oracle PCA X9-2** Platform PCI DSS 3.2.1 Requirement 2 Scoring*

## Requirement 3: Protect stored CHD

Protection methods such as encryption, truncation, masking, and hashing are critical components of CHD protection. If an intruder circumvents other security controls and gains access to encrypted data, the data is unreadable and unusable to that person without the proper cryptographic keys. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing CHD unless absolutely necessary, truncating CHD if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

The protection of CHD stored within the Oracle PCA X9-2 is the sole responsibility of the customer. This requirement is a typical customer responsibility excluded from infrastructure or appliance solutions like Oracle PCA X9-2.

## Requirement 4: Encrypt transmission of CHD across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to CDEs.

Oracle PCA X9-2 will typically be deployed in an environment in which no data is transmitted over open, public networks. However, customer deployment needs vary, and data transmission from cloud resources may need to travel over open, public networks. Encryption for such transmission will be implemented at the data plane (worker node) and is supported by Oracle PCA X9-2, subject only to any limitations of the container and applications.

## Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware” (e.g., including viruses, worms, and Trojans) can enter a network during many business-approved activities, including employee e-mail and use of the internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

The operating system used for the management of the Oracle PCA X9-2 environment, Oracle Linux, is typically considered to be “not commonly affected by malicious software,” but may be managed as any other operating system and protected by anti-virus software if deemed necessary by the organization. Organizations must address the malware risk to operating system management using their own formal IT risk assessment processes and consultation with their QSA.

While any virtual machine hosted within the Oracle PCA X9-2 environment is subject to this requirement and must be managed accordingly, management of this requirement is out of scope for the Oracle PCA X9-2 compliance environment.

## Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of CHD by malicious individuals and malicious software.

The Oracle PCA X9-2 supports PCI DSS requirements for patching through dedicated channels on the Unbreakable Linux Network (ULN). Additional requirements, such as development processes, change management, code review, and application vulnerability testing, are typical customer responsibilities excluded from infrastructure or appliance solutions like Oracle PCA X9-2.

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| **6** | **Develop and maintain secure systems and applications.** | | |
| 6.2 | Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.<br>**Note**: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | The Oracle PCA X9-2 component patches are delivered as RPM packages through a series of dedicated channels on the ULN. To gain access to these channels, a Customer Support Identifier (CSI) and a ULN subscription are required. | 4 |
| 6.4.1 | Separate development/test environments from production environments and enforce the separation with access controls. | Separate test, development, and production environments can be created within Oracle PCA X9-2 using the segmentation options discussed in requirement one. | 3 |

*Table 6: **Oracle PCA X9-2** Platform PCI DSS 3.2.1 Requirement 6 Scoring*

## Requirement 7: Restrict access to CHD by business need-to-know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

The Oracle PCA X9-2 IAM service provides access controls and default deny-all capability to cloud resources with Oracle PCA X9-2 tenancies. Fine-grained policies in IAM can be applied to cloud resources to restrict access to users, groups, and compartments.

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| **7** | **Restrict access to CHD by business need to know.** | | |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| 7.1 | Limit access to system components and CHD to only those individuals whose job requires such access. | The IAM service supports this requirement when used to manage access to Oracle PCA X9-2 cloud resources. IAM's ability to manage access to cloud resources both supports and facilitates compliance with features such as granular system access policy and default implicit "deny-all" settings for provisioned resources. | 4 |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | | 4 |
| 7.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.<br>This access control system(s) must include the following: | | 4 |
| 7.2.1 | • Coverage of all system components | | 4 |
| 7.2.3 | • Default "deny-all" setting. | | 4 |

*Table 7: **Oracle PCA X9-2** Platform PCI DSS 3.2.1 Requirement 7 Scoring*

## Requirement 8: Identify and authenticate access to system components

Assigning a unique ID to each person with system access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system. In particular, how frequently password attempts can be made by an attacker and the security methods in place to protect user passwords at the point of entry, during transmission, and while in storage.

Oracle PCA X9-2 leverages IAM to manage accounts and access controls. . Additionally, Oracle PCA X9-2 also supports integration with identity provider Microsoft Active Directory, via Active Directory Federation Services.

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| **8** | **Identify and authenticate access to system components.** | | |
| 8.1.1 | Assign all users a unique ID before allowing them to access system components or CHD. | The IAM service supports this requirement when used to manage access to the Oracle PCA X9-2 cloud resources. IAM's ability to manage access to cloud resources both supports and facilitates compliance with features such as access policy, account maintenance, password rotation and complexity | 4 |
| 8.1.2 | Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | | 4 |
| 8.1.3 | Immediately revoke access for any terminated users. | | 3 |
| 8.1.4 | Remove/disable inactive user accounts within 90 days. | | 4 |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| 8.1.5 | Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Monitored when in use. | | 4 |
| 8.1.6 | Limit repeated access attempts by locking out the user ID after not | | 4 |
| 8.1.7 | Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | | 4 |
| 8.1.8 | If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | | 3 |
| 8.2 | In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:<br>• Something you know, such as a password or passphrase<br>• Something you have, such as a token device or smart card<br>• Something you are, such as a biometric. | | 4 |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | | 4 |
| 8.2.3 | Passwords/passphrases must meet the following:<br>• Require a minimum length of at least seven characters.<br>• Contain both numeric and alphabetic characters.<br>• Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above. | | 4 |
| 8.2.4 | Change user passwords/passphrases at least once every 90 days. | | 4 |
| 8.2.5 | Do not allow an individual to submit a new password/passphrase that is the same as any | | 4 |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| | of the last four passwords/passphrases he or she has used. | | |
| 8.2.6 | Set passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use. | | 4 |

*Table 8: **Oracle PCA X9-2** Platform PCI DSS 3.2.1 Requirement 8 Scoring*

## Requirement 9: Restrict physical access to CHD

Requirement 9 states, “Any physical access to data or systems that house CHD provides the opportunity for individuals to access devices or data and to remove systems or hard copies, and should be appropriately restricted. For the purposes of Requirement 9, ‘onsite personnel’ refers to full-time and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity’s premises. A ‘visitor’ refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. ’Media’ refers to all paper and electronic media containing CHD” (PCI DSS, 2018).

As Oracle PCA X9-2 must be deployed in a physically secure environment to meet this compliance requirement, this requirement is typically the customer’s responsibility and is excluded from infrastructure or appliance solutions like Oracle PCA X9-2.

## Requirement 10: Track and monitor all access to network resources and CHD

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

The monitoring and audit capabilities of Loki and Grafana enables Oracle PCA X9-2 to meet compliance requirements for logging and monitoring cloud resources.

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| **10** | **Track and monitor all access to network resources and CHD.** | | |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | The Fluentd data collector retrieves logs from Oracle PCA X9-2 components and stores them in a central location. Furthermore, all logs associated with Oracle PCA X9-2 can be exported to a log management tool to support compliance with these requirements. | 4 |
| 10.2 | Implement automated audit trails for all system components to reconstruct the following events: | | |
| 10.2.1 | • All individual user accesses to CHD | | |
| 10.2.2 | • All actions taken by any individual with root or administrative privileges | | |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| 10.2.3 | • Access to all audit trails | | |
| 10.2.4 | • Invalid logical access attempts | | |
| 10.2.5 | • Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | | |
| 10.2.6 | • Initialization, stopping, or pausing of the audit logs | | |
| 10.2.7 | • Creation and deletion of system-level objects | | |
| 10.3 | Record at least the following audit trail entries for all system components for each event: | | |
| 10.3.1 | • User identification | | |
| 10.3.2 | • Type of event | | |
| 10.3.3 | • Date and time | | |
| 10.3.4 | • Success or failure indication | | |
| 10.3.5 | • Origination of event | | |
| 10.3.6 | • Identity or name of affected data, system component, or resource. | | |
| 10.4 | Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. | The Oracle PCA X9-2 can be configured to synchronize with the organization's NTP source in the "Configure Network Params" during initial setup. | 4 |
| 10.4.1 | • Critical systems have the correct and consistent time. | | |
| 10.4.2 | • Time data is protected. | | |
| 10.4.3 | • Time settings are received from industry-accepted time sources. | | |

| PCI Req | PCI DSS Requirements and Oracle PCA X9 2 Platform | Comments | Score |
|---|---|---|---|
| 10.5 | Secure audit trails so they cannot be altered. | All logs associated with the Oracle PCA X9-2 can be reviewed via Grafana and Prometheus monitoring and Grafana support default and custom monitoring dashboards to query logs aggregated in Loki. Customers can also export audit logging and telemetry to an external log management tool to meet compliance requirements. | 3 |
| 10.5.1 | Limit viewing of audit trails to those with a job-related need. | | 3 |
| 10.5.2 | Protect audit trail files from unauthorized modifications | | 3 |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | | 3 |
| 10.5.4 | Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | | 3 |
| 10.5.5 | Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | | 3 |
| 10.6 | Review logs and security events for all system components to identify anomalies or suspicious activity.<br><br>**Note**: Log harvesting, parsing, and alerting tools may be used to meet this requirement. | | 3 |
| 10.6.1 | 10.6.1 Review the following at least daily:<br>• All security events<br>• Logs of all system components that store, process, or transmit CHD and/or SAD<br>• Logs of all critical system components<br>• Logs of all servers and system components that perform security functions (for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc.). | | 3 |
| 10.7 | Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | | 3 |

*Table 9: **Oracle PCA X9-2** Platform PCI DSS 3.2.1 Scoring*

## Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by both malicious individuals and researchers, as well as being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Although Oracle PCA X9-2 does not directly support the requirements for testing and monitoring in Requirement 11, customers can employ external solutions and/or integration with OCI.

## Requirement 12: Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole entity and sets expectations of behavior for personnel. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the CDE.

The requirements detailed throughout Requirement 12 of the PCI DSS 3.2.1 cover the policy and procedures necessary to enforce the technical and process controls of all the PCI DSS requirements. This requirement is typically the customer's responsibility and is excluded from infrastructure or appliance solutions like Oracle PCA X9-2.

## Customer responsibilities for PCI DSS use of the Oracle PCA X9-2 platform

Summarized below are PCI DSS design considerations and customer responsibilities for the bespoke POS system use case.

- Customers should:
  - Use network diagrams to properly depict CDE dataflow, particularly to protected volumes for CDE storage and for adherence to the security boundaries for CDE and out-of-scope data segments.
  - Allocate virtual and physical resources for input and output rates (I/Os), the management plane, VMs as supported by AHV hypervisor, and data paths to create necessary segmentation boundaries and support the intended PCI DSS architecture.
  - Assign dedicated storage volumes for CDE data (specifically, PAN, SAD, and other security essentials) and other similar storage assignments to support the segregation of CDE data and to keep CT/SI systems storage inaccessible to corporate LAN workloads.
  - Require the elimination of system defaults and self-signed certificates for SSL per details of Requirement 2.
  - Implement proper RBAC to restrict administration of the required I/O configuration to roles that support storage allocation
  - Ensure FIM receives all data storage services' contributions to support ongoing the security posture as specified by Requirement 11.
  - Implement notional SIEM logging and alerting systems with integration for systems administration and change verification, access to CDE logging, and ensure the integration of Syslog and advanced logging (Elastic, ELK, and similar) to such a system.
- Customers should take into consideration that:
  - Actual code development practices, policies, and procedures must satisfy the majority of PCI DSS Requirement 6: Develop and maintain secure systems and applications. These areas were considered bespoke (meaning they would be subject to the scrutiny of a QSA or reported in detail in an SAQ) and outside the scope of Coalfire's review.
  - The key to successful PCI implementation is using Core HCI platform virtualization techniques to properly construct the network segmentation to support CDE, CT/SI, and out-of-scope pod allocations. Coordination of this feature with external switching and firewall design patterns requires a holistic design.
  - The creation of network diagrams depicting the combination of the Oracle PCA X9-2 platform, conventional network switching, firewall, and DMZs is essential.

# Conclusion and Coalfire opinion

Coalfire reviewed ***Oracle PCA X9-2*** for its efficacy in assisting payment card entities with successful deployments resulting in a compliant SAQ or ROC for PCI DSS 3.2.1, and has the following opinion of the potential product use in the compliance program:

Oracle PCA X9-2 can be implemented as part of a CDE. When deployed with controls described in this paper, Oracle PCA X9-2 can support and can often meet PCI DSS compliance requirements. While there are additional factors unique to a cloud solution, these factors are in no way insurmountable. In fact, many features of Oracle PCA X9-2 can easily support compliance with PCI DSS requirements and assist organizations with a more secure and cost-effective solution.

Coalfire is of the opinion that the reviewed ***Oracle PCA X9-2*** solution can be effective in providing significant and substantial support for PCI DSS payment entities' objectives and requirements. This opinion applies to scenarios like the suggested merchant POS use case, as well as a considerable number of other real-world payment card applications, based on the observed PCI DSS control support that is common to both the reviewed scenario and those other applications.

This opinion is also dependent on many underlying presumptions (caveats), which are expectations of an actual payment card processing environment and are listed below:

- Adherence to vendor best practices for ***Oracle PCA X9-2*** and other associated vendors used in an actual deployment.
- Required ancillary services to provide CT/SI systems, including potential Microsoft AD, LDAP, DNS, NTP, and other likely services.
- Implementation of specific external firewalls, external network switches, anti-malware/anti-virus, FIM, IDPS, SIEM, and other required PCI systems.
- Use of supporting services and providers to process payments (upstream payment providers), supply continuous repair and maintenance, and other contracted and PCI DSS compliant services consumed by the entity.
- Actual organizational controls support their payment card entity roles, responsibilities, policies, procedures, baselines, and mandates.
- Physical controls to control and secure access to the facilities.
- Periodic penetration testing (internal and external), and vulnerability scans, including internal scans and external scans by an PCI DSS Approved Scan Vendor (ASV).
- Presence of IT staff to support the workload and business operations.
- Actual payment card bespoke, organization-custom POS applications, POI devices, and other POS components.

## A comment regarding regulatory compliance

Coalfire disclaims the generic suitability of any product to establish regulatory compliance strictly by use of that product. Agencies and entities attain compliance through a Governance, Risk Management, and Compliance (GRC) program, not via the use of a specific product. This is true for merchants or service providers subject to PCI DSS and customers targeting compliance with other regulations.

# Legal disclaimer

- Coalfire corporate information is available at the following link:

  https://www.coalfire.com/about

## About the author

**Allen Mahaffy,** *CISSP, CISA, QSA* | Principal Consultant

Allen has over a decade of experience performing PCI DSS assessments and advisory services for merchants, service providers, large enterprises, and major cloud service providers. His other experience in cloud includes assessing and analyzing cloud micro-service architectures, container orchestration, security and compliance automation, and various emerging cloud technologies.

## About Oracle

Oracle provides products and services that address enterprise information technology environments worldwide. Oracle offers cloud-based industry solutions for various industries. In addition, it provides infrastructure technologies, such as the Oracle Database, an enterprise database; Java, a software development language; and middleware, including development tools and others, for cloud and license businesses. Oracle's cloud and license business infrastructure technologies also comprise cloud-based compute, storage, and networking capabilities as service offerings through its Oracle cloud infrastructure. Additionally, it provides hardware products and other hardware-related software offerings, including Oracle engineered systems, enterprise servers, storage solutions, industry-specific hardware, virtualization software, operating systems, management software, and related hardware services and consulting services. Oracle markets and sells its cloud, license, hardware, support, and services offerings directly to businesses in various industries, government agencies, and educational institutions, as well as through indirect channels. Oracle was founded in 1977 and is headquartered in Austin, Texas. **Oracle.com**.

## About Coalfire

The world s leading technology infrastructure providers, SaaS companies, and enterprises including the top 5 cloud service providers and 8 of the top 10 SaaS businesses rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.



WP_OraclePCA_2022