ORACLE

Oracle Cloud Native SCCA Landing Zone – Customer Responsibility

Guidance to the US Department of Defense (DoD) and Implementation Partners for using Oracle Cloud Native Platform Automation in connection with Secure Cloud Computing Architecture Requirements

July, 2023, Version 2.0

Public

Purpose statement

The Oracle Cloud Native Secure Cloud Computing Architecture (SCCA) Landing Zone Architecture Guide provides an overview of how the DOD community can use the Oracle DOD Cloud platform to comply with DOD requirements of the SCCA, as described DOD Functional Requirements Document (FRD). It is intended solely to help the customer/mission owner understand the Oracle DOD Cloud platform and to plan IT projects that require the use of Oracle DOD Cloud (IaaS and PaaS) to provide native services to build the SCCA ecosystem. This Guide is not meant to supplant the guidance outlined in the Cloud Computing Security Resource Guide, Cloud Connection Process Guide, Secure Cloud Computing Architecture Functional Requirements Document, or any other official Department of Defense guidance or mandates. This Guide provides the Oracle DOD Cloud Guidance on how to use the Oracle cloud native services (IaaS and PaaS) in connection with DOD SCCA requirements as set forth by DISA FRD.

Disclaimer

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. *This document may reference products/services or security controls that currently are in the process of obtaining DISA Impact Level 5 provisional authorization. Due to the nature of the document, it may not be possible to include all features described in this document. For additional information specific to certain Oracle Cloud Services with DISA Impact Level 5 authorization, please refer to this informational website, located at:* ***Oracle Cloud US Federal Cloud with DISA Impact Level 5 Authorization.***

Some of the services are under accreditation by DISA or the U.S. Intelligence Community and may not be available as a general release.

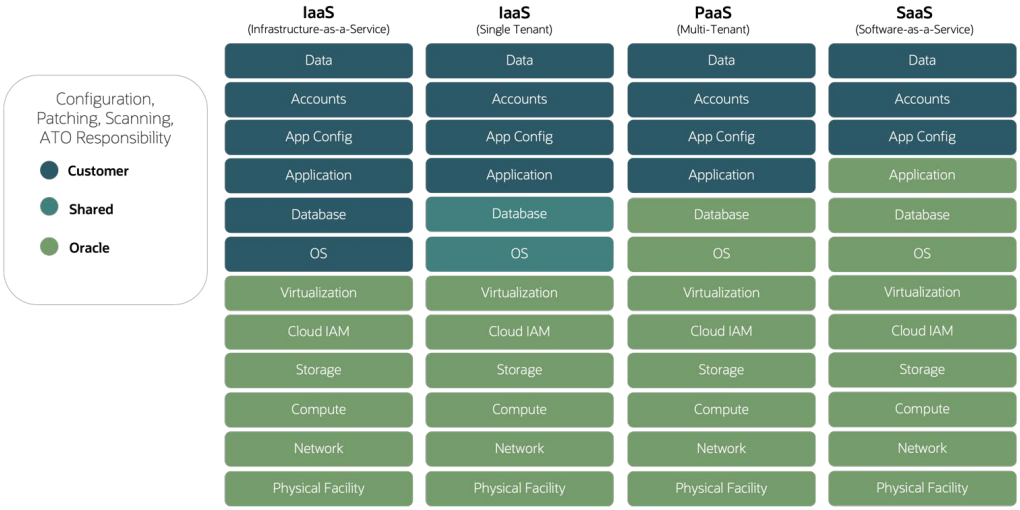
Table of contents

Oracle Cloud Shared Responsibility Model

Oracle Cloud for Government and DOD include security technology and operational processes to secure enterprise cloud services. For you to securely run your workloads, you must be aware of your security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations such as cloud operator access controls and infrastructure security patching. You as the customer/mission owner are responsible for securely configuring your cloud resources. Security in the cloud is a shared responsibility between you and the Cloud Service Provider (CSP). Figure 1 illustrates this shared responsibility model and how it varies depending on which tier of cloud computing you choose to employ.

With respect to the Shared Responsibility Model, security capabilities identified by the SCCA can be delivered by either DOD, the CSP, or third-party organizations. This presents an opportunity to utilize a mix of DOD-standard security solutions, best-in-class security solutions, and CSP-offered capabilities for a uniquely catered solution that meets security and cost objectives.

Figure 1. Shared Responsibility in Oracle Cloud



Virtual Data Center Security Stack (VDSS) Oracle Cloud Guidance

Table 1. VDSS Customer Responsibility

Customer Responsibility VDSS – Oracle Cloud Guidance

Req. ID	SCCA functional requirements	Oracle Cloud PaaS	Customer/Mission Owner responsibility description
2.1.2.10	The VDSS shall provide an interface to conduct ports, protocols, and service management (PPSM) activities to provide control for MCD operators	PPSM Interface, Oracle Cloud Security List, Network Firewall	In accordance with DoDI 8551.01: Ports, Protocols, and Services Management (PPSM), customers are responsible for conducting PPSM. Customers are responsible for providing Oracle with PPSM data to assist in the build-out of the Customer Tenancy. Customers must coordinate continuous monitoring efforts with and request PPSM verification from Oracle in accordance with Customer requirements.

2.1.2.11	The VDSS shall provide a monitoring capability that captures log files and event data for cybersecurity analysis.	Logging Analytics, OAM/OIM/OEM, Oracle Cloud Monitoring	Customers can update the audit logging configuration within the Customer tenancy to ensure that the Customer workload satisfies Customer's audit and compliance requirements.
2.1.2.12	The VDSS shall provide or feed security information and event data to an allocated archiving system for common collection, storage, and access to event logs by privileged users performing Boundary and Mission CND activities.	Logging, Service Connector Hub, Object Storage	Customers are responsible for requesting security information and event data and managing access control to the Object Storage bucket containing such information.
2.1.2.13	The VDSS shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions.	Virtual Private Vault	Customers are responsible for creating and controlling permissions for an Oracle Cloud Vault and the encryption keys contained within.
2.1.2.14	The VDSS shall provide the capability to detect and identify application session hijacking.	Network Firewall/WAF v2	Customers are responsible for providing Oracle PKI certificates issued by DOD-approved Certificate Authorities.
2.1.2.16	The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording.	vTAP	Oracle will provide the logs. Customer is responsible for interpreting traversing communications.

2.1.2.4	The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content.	WAF + NGFW	Customers are responsible for acquiring third party licenses/third party tools.
2.1.2.5	The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic.	Oracle Cloud WAF, Network Firewall (NGFW) , Oracle Cloud Observability and Management Platform	Customers must work with Oracle to identify authorized application layer traffic within the Customer Tenancy in accordance with their architecture and business requirements.
2.1.2.6	The VDSS shall provide a capability that monitors network and system activities to detect and report malicious activities for traffic entering and exiting Mission Owner virtual private networks/enclaves.	WAF, Network Firewall, Oracle Cloud Observability and Management Platform	Customers are responsible for ensuring that the SIEM's alerting framework meets Customer monitoring and reporting requirements. Customers are responsible for reporting security incidents related to their application workload in Customer tenancy to and coordinating incident response activities with DOD agencies per their ATO reporting requirements.
2.1.2.7	The VDSS shall provide a capability that monitors network and system activities to stop, or block detected malicious activity.	WAF,Network Firewall, Oracle Cloud Observability and Management Platform	Customers must work with Oracle to identify authorized application layer traffic within the Customer Tenancy in accordance with their architecture and business requirements.
2.1.2.8	The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves.	WAF, Network Firewall, Oracle Cloud Observability and Management Platform	Customers are responsible for inspecting traffic and configuring Security List, network security groups, and security rules within their Customer Tenancy.

2.1.2.9	The VDSS shall perform break and inspection of SSL/TLS communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE.	WAF, Network Firewall, Oracle Cloud Observability and Management Platform	Customers are responsible for DoD-compliant PKI certificates.
2.3.4.6	SCCA shall provide Boundary Cyberspace Protection (BCP) and Mission Cyberspace Protection (MCP) operator access to security information and security relevant event data derived from SSL/TLS session traffic which is broken and inspected at the VDSS and ICAP.	Log Insight Detector	Customers are responsible for Boundary Cyberspace Protection (BCP) and Mission Cyberspace Protection (MCP) operator access.
2.5.2.1	The VDSS management systems shall provide a mechanism for managing failover in accordance with DoD UCR 2013.	Oracle Cloud Networking	Customer must configure failover of Workload from Primary to Secondary site.
2.5.2.2	The VDSS management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable.	Oracle Cloud High Availibility, Networking	Customer is responsible for adhering to applicable policies for retention and recovery.
2.5.2.3	The VDSS shall maintain offsite backup configurations for the recovery of operations.	Cross region Replication (Object Storage)	Customer is responsible for configuration of offsite backup policy.
2.5.3.1	The VDMS management systems shall provide a mechanism for managing failover.	Oracle Cloud Networking	Customer must configure failover of Workload from Primary to Secondary site.

2.7.2.1	The VDSS shall provide the ability to backup and restore security, network, account, and system configurations.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.
2.7.2.2	The VDSS shall provide the capability to backup configuration and system data of all VDSS elements.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.
2.7.2.3	The VDSS shall provide the means to restore operational capability.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.

Virtual Data Center Managed Services (VDMS) Oracle Cloud Guidance

Table 2. VDMS Customer Responsibility

Customer Responsibility VDMS – Oracle Cloud Guidance

Req. ID	SCCA functional requirements	Oracle Cloud PaaS	Customer responsibility description
2.1.3.1	The VDMS shall provide Assured Compliance Assessment Solution (ACAS), or approved equivalent, to conduct continuous monitoring for all enclaves within the CSE.	No service available.	Customers are responsible for coordinating scanning activities in accordance with their Agency's or Department's guidance and requirements.
2.1.3.2	The VDMS shall provide Host Based Security System (HBSS), or approved equivalent, to manage endpoint security for all enclaves within the CSE.	Vulnerability scanning	Customer must provide endpoint protection (HBSS) configuration.
2.1.3.3	The VDMS shall provide identity services to include an Online Certificate Status Protocol (OCSP) responder for remote system DoD Common Access Card (CAC) two factor authentication of DoD privileged users to systems instantiated within the CSE.	Identity Domain	Customers are responsible for DoD PKI certificates and their associated Certificate Revocation List (CRL) and/or OCSP responder URL. Open-Source Servers for CRL to be updated by mission owner.

2.1.3.4	The VDMS shall provide a configuration and update management system to serve systems and applications for all enclaves within the CSE.	Oracle Cloud Resource Manager, WSUS, Repo, YUM	Customers are responsible for updating Customer-installed applications within the Customer Tenancy.
2.1.3.5	The VDMS shall provide logical domain services to include directory access, directory federation, Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS) for all enclaves within the CSE.	DNS	Customers are responsible for managing their on-premises identity and access management solution. Customers must host their DoD DNS records in the DoD NIPRNet authoritative DNS servers. Customers are responsible for managing their on-premises identity and access management solution.
2.1.3.7	The VDMS shall provide a system, security, application, and user activity event logging and archiving system for common collection, storage, and access to event logs by privileged users performing Boundary Cyberspace Protection (BCP) and Mission Cyberspace Protection (MCP) activities.	Object Storage Archive Storage / Oracle Cloud Logging	Customers must ensure that audit logging within Customer-provisioned instances and applications is configured in accordance with agency auditing policies and procedures.
2.1.3.8	The VDMS shall provide for the exchange of DoD privileged user authentication and authorization attributes with the CSP's Identity and access management system to enable cloud system provisioning, deployment, and configuration.	Identity Domain	Customers are responsible for managing their end-user authentication and authorization attributes within their on-premises IdP.
2.1.3.9	The VDMS shall implement the technical capabilities necessary to execute the mission and objectives of the TCCM role.	IAM, Identity Domain	Customers are responsible for managing and reviewing access to their own employee accounts and for all activities that occur under their tenancy. Oracle provides IAM services including identity management, authentication, authorization, and auditing for the customer to configure accounts within their tenancy. Customers are responsible for OS user administration for customer user access. This is applicable for bare metal compute, VM, and database instances.

2.3.2.5	SCCA management systems shall support the sharing of Combatant Commands, Services, Agencies (CC/S/A) log insight detector event & correlation data with the CC/S/A and CND Service Providers.	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.2.8	SCCA components shall provide sensor events, performance, and resource utilization metrics to the component operators.	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.4.1	SCCA elements shall support the delivery of security relevant events through element management ports.	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.4.3	SCCA elements shall provide a checksum mechanism to detect the unauthorized alteration of event information during transmission of event data.	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.4.4	SCCA elements shall securely provide security relevant events to SCCA element management systems for logging, filtering, and correlating.	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.4.5	SCCA elements shall support caching of security relevant events if logging of events is not available.	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.4.7	SCCA shall feed specifically identified security information and security relevant event data necessary for situational awareness (SA) to Acropolis	Log Insight Detector	Customers are responsible for Log Insight Detector.
2.3.4.2	SCCA elements shall support CC/S/A unique tagging of events.	Log Insight Detector	Customers are responsible for unique tagging of events.

2.3.5.1	The FPC shall support integration with SIEM systems to effect data search and retrieval, such as the capability to pull select timeframes of captured data.	vTAP	vTAP is implemented on workload resources.
2.3.5.2	The FPC shall provide the means to reconstruct all network traffic sessions traversing the SCCA Component.	vTAP	vTAP is implemented on workload resources.
2.3.5.3	The FPC shall provide defined data queries that run against metadata.	vTAP	vTAP is implemented on workload resources.
2.3.5.4	The FPC shall provide a capability to request an arbitrary subset of packets.	vTAP	vTAP is implemented on workload resources.
2.3.5.5	The FPC shall locally store captured traffic for 30 days.	vTAP, Object Storage	vTAP is implemented on workload resources.
2.3.5.6	The FPC data shall be isolated from user and data plane traffic via cryptographic or physical means.	vTAP	vTAP is implemented on workload resources.
2.3.5.7	The FPC data shall be query-able from a secure remote location on the management network.	vTAP	vTAP is implemented on workload resources.
2.3.5.8	The FPC function shall be configurable according to traffic flow source and destination points to avoid multiple point capture.	vTAP	vTAP is implemented on workload resources.
2.5.3.2	The VDMS management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable.	Oracle Cloud HA/Networking	Customer is responsible for configuration for recovery.
2.5.3.3	The VDMS shall maintain offsite backup configurations for the recovery of operations.	Cross region Replication (Object Storage)	Customer is responsible for offsite backup retention policy.
2.7.3.1	The VDMS shall provide the ability to backup and restore security, network, account, and system configurations.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.

2.7.3.2	The VDMS shall provide the capability to backup configuration and system data of all VDMS elements.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.
2.7.3.3	The VDMS shall provide the means to restore operational capability.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.

Boundary Cloud Access Point (BCAP) Oracle Cloud Guidance

Table 3. BCAP Customer Responsibility

Customer Responsibility BCAP – Oracle Cloud Guidance

Req. ID	SCCA functional requirements	Oracle Cloud PaaS	Customer responsibility description
2.2.5.10	(Optional) The BCAP shall provide secure DNS proxy to support cloud hosted system URL resolution of public IP space using DISN IP translation.	Native DNS	Customer is responsible to provide DNS configurations/DISA provided DNS services.
2.2.5.5	(Optional) The BCAP and ICAP shall provide the capability to dynamically manage the opening and closing of User Datagram Protocol (UDP) ports carrying Real-time Transport Protocol (RTP)/RTP Control Protocol (RTCP) media streams.	Oracle Cloud Networking	Infrastructure outside of Oracle Cloud is the customer responsibility.
2.5.1.1	In the event of a catastrophic site failure, the ICAP and BCAP/MeetMe shall allow the failover of functionality from one site to another with minimum impact to mission user application traffic and mission owner management traffic. The amount of time needed to failover a site should be less than 30 seconds once initiated.	Oracle Cloud Disaster Recovery, (Dynamic Routing Gateways DRGv2 and Transit Routing via Backbone to other region)	Customer is responsible for the export and import configuration.
2.5.1.2	The BCAP/ICAP shall maintain online backup configurations for recovery of operations.	Backup Object storage Archive storage	Customer is responsible for the export and import configuration.

2.5.1.3	The BCAP/ICAP management systems shall provide a mechanism for managing failover.	Oracle Cloud DR (DRGv2 and TR via Backbone to other region)	Customer is responsible for the export and import configuration.
2.5.1.4	The BCAP/ICAP management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable.	Resource Manager (Also, Backup Object storage Archive storage)	Customer is responsible for the export and import configuration.
2.5.1.5	The BCAP/ICAP shall maintain offsite backup configurations for the recovery of operations.	Cross region Replication (Object Storage)	Customer is responsible for offsite backup of data and configurations that can be stored in an object storage bucket and accessed from on-premises systems and from other cloud regions.
2.7.1.1	The BCAP/ICAP shall provide the ability to backup and restore security, network, account, and system configurations.	Backup Object storage Archive storage	Customer is responsible for export and import configuration.
2.7.1.2	The BCAP/ICAP shall provide the capability to backup configuration and system data of all SCCA elements.	Backup Object storage Archive storage	Customer is responsible for the export and import configuration.
2.7.1.3	The BCAP/ICAP shall provide the means to restore operational capability.	Backup Object storage Archive storage	Customer is responsible for the export and import configuration.

Table 4. TCCM Customer Responsibility

Customer Responsibility TCCM – Oracle Cloud Guidance

Req. ID	SCCA functional requirements	Oracle Cloud PaaS	Customer responsibility description
2.1.4.1	The TCCM shall develop and maintain a Cloud Credential Management Plan (CCMP) to address the implementation of policies, plans, and procedures that will be applied to mission owner customer portal account credential management.	IAM, Identity Domain	Customer is responsible for developing and maintaining a CCMP.
2.1.4.2	The TCCM shall collect, audit, and archive all Customer Portal activity logs and alerts.	IAM Object Storage Logging	Customer is responsible for implementing an alerting capability associated with Customer Portal activity logs.
2.1.4.3	The TCCM shall ensure activity log alerts are shared with, forwarded to, or retrievable by DOD privileged users engaged in Mission Cyberspace (MCP) and Boundary Cyberspace Protection (BCP) activities.	IAM Object Storage Logging	Customer is responsible for sharing logs with the appropriate authority.
2.1.4.4	The TCCM shall, as necessary for information sharing, create log repository access accounts for access to activity log data by privileged users performing both Mission Cyberspace Protection (MCP) identified in Cloud Cyberspace Protection Guide (CCPG) and Boundary Cyberspace Protection (BCP) activities.	IAM Object Storage Logging	Customer is responsible for managing access and permissions within their tenancy via the Oracle Cloud IAM service.
2.1.4.5	The TCCM shall recover and securely control customer portal account credentials prior to mission application connectivity to the DISN.	IAM Identity Domain	Customer is responsible to configure account credentials on their end in their identity system to meet this control.

2.1.4.6	The TCCM shall create, issue, and revoke, as necessary, role-based access least privileged customer portal credentials to mission owner application and system administrators (i.e., DoD privileged users).	Identity Domain, IAM	Customer is responsible for managing access and permissions within their tenancy via the Oracle Cloud IAM service.
2.1.4.7	The TCCM shall limit, to the greatest extent possible, the issuance of customer portal and other CSP service (e.g., API, CLI) end-point privileges to configure network, application, and CSO elements.	Identity Domain	Customer is responsible for managing access and permissions within their tenancy via the Oracle Cloud IAM service.
2.1.4.8	The TCCM shall ensure that privileged users are not allowed to use CSP IdAM derived credentials which possess the ability to unilaterally create unauthorized network connections within the CSE, between the CSO and the CSP's private network, or to the Internet.	Identity Domain	Customer is responsible for managing access and permissions within their tenancy via the Oracle Cloud IAM service.

Acronyms

- BCAP: Boundary CAP
- BCND: Boundary CND
- CAC: Common Access Card
- CAP: Cloud Access Point
- CND: Computer Network Defense
- CSE: Cloud Service Environment
- CSO: Cloud Service Offerings
- CSP: Cloud Service Provider
- CSSP: Cyber Security Service Providers
- DISA: Defense Information Systems Agency
- DISN: Defense Information System Network
- DOD CIO: DOD Chief Information Officer
- DOD: Department of Defense'
- DODIN: DOD Information Network
- FRD: Functional Requirements Document
- IaaS: Infrastructure as a Service
- IL: Impact Level
- LZ: Landing Zone
- MCD: Mission Cyber Defense
- NSG: Network Security Groups
- PaaS: Platform as a Service
- PIV: Personal Identity Verification
- RoT: Root of Trust
- SaaS: software as a Service
- SCCA LZ: SCCA Landing Zone
- SCCA: Secure Cloud Computing Architecture
- SRG: Security Resource Guide
- STIG: Security Technical Implementation Guides
- TCCM: Trusted Cloud Credential Manager
- USCYBERCOM: United States Cyber Command
- VDMS: Virtual Data-center Managed Services
- VDSS: Virtual Data-center Security Services
- vTAP: Virtual Testing Access Point

Additional Information

For additional information specific to Oracle Cloud Native SCCA Solution, please reach out to the Oracle Cloud DOD Product Management team via email below.
oci-g2s-dod-prod-mgmt_us_grp@oracle.com

This paper will be updated as new guidance, requirements, design patterns, and cloud-native services are released. New or updated guidance, requirements, patterns and/or services will be released at Oracle's sole discretion.

For additional information specific to Oracle Cloud's US Federal Cloud with DISA Impact Level 5 authorization, please refer to the Oracle Cloud's US Federal Cloud with DISA Impact Level 5 Authorization website, located at:

Oracle Cloud's US Federal Cloud with DISA Impact Level 5 Authorization