Oracle Cloud Native SCCA Landing Zone (LZ)

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

October, 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 in the DoD Functional Requirements Document (FRD). It is intended solely to help the customer/mission owner understand the Oracle DoD Cloud platform and to plan your 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 Defense Information Systems Agency (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.*

Revision History

The following revisions have been made to this architecture guide:

Date	Revision
July, 2023	Initial - Cloud Native SCCA Landing Zone

Table of contents

List of figures

List of tables

Introduction

The purpose of Secure Cloud Computing Architecture (SCCA), as stated by DISA, is to provide a scalable, cost-effective approach to securing cloud-based programs under a common security architecture. This framework provides you, as a mission owner, a consistent level of security that enables the use of commercially available Cloud Service Offerings (CSO) for hosting DoD mission applications operating at all DoD Information System Impact Levels (i.e., IL2, IL4, IL5, and IL6).

Oracle's mission regarding DoD Cloud Computing is to build cloud infrastructure and platform services where you, the DoD mission owner, have effective and manageable security to run your mission-critical workloads and store your data with confidence. This architectural guide highlights DISA guidance from the DISA SCCA Functional Requirements Document (FRD), Oracle best practices, and lessons learned from working with our DoD customers deploying to Oracle Cloud.

In addition to this document, DoD cloud adopters should also reference the following DoD reference guides:

- Cloud Computing Security Requirements Guide (CC SRG) version v1r4
- Cloud Connection Process Guide (CC-PG)
- DISA Cloud Playbook (a general guide and lessons learned by early cloud adopters across the DoD)

**The Secure Cloud Computing Architecture – Functional Requirements (SCCA FRD) – version 2.9 document requires a Controlled Access Card (CAC) login.*

Benefits of Oracle Cloud Native SCCA

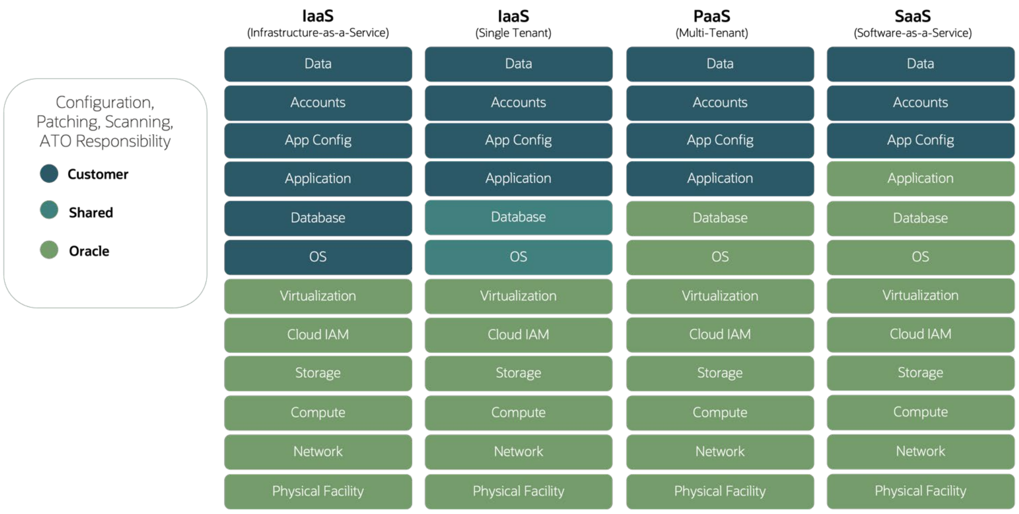
Time Savings	Oracle is working with the DoD Hosting and Computing Center to pre-ATO our Oracle Cloud Native SCCA Solution to make a compliant architecture available in hours instead of months.
Cost Avoidance	The Oracle Cloud Native SCCA Landing Zone (LZ) script and associated technical documentation are provided at no separate or additional charge under a customer's contract. Underlying consumable cloud services used to stand up Oracle Cloud Native SCCA in a customer's tenancy may be billable in accordance with the customer's contract.
Agility	Customers can use as many LZs as needed. Operations can be delegated to mission support partners with less maintenance required instead of relying on complex third-party product maintenance and the associated skills required.
Simplicity	Customers can use out-of-the-box configurations, rules, and templates instead of architecting and manually configuring on their own. Customers can leverage Oracle Cloud Infrastructure (OCI)-managed Platform as a Service (PaaS) rather than a virtual machine-based implementation. Customers can use guided security configuration with minimal decision points.

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



Configuration, Patching, Scanning, ATO Responsibility

● Customer

◐ Shared

○ Oracle

IaaS (Infrastructure-as-a-Service)	IaaS (Single Tenant)	PaaS (Multi-Tenant)	SaaS (Software-as-a-Service)
● Data	● Data	● Data	● Data
● Accounts	● Accounts	● Accounts	● Accounts
● App Config	● App Config	● App Config	● App Config
● Application	● Application	● Application	○ Application
● Database	◐ Database	○ Database	○ Database
● OS	◐ OS	○ OS	○ OS
○ Virtualization	○ Virtualization	○ Virtualization	○ Virtualization
○ Cloud IAM	○ Cloud IAM	○ Cloud IAM	○ Cloud IAM
○ Storage	○ Storage	○ Storage	○ Storage
○ Compute	○ Compute	○ Compute	○ Compute
○ Network	○ Network	○ Network	○ Network
○ Physical Facility	○ Physical Facility	○ Physical Facility	○ Physical Facility

DoD Cyber Security Service Provider (CSSP)

The DoD operates a cyber security structure as defined in DoDI 8530.01, "Cyber Security Activities Support to DoD Information Network Operations.” This structure consists of United States Cyber Command (USCYBERCOM) and Joint Forces Headquarters Department of Defense information networks (JFHQ-DoDIN) at the top organizational level and a network of Cyber Security Service Providers (CSSPs) that are accredited by USCYBERCOM IAW DoD policy. Each DoD information system is operated and managed by a mission owner which must be aligned with an accredited CSSP to monitor and protect the information systems and associated assets. CSSPs provide cybersecurity services that help protect, monitor, respond, and sustain capabilities within the Department of Defense Information Network (DoDIN). The mission owner is responsible for the implementation and maintenance of the security posture of your system(s) in accordance with Security Requirements Guides, Security Technology Implementation Guides, and DoD policy in coordination with, or with the assistance of your aligned CSSP. CSSPs report information to USCYBERCOM which maintains cyber situational awareness over all DoD networks and information systems. USCYBERCOM also provides threat information collected from various sources and threat mitigation orders to CSSPs and you as the mission owner. The CSSP provides cyber security services and command and control direction addressing the protection of the network, detection of threats, and response to incidents. DoD Program Managers must ensure that CSSP processes are in place and functional for their application prior to any transition to or use of a Cloud Service Offering (CSO).

Additional CSSP information can be found at https://cyber.mil/ (CAC required.)

Information Impact Levels

The Cloud Computing Security Requirements Guide (CC SRG) provides guidance on acquiring cloud services and understanding levels of data. Both commercial companies and government cloud providers are authorized to provide cloud offerings for different levels of data. The definitions for these data levels are defined in the CC SRG. There are now four levels of data that are used as the framework for authorizing cloud providers: Impact Level (IL) 2, 4, 5, and 6. Table 1 provides a comparison of these Impact Levels, embodying these principles:

- All DoD data is important, but not all data needs to be equally protected.
- Information Impact Levels (IILs) consider the potential impact, should the confidentiality and integrity of information be compromised.
- Once a mission owner understands their data level(s), they may determine which CSPs are authorized to provide CSOs for those levels.

Oracle Cloud is currently accredited for DoD workloads up to Information Impact Level 5 (IL2, IL4, IL5). In addition, Oracle is going through the process for IL6 accreditation. Table 1 summarizes and compares the set of Oracle Cloud regions available to various government agencies in the United States.

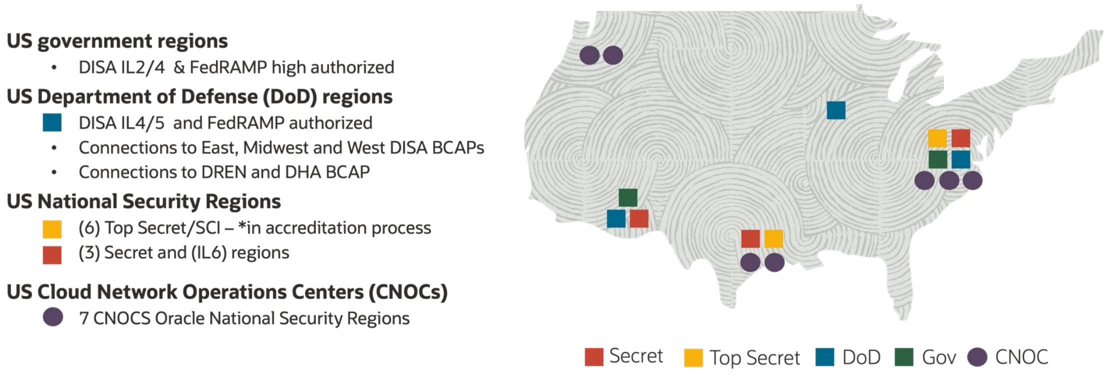
Oracle Cloud Regions

Table 1. Authorization, Connectivity, and Impact Levels

Realm	Region	Authorization and Impact Levels	Customers	Connectivity
[OC2]	US Gov East [Gov 1] US Gov West [Gov 2]	FedRAMP High (JAB) DoD Impact Level 4	US Federal, State, Local, Tribal, Higher Ed, Approved Commercial Entities	Internet FastConnect
[OC3]	US DoD East [Gov 3] US DoD North [Gov 4] US DoD West [Gov 5]	FedRAMP High (JAB) DoD Impact Level 5	Federal Government Community Cloud US Intel Community	Internet NIPRNet (via BCAP)
[OC11]	US Secret East [Gov 13] US Secret West [Gov 14] US Secret S. Central [Gov 15]	DoD Impact Level 6* Intelligence Community Directive (ICD) 705* ICD 503*	US DoD US Intel Community	SIPRNet FastConnect
[OC6]	US TS East [Gov 9] US TS South Central [Gov 6]	DoD Impact Level 6* ICD 705* ICD 503*	US DoD US Intel Community	Joint Worldwide Intelligence Communication System (JWICS) FastConnect
[OC7]	US TS East [Gov 7]	ICD 705* ICD 503*	Special Access Program (SAP)	JWICS FastConnect

**Some of the services are under accreditation by DISA or the U.S. Intelligence Community and may not be available as a general release. US personnel are required for all US government realms.*

Figure 2. Oracle Cloud Regions Map for US Government



US government regions

- DISA IL2/4 & FedRAMP high authorized

US Department of Defense (DoD) regions

- 🟦 DISA IL4/5 and FedRAMP authorized
- Connections to East, Midwest and West DISA BCAPs
- Connections to DREN and DHA BCAP

US National Security Regions

- 🟨 (6) Top Secret/SCI – *in accreditation process
- 🟥 (3) Secret and (IL6) regions

US Cloud Network Operations Centers (CNOCs)

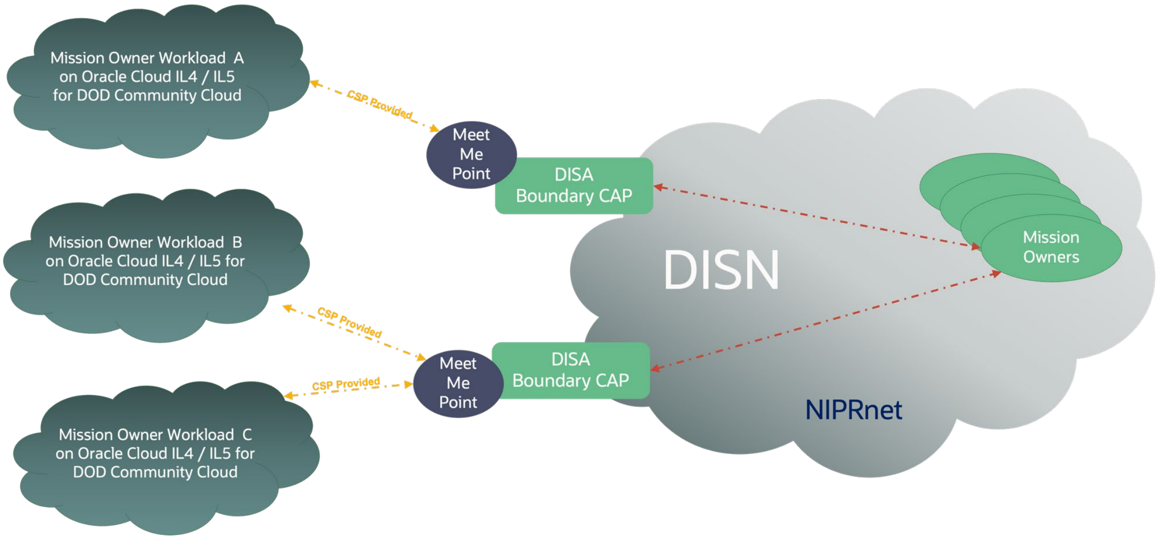
- ● 7 CNOCS Oracle National Security Regions

DoD Boundary Cloud Access Point (BCAP)

A DoD Boundary Cloud Access Point (BCAP) is a system of network boundary protection and monitoring devices, otherwise known as an information assurance stack, through which cloud service provider infrastructure and networks will connect to the Defense Information Systems Network (DISN). Figure 3 illustrates this logical architecture.

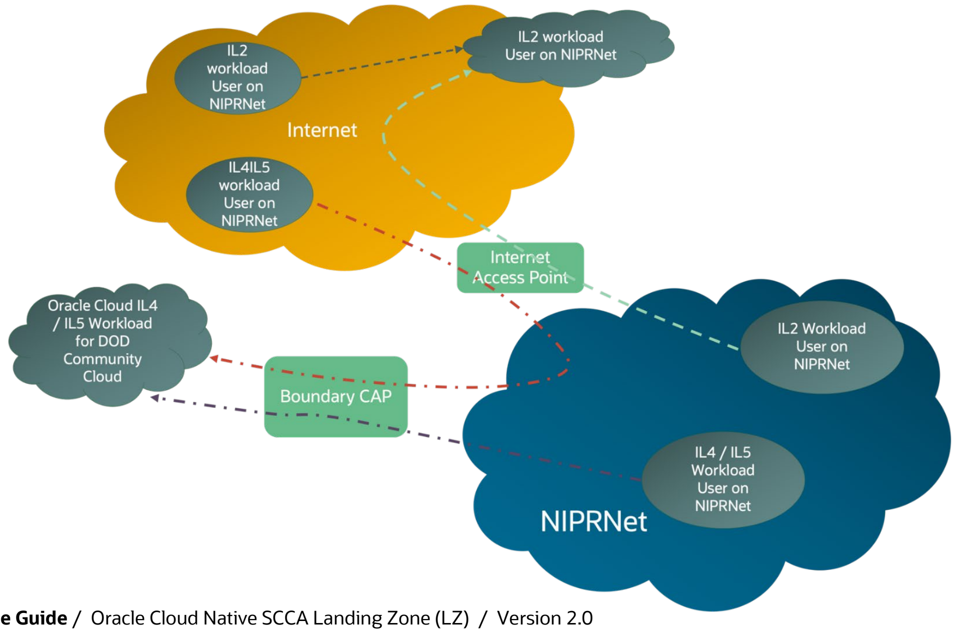
- A BCAP is not an architecture or service provided by a Cloud Service Provider (CSP) but required between the DISN and the Cloud Service Offering (CSO) with controlled unclassified information data (IL4/5).
- The BCAP is used to protect the DISN, systems, information, and users residing on the DISN from attacks that may be launched from within a compromised cloud service offering. The BCAP facilitates protected connections between users on a DoD network and systems or applications on the CSO.

Figure 3. DoD Boundary Cloud Access Points (BCAPs)


Mission Owner Workload A on Oracle Cloud IL4 / IL5 for DOD Community Cloud
CSP Provided
Meet Me Point
DISA Boundary CAP
Mission Owner Workload B on Oracle Cloud IL4 / IL5 for DOD Community Cloud
CSP Provided
CSP Provided
Meet Me Point
DISA Boundary CAP
Mission Owner Workload C on Oracle Cloud IL4 / IL5 for DOD Community Cloud
DISN
Mission Owners
NIPRnet

Oracle offers connectivity to two DISA MeetMe points – East and West. Oracle also coordinates connectivity to component CAPs, such as the Defense Health Agency (Med COI) CAP. If you utilize networks other than NIPRNet or SIPRNet, you will need to implement BCAPs or Internet Cloud Access Points (ICAPs) for those networks that provide equivalent protections to those defined in the SCCA FRD when connecting CSP infrastructure to your network. All CAP instantiations, user connections to cloud service providers, and cloud service offerings must be approved by the DoD CIO.

Figure 4. NIPRNet and Oracle Cloud Workload Data Transfer


IL2 workload User on NIPRNet
IL2 workload User on NIPRNet
Internet
IL4IL5 workload User on NIPRNet
Internet Access Point
Oracle Cloud IL4 / IL5 Workload for DOD Community Cloud
Boundary CAP
IL2 Workload User on NIPRNet
IL4 / IL5 Workload User on NIPRNet
NIPRNet

A CAP does not support or provide direct internet access to an Information Impact Level 4/5 CSP-CSO. Information exchanges between a Level 4/5 CSP-CSO and the internet must transit both an Internet Access Point (IAP) and a CAP. As the DoD "Cloud Connection Process Guide" explains, and Figure 4 illustrates, the information flows for Information Impact Levels 2, 4, and 5. These are:

BCAP

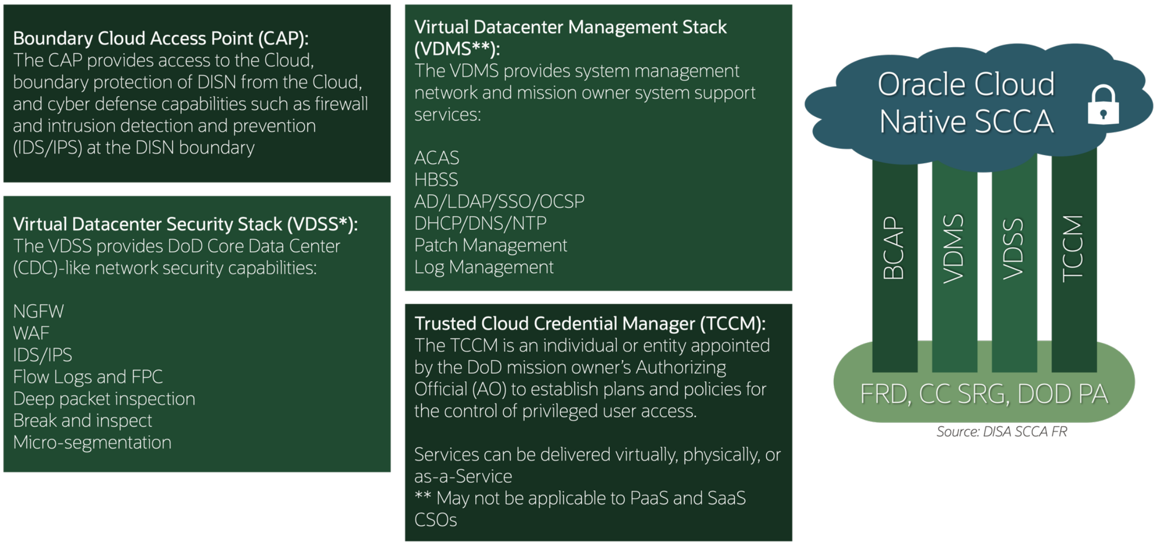
Table 2. BCAP Flow Descriptions

Flow #	Flow description
1.7.a	Information exchanges between a user connected to the NIPRNet and a Cloud Information Technology Project (C-ITP) operating in an Off-Premise Information Impact Level 4 (or 5) CSP-CSO must traverse a DoD CIO-approved BCAP.
1.7.b	Information exchanges between a user connected to the internet and a C-ITP operating in an Off-Premises Information Impact Level 4 or 5 CSP-CSO must traverse a DoD Internet Access Point (IAP), and a DoD CIO-approved BCAP.
1.7.c	Information exchanges between a user connected to the NIPRNet and a C-ITP operating in an Information Impact Level 2 CSP-CSO connected to the internet must traverse a DoD IAP.
1.7.d	Information exchanges between a user connected to the internet and a C-ITP operating in an Information Impact Level 2 CSP-CSO connected to the Internet are direct via the internet.

DoD SCCA and DISA Secure Cloud Computing

SCCA is designed to deliver the security capabilities defined by the DoD Cloud Computing Requirements Guide (CC SRG) as necessary to support secure deployment of DoD systems and information into the commercially owned and operated CSP industry segment. A DoD Provisional Authorization (PA) provides a validation of a CSP's compliance with the DoD CC SRG guidance for hosting systems operating at an indicated DoD System Impact Level. Assuming a CSP has achieved a DoD PA, the SCCA defines DoD system implementation and governance requirements necessary to protect the DISN boundary and commercial cloud hosted DoD mission systems and information. The construction of the SCCA is intended to levy no additional requirements upon the commercial CSP industry other than those related to secure connectivity.

Figure 5. DoD Secure Cloud Computing Architecture



Boundary Cloud Access Point (CAP): The CAP provides access to the Cloud, boundary protection of DISN from the Cloud, and cyber defense capabilities such as firewall and intrusion detection and prevention (IDS/IPS) at the DISN boundary

Virtual Datacenter Security Stack (VDSS*): The VDSS provides DoD Core Data Center (CDC)-like network security capabilities:

NGFW
WAF
IDS/IPS
Flow Logs and FPC
Deep packet inspection
Break and inspect
Micro-segmentation

Virtual Datacenter Management Stack (VDMS**): The VDMS provides system management network and mission owner system support services:

ACAS
HBSS
AD/LDAP/SSO/OCSP
DHCP/DNS/NTP
Patch Management
Log Management

Trusted Cloud Credential Manager (TCCM): The TCCM is an individual or entity appointed by the DoD mission owner's Authorizing Official (AO) to establish plans and policies for the control of privileged user access.

Services can be delivered virtually, physically, or as-a-Service
** May not be applicable to PaaS and SaaS CSOs

Source: DISA SCCA FR

SCCA Technical Components

The SCCA FRD describes the following four technical components:

1. **Cloud Access Point (CAP):** The CAP provides access to the cloud, boundary protection of DISN from the cloud, and cyber defense capabilities such as firewall and intrusion detection and prevention (IDS/IPS) at the DISN boundary. Full Packet Capture (FPC) and interface translation may be provided, as needed, to support secure connectivity and access to individual commercial cloud hosting systems. The CAP is specifically tailored to operate at DoD Impact levels 4 and 5. To support both on-premises and off-premises non-DoD CSPs, CAP requirements are decomposed into Internal-CAP (ICAP) and Boundary-CAP (BCAP) requirements.
2. **Virtual Datacenter Security Stack (VDSS):** The VDSS provides DoD Core Data Center (CDC)-like network security capabilities, such as:
    - Next-generation firewall (NGFW)
    - Web application firewall (WAF)
    - IDS/IPS
    - Flow Logs and FPC
    - Deep packet inspection
    - Break and inspect
    - Micro-segmentation

    The VDSS provides DoD CDC-like network security capabilities such as firewall, intrusion detection, and intrusion prevention systems. It also provides application security capabilities such as WAF and proxy systems. The VDSS can reside within or outside of the CSP's infrastructure virtually or physically. VDSS capabilities can also be provided as-a-service by a third-party vendor for IaaS or a CSP for IaaS and SaaS. VDSS feeds should be provided to a DoD Cyber Security Service Provider (CSSP) performing enclave boundary defense. The VDSS also supports sharing of security event data among cyber security stakeholders. The VDSS is specifically tailored to operate at all DoD Information Impact Levels.
3. **Virtual Datacenter Managed Services (VDMS):** The VDMS provides system management network and mission owner system support services, such as:
    - Assured Compliance Assessment Solution (ACAS)
    - Host Based Security System (HBSS)
    - Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) / Single Sign-on (SSO) / Online Certificate Status Protocol (OCSP)
    - Dynamic Host Configuration Protocol (DHCP) / Domain Name System (DNS) / Network Time Protocol (NTP)
    - Patch Management
    - Log Management

    The VDMS provides system management network and mission owner system support services necessary to achieve Joint Information Environment (JIE) management plane connectivity and mission owner system compliance. It provides secure management network connectivity to the DISN, virtual host-based management services, and identity and access management services for DoD CAC authentication to virtual systems. The VDMS is specifically tailored to operate at all DoD mission Impact Levels. VDMS functionality applies directly to IaaS environments but may not be specifically applicable to PaaS and SaaS CSOs as such functionality may be inherent to the associated CSP and validated through the DoD PA.
4. **Trusted Cloud Credential Manager (TCCM):** The TCCM is an individual or entity appointed by the DoD mission owner's Authorizing Official (AO) to establish plans and policies for the control of privileged user access to include root account credentials used to establish, configure, and control a mission owner's Virtual Cloud Network (VCN) configuration once connected to the DISN.

    The TCCM is an SCCA business role responsible for credential management with the purpose of enforcing least privilege access for privileged accounts that are established and managed using the CSP's Identity and Access Management (IdAM) The TCCM establishes and manages Least-Privilege Attribute-Based Access Control (ABAC) accounts and credentials used by privileged DoD users and systems to administer and control DoD CSO configurations. The role of TCCM is intended to operate at all DoD information Impact Levels. However, the TCCM may not apply to some SaaS solutions where DoD account owners are not required to use the CSP's IdAM system to administer user accounts and service configurations.

SCCA Roles and Responsibilities

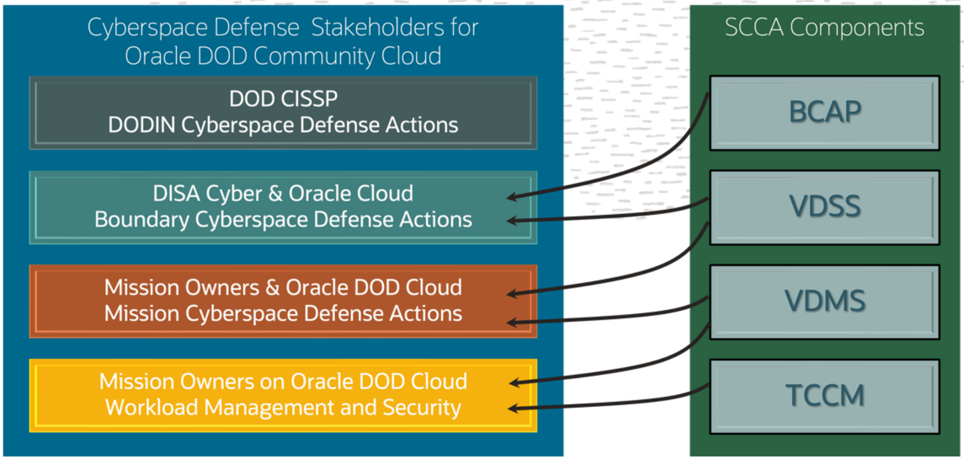
The SCCA is architected to support three primary roles and responsibilities:

1. **Mission Owner (MO):** The DoD entity responsible for delivering and operating a DoD mission system.
2. **Mission Cyberspace Protection (MCP):** The DoD entity charged with the responsibility of securing a MO's enclave and networked systems by establishing and delivering cybersecurity capabilities.
3. **DISN Boundary Cyberspace Protection (BCP):** The DoD entity charged with the responsibility to establish and deliver cyber security capabilities to protect the DISN.

Figure 6 illustrates the alignment of SCCA Components (right side) to stakeholder communities (left side):

1. **CAP:** Cyber security information from the CAP supports the mission of the organization providing BCP.
2. **VDSS:** Cyber security information from the VDSS supports the missions of organizations providing both BCP and MCP.
3. **VDMS:** The VDMS acts similarly to support the missions of organizations providing both MCP and missions.
4. **TCCM:** Establishment and execution of TCCM governance activities is specifically a MO responsibility.

Figure 6. Roles and Responsibilities for Individual SCCA Components


Cyberspace Defense Stakeholders for Oracle DOD Community Cloud
DOD CISSP
DODIN Cyberspace Defense Actions
DISA Cyber & Oracle Cloud
Boundary Cyberspace Defense Actions
Mission Owners & Oracle DOD Cloud
Mission Cyberspace Defense Actions
Mission Owners on Oracle DOD Cloud
Workload Management and Security
SCCA Components
BCAP
VDSS
VDMS
TCCM

SCCA Requirements: Security and Mission Support Systems

The SCCA Functional Requirements Document (FRD) lists requirements in the following categories:

- 2.1 Security Requirements
- 2.2 System Connectivity Requirements
- 2.3 Mission Support System Requirements
- 2.4 Performance
- 2.5 Continuity of Operations (COOP)
- 2.6 System Scalability
- 2.7 Backup & Restoration

SCCA Requirements

Table 3. Security Objectives and Components

Within **Security Requirements**, the FRD identifies four objectives and allocates them to SCCA components:

Security objective	Allocated SCCA component	In this document
DISN Boundary Defense	CAP	No
Mission Owner Enclave and Application Defense	VDSS	Yes
Mission Application End-Point Defense	VDMS	Yes
DISN and Mission Defense	TCCM	Yes

The pages that follow provide Oracle Cloud specific guidance in these categories:

- 2.1.2 Security Requirements: VDSS
- 2.1.3 Security Requirements: VDMS
- 2.1.4 Security Requirements: TCCM
- 2.3.5 Mission Support Systems: Full Packet Capture

SCCA Functional Requirements

Table 4. Virtual Datacenter Security Stack (VDSS) Requirements

Functional Requirements: VDSS Oracle Cloud Guidance

Req. ID	VDSS Security Requirements	Oracle Cloud Native Services
2.1.2.1	The VDSS shall maintain virtual separation of all management, user, and data traffic.	IP Address Management (IPAM), Security List, VCN, Subnets
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
2.1.2.11	The VDSS shall provide a monitoring capability that captures log files and event data for cyber security analysis.	Logging Analytics, Oracle Access Manager (OAM), Oracle Identity Manager (OIM), Oracle Enterprise Manager (OEM), Oracle Cloud Monitoring
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 Computer Network Defense (CND) activities.	Logging, Service Connector Hub, Object Storage

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
2.1.2.14	The VDSS shall provide the capability to detect and identify application session hijacking.	Network Firewall/WAF v2
2.1.2.15	The VDSS shall provide a DoD DMZ Extension to support Internet Facing Applications (IFAs).	Network Firewall/WAF v2
2.1.2.16	The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communications.	vTAP
2.1.2.17	The VDSS shall provide network packet flow metrics and statistics for all traversing communications.	vTAP
2.1.2.18	The VDSS shall provide for the inspection of traffic entering and exiting each mission owner virtual private network.	Virtual Test Access Points (vTAP)
2.1.2.2	The VDSS shall allow the use of encryption for segmentation of management traffic.	VCN
2.1.2.3	The VDSS shall provide a reverse proxy capability to handle access requests from client systems.	Web App Acceleration
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
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
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
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
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

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 Cloud Service Environment (CSE).	WAF/Network Firewall, Oracle Cloud Observability and Management Platform
2.3.1.2	The VDSS shall provide CSO resident or remotely hosted mission enclave perimeter protection and sensing.	Network Firewall, IPAM, VCN, Subnets, Security Lists
2.3.2.2	SCCA component managers shall be able to manage (e.g., set security, configuration, & routing policies and install patches) SCCA system security and network components.	APIs, Console, Security List, OS Management
2.3.2.3	SCCA component managers shall allow for the configuration, control, and management of Ports, Protocols, and Services Management (PPSM) in accordance with DoDI 8551.0120.	Security List, Network Firewall
2.3.2.6	SCCA components shall provide logically separate network interfaces for access from the management network infrastructure that is logically separate from production.	Oracle Cloud Networking
2.3.2.7	SCCA components shall support management administration from the DISN management system and/or DISA Datacenter Management System.	Oracle Cloud Console, Identity Domain
2.3.2.9	SCCA components shall provide for management traffic segmentation from user and data plane traffic.	Oracle Cloud Networking
2.4.2.1	The VDSS unit processing latency shall be no greater than 35 milliseconds.	Oracle Cloud Networking
2.4.2.2	The VDSS unit packet loss shall be <1%.	Oracle Cloud Networking
2.4.2.5	The VDSS shall support IP packet forwarding in accordance with Mission Owner Differentiated Services Code Point (DSCP) tagged QOS prioritization.	Oracle Cloud Networking
2.5.2.1	The VDSS management systems shall provide a mechanism for managing failover in accordance with DoD UCR 2013.	Oracle Cloud Networking
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 Availability Networking
2.5.2.3	The VDSS shall maintain offsite backup configurations for the recovery of operations.	Cross-region Replication (Object Storage)
2.5.3.1	The VDMS management systems shall provide a mechanism for managing failover.	Oracle Cloud Networking
2.6.2.1	The VDSS shall be designed to rapidly scale virtual elements up and down in capacity to achieve negotiated (between components provider and Mission Owner) SLA objectives while minimizing metered billing CSO costs incurred by DoD procuring component.	Organization Management, Billing / Budget Instance pool

2.6.2.2	The VDSS shall support scalability in increments of 1 Gigabit/second throughput at all points within the design without costly modification.	Oracle Cloud Networking
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
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
2.7.2.3	The VDSS shall provide the means to restore operational capability.	Backup, Object storage, Archive storage

SCCA Functional Requirements

Table 5. Virtual Datacenter Managed Services (VDMS) Requirements

Functional Requirements: VDMS Oracle Cloud Guidance

Req. ID	VDMS Security Requirements	Oracle Cloud Native Services
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
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
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, OS Management Service Repo, YUM
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
2.1.3.6	The VDMS shall provide a network for managing systems and applications within the CSE that is logically separate from the user and data networks.	Dynamic Routing Gateway (DGR), Local Peering Gateway (LPG), Security Lists, VCN, Subnets

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
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
2.1.3.9	The VDMS shall implement the technical capabilities necessary to execute the mission and objectives of the TCCM role.	Identity and Access Management (IAM), Identity Domains
2.2.3.1	The VDMS enclave shall form the DISN management network within the CSE.	Oracle Cloud Networking
2.2.3.2	The VDMS shall allow DoD privileged user access to mission owner management interfaces inside the CSO.	IAM
2.2.3.3	The VDMS shall provide secure connectivity to mission owner management systems inside the CSO that is logically separate from mission application traffic.	Oracle Cloud Networking
2.2.4.5	(Optional) The VDMS enclave shall form the DISN management network within the CSE and provide the same capabilities identified in Table 9.	Oracle Cloud Networking, Identity Domain
2.3.2.1	SCCA components shall provide element managers to manage the configuration of system elements comprising the CAP, VDSS, and the VDMS.	Console
2.3.2.4	SCCA component managers shall provide a capability to implement and control system configuration, report configuration change incidents, and support DoD Component change configuration management systems and processes.	Oracle Cloud Resource Manager, Terraform
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.	Oracle Cloud Analytics, Identity Domain, Oracle Cloud Logging, Oracle Cloud Logging Analytics, Service Connector Hub *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.	Logging, Identity Domain, Service Connector Hub *Customers are responsible for Log Insight Detector

2.3.3.1	SCCA security elements (i.e., BCAP, ICAP, VDSS, and VDMS) shall provide a performance management capability to monitor the health and status of security elements.	Oracle Cloud Monitoring, Observability and Management Platform
2.3.3.2	SCCA security elements shall provide performance data, such as CPU, bandwidth, memory and disk I/O, and storage utilization to SCCA management systems for performance analysis and reporting.	Oracle Cloud Monitoring, Metrics, Logging
2.3.3.3	The SCCA security elements shall be able to generate reports and alerts based on performance information provided by SCCA systems.	Oracle Cloud Monitoring, Metrics, Logging
2.3.5.1	The FPC shall support integration with log insight detector systems to effect data search and retrieval, such as the capability to pull select timeframes of captured data.	vTaP *Customers are responsible for Log Insight Detector
2.3.5.2	The FPC shall provide the means to reconstruct all network traffic sessions traversing the SCCA Component.	vTaP
2.3.5.3	The FPC shall provide defined data queries that run against metadata.	vTaP
2.3.5.4	The FPC shall provide a capability to request an arbitrary subset of packets.	vTaP
2.3.5.5	The FPC shall locally store captured traffic for 30 days.	vTAP, Object Storage
2.3.5.6	The FPC data shall be isolated from user and data plane traffic via cryptographic or physical means.	vTaP
2.3.5.7	The FPC data shall be query-able from a secure remote location on the management network.	vTaP
2.3.5.8	The FPC function shall be configurable according to traffic flow source and destination points to avoid multiple point capture.	vTaP
2.5.3.2	The VDMS management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable.	Oracle Cloud High Availability Networking
2.5.3.3	The VDMS shall maintain offsite backup configurations for the recovery of operations.	Cross-region Replication (Object Storage)
2.6.3.1	The VDMS shall be designed to rapidly scale virtual elements up and down in capacity to achieve negotiated (between components provider and Mission Owner) SLA objectives while minimizing metered billing CSO costs incurred by DoD procuring component.	Organization Management, Billing / Budget Instance pool

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
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
2.7.3.3	The VDMS shall provide the means to restore operational capability.	Backup, Object storage, Archive storage

Mission Support Systems

Table 6. Full Packet Capture Requirements

Mission Support Systems: Full Packet Capture Oracle Cloud Guidance

Req. ID	Full Packet Capture (FPC) Requirements	Oracle Cloud Native Services
2.3.5.1	The FPC shall support integration with log insight detector systems to effect data search and retrieval, such as the capability to pull select timeframes of captured data.	vTAP *Customers are responsible for Log Insight Detector
2.3.5.2	The FPC shall provide the means to reconstruct all network traffic sessions traversing the SCCA Component.	vTAP
2.3.5.3	The FPC shall provide defined data queries that run against metadata.	vTAP
2.3.5.4	The FPC shall provide a capability to request an arbitrary subset of packets.	vTAP
2.3.5.5	The FPC shall locally store captured traffic for 30 days.	vTAP, Object Storage Lifecycle
2.3.5.6	The FPC data shall be isolated from user and data plane traffic via cryptographic or physical means.	vTAP
2.3.5.7	The FPC data shall be query-able from a secure remote location on the management network.	vTAP
2.3.5.8	The FPC function shall be configurable according to traffic flow source and destination points to avoid multiple point capture.	vTAP

Boundary Cloud Access Point (BCAP)

Table 7. Boundary Cloud Access Point (CAP) Requirements

Functional Requirements: BCAP Oracle Cloud Guidance

Req. ID	Boundary Cloud Access Point Requirement	Oracle Cloud Native Services
2.2.1.1	The BCAP and ICAP shall extend the DoDIN into the virtual network of the CSE.	Oracle Cloud VCN, FastConnect, DRG

2.2.1.2	The BCAP shall provide a network connection to established MeetMe Points in order to route DISN traffic to impact level 4 & 5 mission applications hosted in Off-Premises CSEs.	FastConnect
2.2.1.3	The MeetMe facility shall provide the capability to host a DISN endpoint router and provide cross connect transport to a CSP router.	Oracle Cloud Infrastructure
2.2.1.4	The BCAP shall provide a capability to simultaneously connect to multiple CSPs via a MeetMe Point.	Oracle Cloud Networking
2.2.4.2	The ICAP shall allow secure client access to the by CSP privileged users to CSP owned and operated management network.	Oracle Cloud Networking, Identity Domain, Bastion
2.2.4.3	The ICAP shall allow the transfer of security sensor data from the mission owner virtual networks to the DISN management network.	Oracle Cloud Networking
2.2.4.4	The ICAP shall provide network traffic isolation between the CSP's privileged user (i.e., CSP Personnel) management network and DoD Mission Owner virtual networks.	Oracle Cloud Networking, Identity Domain
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
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
2.2.5.9	(Optional) The BCAP shall provide network address translation (NAT) to translate public IP to DISN IP when Software-as-a-Service (SaaS) CSOs require the use of public IP.	NAT Gateway
2.3.1.1	The BCAP, ICAP, and VDSS shall allow approved ports and protocols communications to include whitelisted mission application traffic & services access from internet via the DISN Internet Access Point (IAP).	Ports, Protocols, and Services Management (PPSM)
2.3.1.3	The BCAP, ICAP, and VDSS shall allow secure connections to the mission owner application enclave for user plane traffic sourced from within the DISN or the internet via the IAP.	Network Firewall, IPAM, VCN, Subnets, Security Lists
2.3.1.4	The BCAP, ICAP, and VDSS shall provide for logical separation of mission owner application networks.	Network Firewall, IPAM, VCN, Subnets, Security Lists

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 (DRGv2 and transit route via backbone to another region)
2.5.1.2	The BCAP/ICAP shall maintain online backup configurations for recovery of operations.	Backup, Object storage, Archive storage
2.5.1.3	The BCAP/ICAP management systems shall provide a mechanism for managing failover.	Oracle Cloud DR (DRGv2 and transit route via backbone to another region)
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, Backup, Object storage, Archive storage
2.5.1.5	The BCAP/ICAP shall maintain offsite backup configurations for the recovery of operations.	Cross-region Replication (Object Storage)
2.6.1.1	The BCAP/MeetMe shall be designed to scale to meet the bandwidth and session demands of all projected CSO hosted mission applications and to support accessibility by multiple CSPs.	Oracle Cloud Networking
2.6.1.2	In the event of a failover, the surviving BCAP/MeetMe at an alternate site shall have sufficient capacity to meet the combined bandwidth and session demands of its own plus those failed over from the other site.	Oracle Cloud Infrastructure
2.6.1.3	The BCAP/ICAP shall support scalability of up to 10 Gigabit/second throughput at all points within the design.	Oracle Cloud Infrastructure
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
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
2.7.1.3	The BCAP/ICAP shall provide the means to restore operational capability.	Backup, Object storage, Archive storage

Trusted Cloud Credential Manager (TCCM)

Table 8. Trusted Cloud Credential Manager (TCCM) Requirements

Functional Requirements: TCCM Oracle Cloud Guidance

Req. ID	Trusted Cloud Credential Manager Requirements	Oracle Cloud Native Services

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
2.1.4.2	The TCCM shall collect, audit, and archive all Customer Portal activity logs and alerts.	IAM, Object Storage, Logging
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
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
2.1.4.5	The TCCM shall recover and securely control customer portal account credentials prior to mission application connectivity to the DISN.	Identity Domain, IAM
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
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
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

Oracle Cloud Native SCCA LZ Reference Architecture

Figure 7. SCCA Deployment Concepts

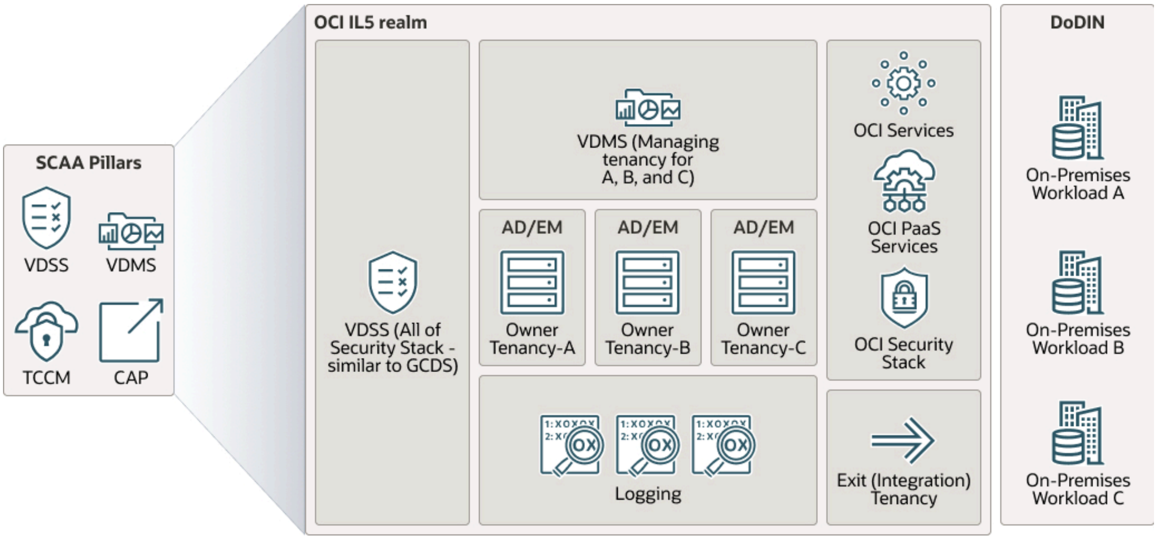


Figure 7 above represents the reference architecture for the Cloud Native SCCA Landing Zone that provides the abstract building blocks for constructing SCCA components and configurations for you to become SCCA compliant. You may deploy this architecture based on OCI cloud native services found here. This reference architecture is based on the DISA FRD and has components of CAP/BCAP, VDSS, VDMS, and TCCM.

Oracle Cloud Native SCCA LZ Reference Architecture for TCCM

Figures 7 and 8 represent high-level SCCA concepts and a reference architecture for deploying your SCCA within an Oracle Cloud tenancy.

Figure 8. Trusted Cloud Credential Manager

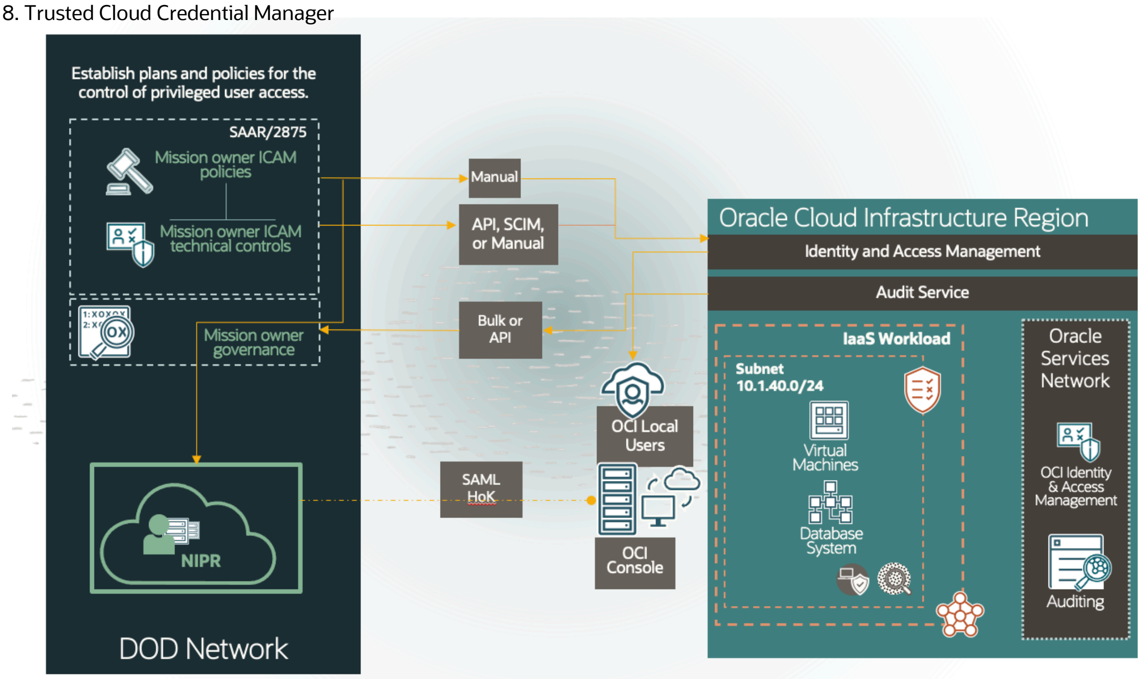

Establish plans and policies for the control of privileged user access.
SAAR/2875
Mission owner ICAM policies
Mission owner ICAM technical controls
Mission owner governance
NIPR
DOD Network
Manual
API, SCIM, or Manual
Bulk or API
SAML HoK
OCI Local Users
OCI Console
Oracle Cloud Infrastructure Region
Identity and Access Management
Audit Service
IaaS Workload
Subnet 10.1.40.0/24
Virtual Machines
Database System
Oracle Services Network
OCI Identity & Access Management
Auditing

Figure 8 shows the DoD Identity, Credential and Access Management (ICAM), OCI Identity and Access Management (IAM), and Identity Domain Services controlling access on a least trust model design. Your DoD network users access the OCI tenancy and workloads through ICAM policies and CAC authorization. Oracle only authenticates users via CAC, X.509, Public Key Infrastructure (PKI), or an external authentication method that is supported and authorized by the DoD. Welcome emails are sent to the mission owner and administrator. Oracle recommends federating or authenticating from CAC to the DoD user database and disabling local users' and local administrators' logins. OCI IAM provides OCI Audit to users who need access to auditing management.

Oracle Cloud Native SCCA Landing Zone Monitoring Architecture

Figure 9. Oracle Cloud SCCA LZ Monitoring Architecture

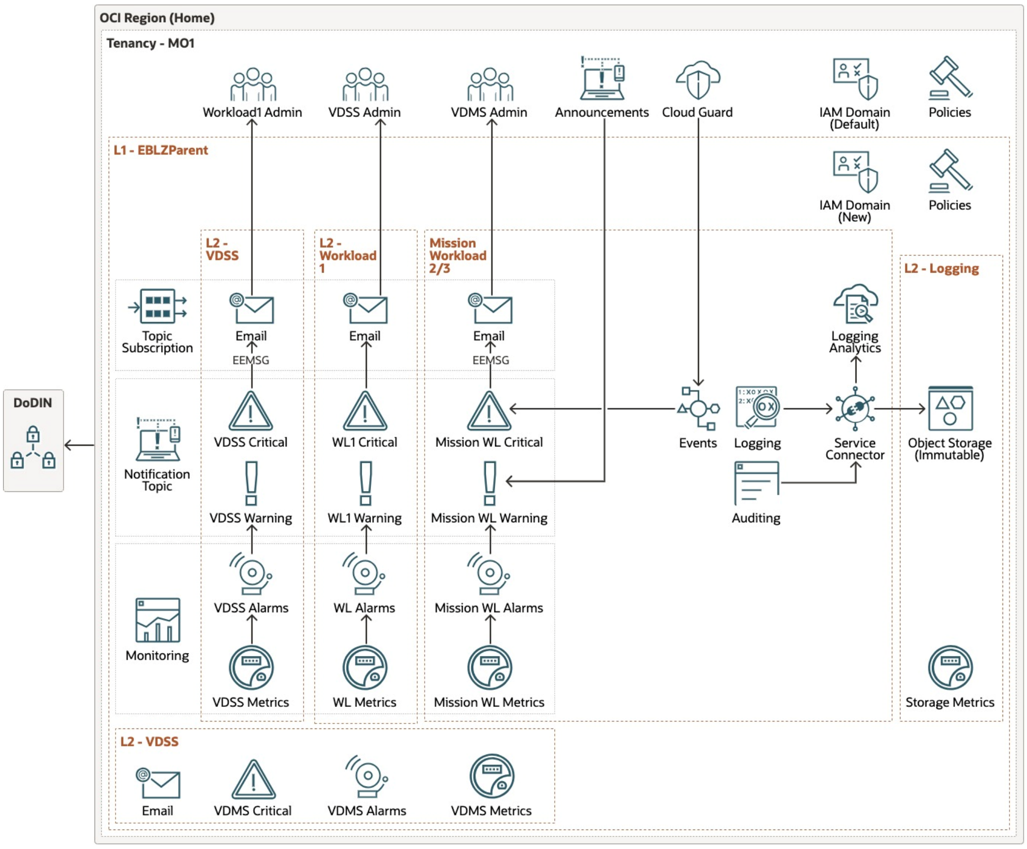
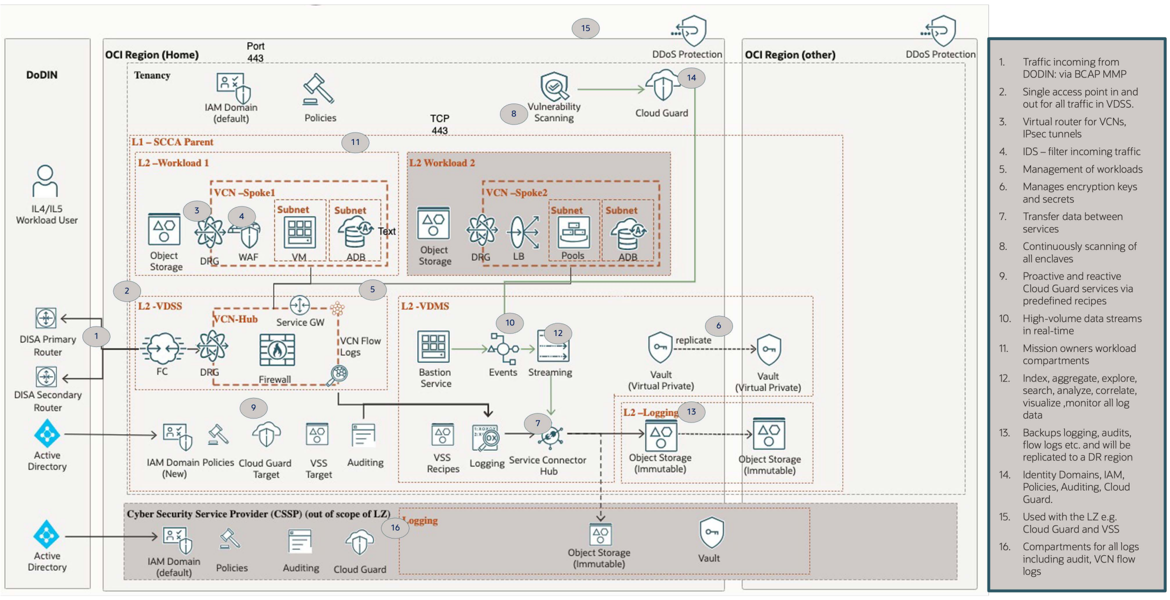


Figure 9 above represents several services that provide you monitoring capabilities across your tenancy. Services include but not are not limited to Object Storage, Events, Notifications, and Logging Analytics. These services are part of our OCI Monitoring Platform which may be referenced from this link.

As part of this Cloud Native SCCA solution, there is a monitoring structure in the VDSS, VDMS, and workload compartments that fulfills your initial SCCA requirement. This may be adjusted according to your administrators operational model. Services inside OCI provide metrics and events that may be monitored through your metrics dashboard. You may create alerts based upon queries of these metrics and events. You may organize these alerts into groups with topics you create. You may create different topics by compartment (VDSS, VDMS and workload) and assign different monitoring rules assigned to them.

Oracle Cloud Native SCCA LZ Functional Architecture

Figure 10. Oracle Cloud SCCA LZ Functional Architecture



1. Traffic incoming from DODIN: via BCAP MMP
2. Single access point in and out for all traffic in VDSS.
3. Virtual router for VCNs, IPsec tunnels
4. IDS – filter incoming traffic
5. Management of workloads
6. Manages encryption keys and secrets
7. Transfer data between services
8. Continuously scanning of all enclaves
9. Proactive and reactive Cloud Guard services via predefined recipes
10. High-volume data streams in real-time
11. Mission owners workload compartments
12. Index, aggregate, explore, search, analyze, correlate, visualize ,monitor all log data
13. Backups logging, audits, flow logs etc. and will be replicated to a DR region
14. Identity Domains, IAM, Policies, Auditing, Cloud Guard.
15. Used with the LZ e.g. Cloud Guard and VSS
16. Compartments for all logs including audit, VCN flow logs

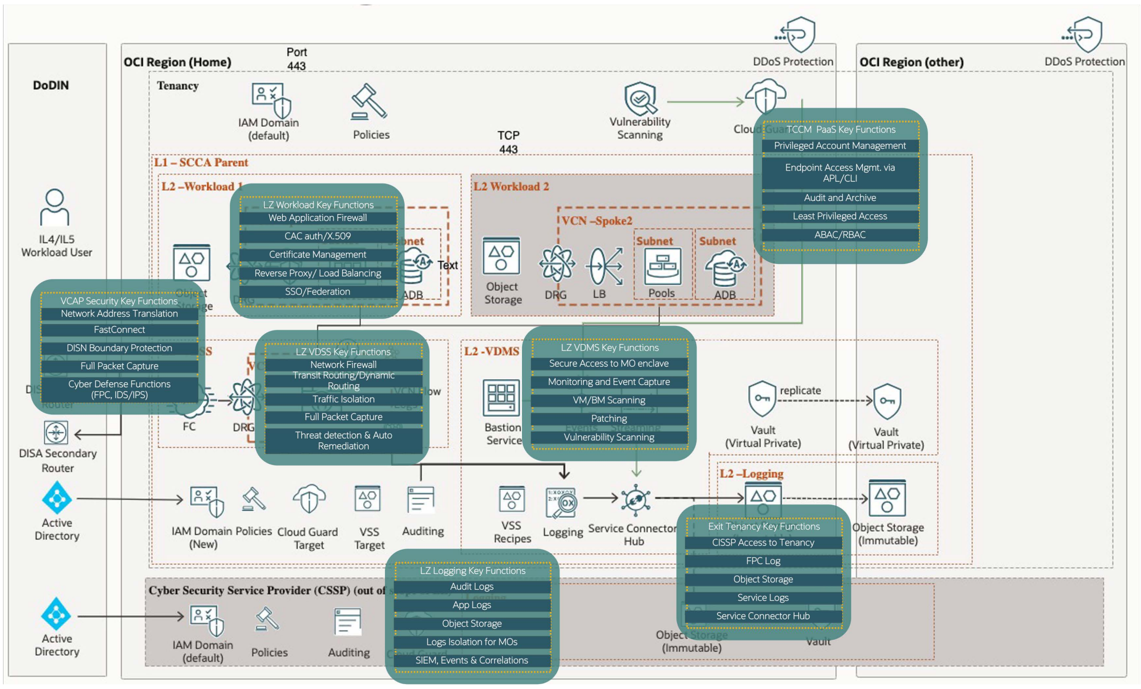
Figure 10 above represents the functions of individual components of our Cloud Native SCCA LZ solution for you as the mission owner.

- **DISA BCAP connection with OCI at MMP:** Security capabilities provided by inspect and filter, Cyber Defense Functions (FPC, IDS/IPS), NAT Gateway, FastConnect, and others.
- **Mission Owners' workload tenancies:** Application security provided by Web Application Firewall, CAC authorization, certificate management, reverse proxy, load balancing, SSO, federation, and others.
- **VDSS: Network Security Functions**: Network firewall, transit routing, traffic isolation, FPC, threat detection/auto-remediation, and others.
- **VDMS: Virtual Datacenter Managed Services:** Secure access to mission owner enclave, monitoring and event capture, key management, VM scanning, patching, vulnerability scanning, and others.
- **Logging:** Audit logs, application logs, Object Storage, log isolation for mission owners, events, correlations, and others.
- **Trusted Cloud Credential Manager (TCCM):** Tenancy-wide functions include privileged account management, endpoint access management via API/CLI, audit, security logs, least privilege access, and Attribute Based Access Control (ABAC).
- **CSSP Access to Tenancy:** FPC Log, Object Storage, service logs accessible via Service Connector Hub, and others.

Oracle Cloud Native SCCA LZ Functional Flow Architecture

Figure 11 below represents the functional flow of our Cloud Native SCCA LZ solution we provide you as the mission owner.

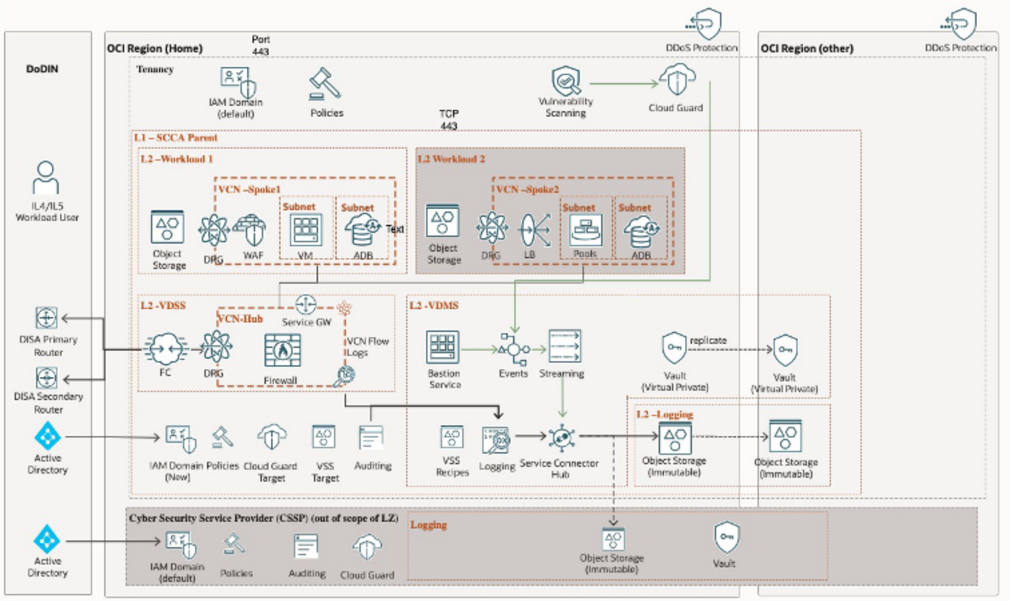
Figure 11. Oracle Cloud SCCA LZ Functional Flow Architecture



- **DoDIN or On-premises:** The CAP Inspects and Filters Cyber Defense Functions (FPC, IDS/IPS), NAT Gateway, and FastConnect.
- **VDSS:** These network security functions include Network Firewall, transit routing, traffic isolation, Full Packet Capture (FPC), threat detection, and auto-remediation.
- **Virtual Datacenter Managed Services:** This mission owner enclave includes monitoring and event capture, key management, VM scanning, patching, and vulnerability scanning.
- **Logging:** Our solution includes audit logs, application logs, Object Storage, log isolation for mission owners, events, and correlations.
- **Application Security:** Our Security includes Web Application Firewall (WAF), CAC authorization, certificate management, reverse proxy, load balancing, SSO, and Federation.

Oracle Cloud Native SCCA LZ Technical Architecture

Figure 12. Oracle Cloud Native SCCA LZ Technical Architecture



- **VDSS:** The VCN is the single access point in and out for your traffic within your environment and your traffic is isolated and network controlled for routing.
- **DRG:** Your virtual router to which you can attach VCNs and IPSec tunnels.
- **Firewall:** Provides intrusion detection and prevention service and filters out incoming traffic based on rules.
- **VDMS:** Corresponds to all the core services required for managing the operations of the environment such as vault, VSS, and object storage.
- **Virtual Private Vault (VPV):** Encryption management service that stores and manages encryption keys and secrets to securely access resources. The VPV will be replicated to DR region for redundancy and key management in case of a disaster.
- **Service Connector Hub:** Your service to transfer data between services.
- **VSS:** You must use this to continuously monitor all enclaves within your Cloud Provider environment.
- **Cloud Guard:** This service will use your organization's tenancy home region as the reporting region. Cloud Guard is used in conjunction with VSS detector recipes to support SCCA requirement [2.1.3.1].
- **Streaming:** This capability will ingest and consuming high-volume data streams in real-time
- **Workload Compartment:** Every workload has a dedicated compartment and VCN routing through the VDSS and the Network Firewall to communicate with on-premises systems.
- **Logging Analytics:** Oracle Logging Analytics is a cloud solution in OCI that lets you index, enrich, aggregate, explore, search, analyze, correlate, visualize, and monitor all log data from your applications and system infrastructure on-premises or in the cloud.
- **Object Storage:** This cloud storage service backups logging, audits, and flow logs and will be replicated to a disaster recovery region simultaneously to external logging tenancy for audit review.
- **Tenancy-wide services:** These services include Identity Domains, IAM, Policies, Auditing, and Cloud Guard.
- **Independent services:** These are tenancy-wide services that will be activated to be used with the LZ, Cloud Guard and VSS.
- **Logging:** This service is available within your tenancy for auditing and includes a compartment where all the audit logs will be dumped into a share location with retention rules so the logs may not be modified. The DoD requirement is for the bucket to be accessible to external users, auditors, etc. without modifying the permissions of the remaining environment.

Oracle Cloud Native Services used in SCCA LZ

Figure 13. Oracle Cloud SCCA LZ Native Services

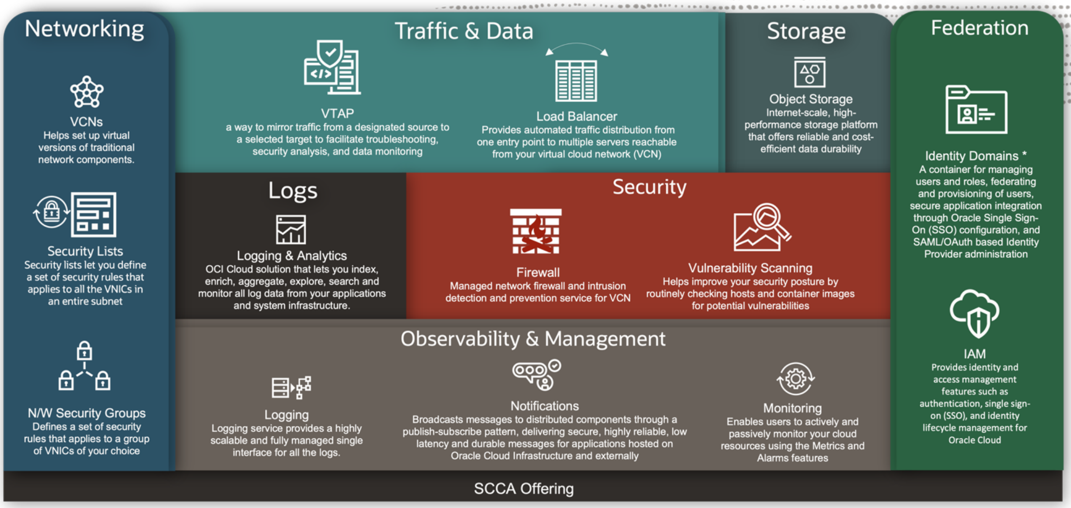

Networking
VCNs
Helps set up virtual versions of traditional network components.
Security Lists
Security lists let you define a set of security rules that applies to all the VNICs in an entire subnet
N/W Security Groups
Defines a set of security rules that applies to a group of VNICs of your choice
Traffic & Data
VTAP
a way to mirror traffic from a designated source to a selected target to facilitate troubleshooting, security analysis, and data monitoring
Load Balancer
Provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN)
Storage
Object Storage
Internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability
Federation
Identity Domains *
A container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and SAML/OAuth based Identity Provider administration
IAM
Provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud
Logs
Logging & Analytics
OCI Cloud solution that lets you index, enrich, aggregate, explore, search and monitor all log data from your applications and system infrastructure.
Security
Firewall
Managed network firewall and intrusion detection and prevention service for VCN
Vulnerability Scanning
Helps improve your security posture by routinely checking hosts and container images for potential vulnerabilities
Observability & Management
Logging
Logging service provides a highly scalable and fully managed single interface for all the logs.
Notifications
Broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency and durable messages for applications hosted on Oracle Cloud Infrastructure and externally
Monitoring
Enables users to actively and passively monitor your cloud resources using the Metrics and Alarms features
SCCA Offering

Figure 13 above represents the available native services for your SCCA LZ. Below is a list with hyperlinks to the Cloud Native Services available within your SCCA LZ Solution:

VCNs

Virtual Cloud Networks set up virtual versions of traditional network components.

Security List

Security lists let you define a set of security rules that applies to all the Virtual Network Interface Cards (VNICs) in an entire subnet.

Network/vTAP Security Groups

These define a set of security rules that applies to a group of VNICs of your choice.

API Gateway

These enable you to create governed HTTP/S interfaces for other services, including Oracle Functions, Container Engine for Kubernetes, and Container Registry.

Object Storage

This internet-scale, high-performance storage platform offers reliable and cost-efficient data durability.

Auto Scaling

Oracle Cloud automatically adjusts the number or the lifecycle state of compute instances in an instance pool.

Logging and Analytics

Oracle Cloud's solution that lets you index, enrich, aggregate, explore, search, and monitor all log data from your applications and system infrastructure.

vTAP

vTAP provides a way to mirror traffic from a designated source to a selected target to facilitate troubleshooting, security analysis, and data monitoring.

Identity Domains

A container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and SAML/OAuth based Identity Provider administration.

Network Firewall

Our Cloud Native managed network firewall and intrusion detection and prevention service for VCN.

Load Balancer

Our service that provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN).

Vulnerability Scanning

Our service helps improve your security posture by routinely checking hosts and container images for potential vulnerabilities.

Observability and Management

Logging	Our Logging service provides a highly scalable and fully managed single interface for all your logs.
Monitoring	Our Monitoring platform enables you to monitor your cloud resources using the Metrics and Alarms features actively and passively.
Notifications	Our Notifications broadcast messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency, and durable messages for applications hosted on Oracle Cloud and externally.

Oracle Services Limits Required

The minimum service limits that you need to run the Cloud Native SCCA Landing Zone in your tenancy are below:

Oracle Cloud Regions

Table 9. Oracle Cloud Native SCCA Service Limits

	Service Limit Name	Service Limit Value
1	oci_announcements_service_announcement_subscription:	25
2	oci_events_rule	50
3	oci_cloud_guard_target	30
4	oci_identity_compartment	1000
5	oci_identity_domain	10
6	oci_identity_dynamic_group	50
7	oci_identity_policy	100
8	oci_kms_vault	1
9	oci_kms_key	1000
10	oci_load_balancer_load_balancer	300
11	oci_load_balancer_load_balancer	300
12	oci_load_balancer_load_balancer	5
13	oci_load_balancer_load_balancer	100
14	oci_load_balancer_load_balancer	5
15	oci_load_balancer_load_balancer	50
16	oci_log_analytics_log_analytics_log_group	50
17	oci_logging_log	500

18	oci_logging_log_group	100
19	oci_core_drg_route_distribution	100
20	oci_core_drg_route_distribution_statement	300
21	oci_core_drg_route_table	100
22	oci_core_drg_route_table_route_rule	100
23	oci_network_firewall_network_firewall	3
24	oci_network_firewall_network_firewall	100
25	oci_network_firewall_network_firewall_policy	50
26	oci_network_firewall_network_firewall_policy	100
27	oci_network_load_balancer_backend_set	50
28	oci_network_load_balancer_listener	50
29	oci_network_load_balancer_network_load_balancer	4
30	oci_ons_notification_topic	100
31	oci_sch_service_connector	20
32	oci_bastion_bastion	5
33	oci_core_service_gateway	2
34	oci_streaming_stream	15
35	oci_monitoring_alarm	100
36	oci_core_default_route_table	10
37	oci_core_default_security_list	300
38	oci_core_drg	5
39	oci_core_drg_attachment	100
40	oci_core_route_table	300
41	oci_core_subnet	300
42	oci_core_vcn	50
43	oci_core_vtap	4
44	oci_vulnerability_scanning_host_scan_recipe	100
45	oci_vulnerability_scanning_host_scan_target	200
46	oci_waa_web_app_acceleration_policy	100
47	oci_waf_web_app_firewall_policy	100
48	oci_announcements_service_announcement_subscription:	25
49	oci_events_rule	50

50	oci_cloud_guard_target	30
51	oci_identity_compartment	1000

Landing Zone Script

This section below provides a sample Native SCCA Landing Zone script. The entire script will be available to download at Oracle Cloud's Architecture site, GitHub, and via Oracle Cloud Console.

Example Script - Manage Identity Domain.

```
# Reference:
# https://docs.oracle.com/en-us/iaas/Content/API/Concepts/signingrequests.htm#seven__Python
# https://vTAP.ateam-oracle.com/post/oracle-cloud-infrastructure-oci-rest-call-walkthrough-with-curl
https://github.com/oracle-quickstart/oci-scca-landingzone
import argparse
import oci
import json
import requests

class ManageIdentityDomain:
    def __init__(self, domain_id, group_names):
        self.config = oci.config.from_file()
        self.auth = oci.Signer(
            tenancy=self.config['tenancy'],
            user=self.config['user'],
            fingerprint=self.config['fingerprint'],
            private_key_file_location=self.config['key_file'],
            pass_phrase=self.config['pass_phrase']
        )
        self.identity_client = oci.identity.IdentityClient(self.config)

        self.host = self.get_domain_url(domain_id)
        self.group_endpoint = self.host + "/admin/v1/Groups"
        self.group_names = group_names

    def get_domain_url(self, domain_id):
        print("Waiting for domain to enter ACTIVE state")
        get_domain_response = self.identity_client.get_domain(domain_id=domain_id)
        wait_until_domain_available_response = oci.wait_until(self.identity_client, get_domain_response, 'lifecycle_state', 'ACTIVE')
        print(f"Got domain url {wait_until_domain_available_response.data.url}")

        return wait_until_domain_available_response.data.url

    def create_group(self, group_name):
        body = {
            "displayName": group_name,
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:Group",
                "urn:ietf:params:scim:schemas:oracle:idcs:extension:group:Group"
            ]
        }

        response = requests.post(self.group_endpoint, json=body, auth=self.auth)
        response.raise_for_status()

        print(f"Display Name: {group_name} \tOCID: {json.loads(response.content)['ocid']}")

    def create_groups(self):
        for group in self.group_names:
            print(f"Provisioning group {group}")
            try:
                self.create_group(group)
            except requests.HTTPError as e:
                print(f"Error creating group {group}")
                print(e)

    def delete_group(self, group_name):
        # @TODO finish delete method and add destroy provisioner
        return
        # filter=displayName eq "john"
        response = requests.delete(
            self.group_endpoint + f"/", auth=self.auth)
        response.raise_for_status()
```

```
        print(f"Display Name: {group_name} deleted")

    def delete_groups(self):
        for group in self.group_names:
            print(f"Deleting group {group}")
            try:
                self.delete_group(group)
            except requests.HTTPError as e:
                print(f"Error deleting group {group}")
                print(e)

if __name__ == "__main__":

    parser = argparse.ArgumentParser(description="Manage an Identity Domain")
    parser.add_argument(vTAP-d', vTAP--domain_id',
                        help="<Required> Id of the domain to manage",
                        required=True)
    parser.add_argument(vTAP-g', vTAP--group_names',
                        nargs=vTAP+vTAP,
                        help=vTAP<Required> Names of the groups to create (space seperated)vTAP,
                        required=True)

    args = parser.parse_args()
    manage_id = ManageIdentityDomain(args.domain_id, args.group_names)
    manage_id.create_groups()
```

CAC and PIV Sign-in to Oracle Cloud's Console

This section describes how you may use a Common Access Card (CAC) or Personal Identity Verification (PIV) Card to sign into the Oracle Cloud Console.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63C provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. Oracle Cloud's OC3 realm supports NIST SP 800-63C Federated Authentication Level (FAL) 3. FAL3 requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the Identity Provider (IdP) and encrypted to the relying parties using approved cryptography.

Oracle Cloud's DoD customers are expected to provide their own X.509-capable IdP that also support the Security Assertion Markup Language (SAML) Holder-of-Key profile. This functionality is provided by Oracle's Identity Domain Cloud Service.

DoD Information Impact Level 5 Isolation Guidance

Customer Isolation

Oracle Cloud is built around our security-first principles. Our architecture helps reduce risk from advanced threats and isolates tenant data to ensure data privacy and security. You, as a DoD mission owner, may benefit from isolated network virtualization that reduces the risk of hypervisor-based attacks. Your tenancy isolation limits the risk of threat proliferation with hardware-based root of trust that ensures each server is provisioned with clean firmware and network segmentation that isolates services to ensure access is controlled, monitored, and driven by your strict policies.

Oracle Cloud's DoD realm supports *only* US Federal Civilian and US Department of Defense and DoD community cloud customers (as defined in SRG) operating up to FedRAMP High or up to DoD Impact Levels 2, 4 or 5. Oracle Cloud's US DoD realm does not host non-Federal US government tenants, such as state, local, or tribal governments, academic partners, or foreign governments. Per the CC SRG (Section 5.2.2.3), "*Information that must be processed and stored at Impact Level 5 can only be processed in a DoD private/community or federal government community cloud, on-premises or off-premises*" […] and:

- Virtual and logical separation between DoD and Federal Government tenants and missions is sufficient. Virtual and logical separation between tenant and mission systems is minimally required.
- Physical separation from non-DoD or non-Federal Government tenants (i.e., public, local, and state government tenants) is required.

Compute Isolation

If you are operating at DoD IL5 and prefer or require an additional level of compute isolation above the virtual or logical separation offered in our community cloud, you may choose to leverage Oracle Cloud Bare Metal or Dedicated Virtual Machine (VM) Host options. A bare metal compute instance provides dedicated physical server access for the highest performance and strong isolation, while Dedicated Virtual Machine Hosts provide the ability to run Compute VM instances on dedicated servers that are a single tenant and not shared with other customers.

Network Isolation

Oracle Cloud reduces your risk by decoupling network virtualization from the hypervisor. Oracle implemented network virtualization as a highly customized hardware and software layer that moves cloud control away from the hypervisor and host and puts it on its own network. This hardened and monitored layer of control is what enables your isolated network virtualization. Isolated network virtualization is implemented in every data center in every region, which means that all Oracle Cloud tenants benefit from this reduced risk.

Oracle Cloud's physical network architecture adds a layer of defense to the isolated network virtualization by further isolating your tenancies and limiting the risk of threat proliferation. The physical network components are the racks, routers, and switches that form the physical layer of OCI.

Access control lists (ACLs) are enforced for the top-of-rack (ToR) switches. ACLs enforce adherence to the communications pathways within the topology. For example, the ToR switch drops any packet in which the virtual network source IP address and its corresponding physical network port don't match the expected mapping. This mismatch would occur if an attacker spoofed the virtual source IP address, to pretend to be a legitimate traffic source to reach other tenants. The ACLs are designed to prevent IP spoofing by associating the expected IP addresses for an isolated network virtualization device with the physical ports that the device is connected to. Additionally, the destination device performs a reverse-path check on packets to prevent encapsulation header tampering.

Hardware-based Root of Trust

A primary design principle of Oracle Cloud is protecting tenants from firmware-based attacks. Threats from the firmware level are becoming more common, which raises the potential risks for public cloud providers. So that each server is provisioned with clean firmware, Oracle implemented a hardware-based root of trust for the process of wiping and reinstalling the server firmware. Oracle Cloud uses this process every time a new server is provisioned for a tenant or between tenancies, regardless of the instance type.

The hardware-based root of trust is a protected hardware component that's manufactured to our specification and inspected visually. It's limited to performing the specific task of wiping and reinstalling firmware. It triggers a power cycle of the hardware host, prompts for the installation of known firmware, and confirms that the process has performed as expected. This method of firmware installation reduces the risk from firmware-based attacks, such as a permanent denial of service attack or attempts to embed backdoors in the firmware to steal data or make it otherwise unavailable.

Cryptographic Isolation of Storage

Vaults are logical entities where the Vault service creates and durably stores keys and secrets. The type of vault you have determines features and functionality such as degrees of storage isolation, access to management and encryption, scalability, and the ability to back up. The type of vault you have also affects pricing. You cannot change a vault's type after you create the vault.

The Vault service offers different vault types to accommodate your organization's needs and budget. All vault types ensure the security and integrity of the encryption keys and secrets that vaults store. A virtual private vault is an isolated partition on a hardware security module (HSM). Vaults otherwise share partitions on the HSM with other vaults.

Keys are logical entities that represent one or more key versions, each of which contains cryptographic material. A key's cryptographic material is generated for a specific algorithm that lets you use the key for encryption or in digital signing. When used for encryption, a key or key pair encrypts and decrypts data, protecting the data where the data is stored or while the data is in transit. With an AES symmetric key, the same key encrypts and decrypts data. With an RSA asymmetric key, the public key encrypts data and the private key decrypts data.

Conceptually, the Vault service recognizes three types of encryption keys: master encryption keys, wrapping keys, and data encryption keys.

When you create a master encryption key, the Vault service can either generate the key material internally or you can import the key material to the service from an external source. When you create master encryption keys, you create them in a vault, but where a key is stored and processed depends on its protection mode.

Master encryption keys can have one of two protection modes: HSM or software. A master encryption key protected by an HSM is stored on an HSM and cannot be exported from the HSM. All cryptographic operations involving the key also happen on the HSM. Meanwhile, a master encryption key protected by software is stored on a server and, therefore, can be exported from the server to perform cryptographic operations on the client instead of on the server. While at rest, the software-protected key is encrypted by a root key on the HSM. For a software-protected key, any processing related to the key happens on the server.

To meet the guidance outlined in the CC SRG, Section 5.11, Oracle recommends customers operating at DoD IL4 and IL5 to use the Virtual Private Vault option in Oracle Cloud.

Database-as-a-Service Isolation

Oracle Cloud provides multiple options for database-as-a-service. If you are operating at DoD IL5 and prefer or require an additional level of database compute isolation above the virtual or logical separation offered in Oracle's community cloud, you may choose to leverage Oracle Cloud single-node database systems on bare metal or Exadata Cloud Service.

DoD Security Technology Implementation Guide (STIG) Guidance

Oracle Linux STIG Image

Oracle Linux STIG Image is an implementation of the Security Technical Implementation Guide (STIG). With this image, you can create an Oracle Linux 8 instance in Oracle Cloud that you can configure to follow certain security standards and requirements that were set by the Defense Information Systems Agency (DISA).

Oracle Linux STIG Image is available at the following locations:

- Oracle Cloud where the image may be accessed by using either the embedded Marketplace or the Oracle Images tab.
- Oracle Cloud Marketplace which is outside of OCI.

STIG Tool for Virtual Machine Database Systems

Oracle Cloud provides a Python script, referred to as the STIG tool, for Oracle Cloud's virtual machine database systems provisioned using Oracle Linux 8. The STIG tool is used to ensure security compliance with DISA's Oracle Linux 8 STIG.

The STIG tool is provided for all newly provisioned virtual machine database systems in the following OS directory location on virtual machine database system nodes:

/opt/oracle/dcs/bin/dbcsstig

The architecture has the following components:

1. **Compartment**
   The SCCA Landing zone creates a compartment structure that organizes the resources in a way that aligns with the SCCA requirements. The following compartments are created as part of the SCCA Landing Zone: SCCA Parent, VDSS, VDMS, Backup, Logging, and Workload.
2. **Identity**
   The SCCA Landing Zone assumes that the Identity Domain feature is available in the realm where it will be deployed. The X.509 feature flag will be enabled in this deployment of Landing Zones. You, as the DoD mission owner, will need to provide your own X.509 Identity Provider (IdP) which should also support the SAML Holder-of-Key profile. Once this is configured, federated users will be able to sign-in into the Oracle Cloud Console with their Common Access Card (CAC) or Personal Identity Verification (PIV) Card. In order to support SCCA access requirements with the above compartment configuration, the following IAM Groups will be deployed: VDSSAAdmin Group, VDMS Admin Group, and Workload Admin Group.
3. **Networking**
   To protect all the traffic flows (North-South and East-West), Oracle Cloud recommends segmenting the network using a hub and spoke topology, where traffic is routed through a central hub called **Virtual Datacenter Security Stack (VDSS) VCN** and is connected to multiple distinct networks (spokes) called **Virtual Datacenter Managed Services (VDMS) VCN** and **Workload VCNs.**

   All traffic between VDMS and Workload, whether to and from the internet, to and from on-premises, or to the Oracle Services Network or between them, is routed through the VDSS and inspected with the network firewall's multi-layered threat prevention technologies. The role of the Network Firewall is critical and being a PaaS service, performance is managed by Oracle Cloud. The VDSS VCN contains a network firewall based on Palo Alto Technologies, an Oracle internet gateway, a DRG, and an Oracle Service Gateway. The VDSS VCN connects to the spoke (VDMS and Workload) VCNs through a DRG. Each VCN has an attachment to the DRG, which allows them to communicate with each other. For further details about DRG and VCN Attachment please refer to this article: Dynamic Routing Gateways. All spoke (from VDMS and Workload) traffic uses route table rules to route traffic through the DRG to the VDSS for inspection by the network firewall.

The architecture also presents the option to use the new packet capture service in Oracle Cloud called Virtual Testing Access Point (vTAP). Another key component of the architecture is the integration between the Load balancer (deployed in VDMS and Workload) and the Web Application Firewall (WAF).

4. **Security**
   The following Oracle Cloud services will be implemented by the SCCA Landing Zone to help your organization meet the SCCA VDMS Security requirements.
   - Vault (Key Management)
   - Log Archiving Storage Bucket
   - Streams & Events
   - Default Log Group
   - Service Connector
   - Vulnerability Scanning Service (VSS)
   - Cloud Guard
   - Bastion
5. **Monitoring**
   Our Oracle Cloud Landing Zone provides several services that work together to provide monitoring capabilities across your tenancy. It creates a monitoring structure in the VDSS, VDMS, and workload components that sets fulfills your initial monitoring requirement. This provides a starting point that administrators may adjust according to their own operational model. To avoid excessive cost and a lot of messages, the landing zone deployment will have these alerts disabled by default. Based upon your operational model, you can enable the relevant alerts from the Oracle Cloud console.

Considerations

Consider the following points when deploying this SCCA LZ architecture:

1. **Performance**
   Within a region, performance isn't affected by the number of VCNs. When you peer VCNs in different regions, consider latency. When deciding which components or applications will be deployed within the VDMS and mission owner Workload Compartments (Spoke VCNs) you will need to carefully consider the throughput that will need to be implemented at the connectivity level with the on-premises environment on your virtual private network (VPN) or FastConnect.
2. **Security**
   Use appropriate security mechanisms to protect the topology. The topology that you deploy by using the provided Terraform code incorporates the following security characteristics:
   - The default security list of the VDSS VCN allows SSH traffic from 0.0.0.0/0. Adjust the security list to allow only the hosts and networks that should have SSH access or any other additional services ports to your infrastructure.
   - Spoke VCNs (VDMS and mission owner Workload) are not accessible from the internet.
3. **Management**
   Route management is simplified as most routes will be at the DRG. Using the DRG as the VDSS, it is possible to have up to 300 attachments.
4. **Operational Costs**
   Cloud Consumption should be monitored closely to ensure that operational costs are within your designated budget. Basic compartment-level tagging should be configured for the VDSS and VDMS compartments. Certain cloud resources such as Virtual Private Vault (dedicated HSM) and Network Firewall are SCCA requirements. These services have a higher operating cost and alternative services can be considered in non-production environments, e.g., a Shared Software Vault could be used instead in a non-production environment.

Deploy

The Terraform code for this reference architecture is available as a sample stack in Oracle Cloud's Resource Manager. You can also download the code from GitHub and customize it to suit your specific requirements.

Deploy using the sample stack in Oracle Cloud's Resource Manager:

Login to Oracle Cloud Resource Manager

If you aren't already signed in, enter the tenancy and user credentials.

Select the region where you want to deploy the stack.

Follow the on-screen prompts and instructions to create the stack.

After creating the stack, click Terraform Actions and select Plan.

Wait for the job to be completed and review the plan.

To make any changes, return to the Stack Details page, click Edit Stack, and make the required changes. Then, run the Plan action again.

If no further changes are necessary, return to the Stack Details page, click Terraform Actions and select Apply.

Deploy using the Terraform code in GitHub:

Go to GitHub.

Clone or download the repository to your local computer.

Follow the instructions in the README document.

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 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

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle