Technical White Paper: **2023**

VMware Government Services IL5 Tenant Configuration Guide & Reference Architecture

vmware®

Table of contents

Abstract

This document aims to guide Department of Defense (DoD) Mission Owners in designing a secure implementation of VMware's cloud service offerings made available in VMware Cloud on AWS GovCloud (US). It offers security best practices and architectural recommendations to ensure proper design and deployment of DoD compliant infrastructure, safeguarding mission applications and data within the VMware Government Services (VGS) authorization boundary.

VMware provides secure infrastructure, platform and software cloud service offerings for Mission Owners to deploy their applications, but the responsibility for the secure deployment, configuration, management and monitoring of their workloads lies with the Mission Owners themselves.

Introduction

VMware Government Services (VGS) is a specialized enclave in VMware's ecosystem designed to meet the stringent security and compliance requirements of the U.S. government, particularly those handling sensitive and controlled data. This enclave is physically and logically separate from VMware's commercial cloud service offerings (CSOs) and is designed to adhere to the various regulatory standards, including those mandated by the U.S. Department of Defense (DoD).

VGS complies with various regulatory frameworks such as FedRAMP High and DoD Impact Levels 2, 4 and 5, enabling U.S. government customers the ability to run highly regulated workloads. VGS operates under a shared responsibility model, providing customers the maximum amount of agility to support their mission.

In support of this shared responsibility model, VMware has developed a series of Tenant Configuration Guides (TCGs) designed to help DoD Mission Owners secure their tenant environment utilizing defined security best practices. These comprehensive guides have been specifically crafted to assist Mission Owners in configuring and deploying workloads within the secure and isolated VGS enclave, ensuring the highest level of confidentiality, integrity and availability for DoD workloads.

VMware shared responsibility model

VMware implements a shared responsibility model that defines distinct roles and responsibilities of the parties involved in the VGS CSOs.

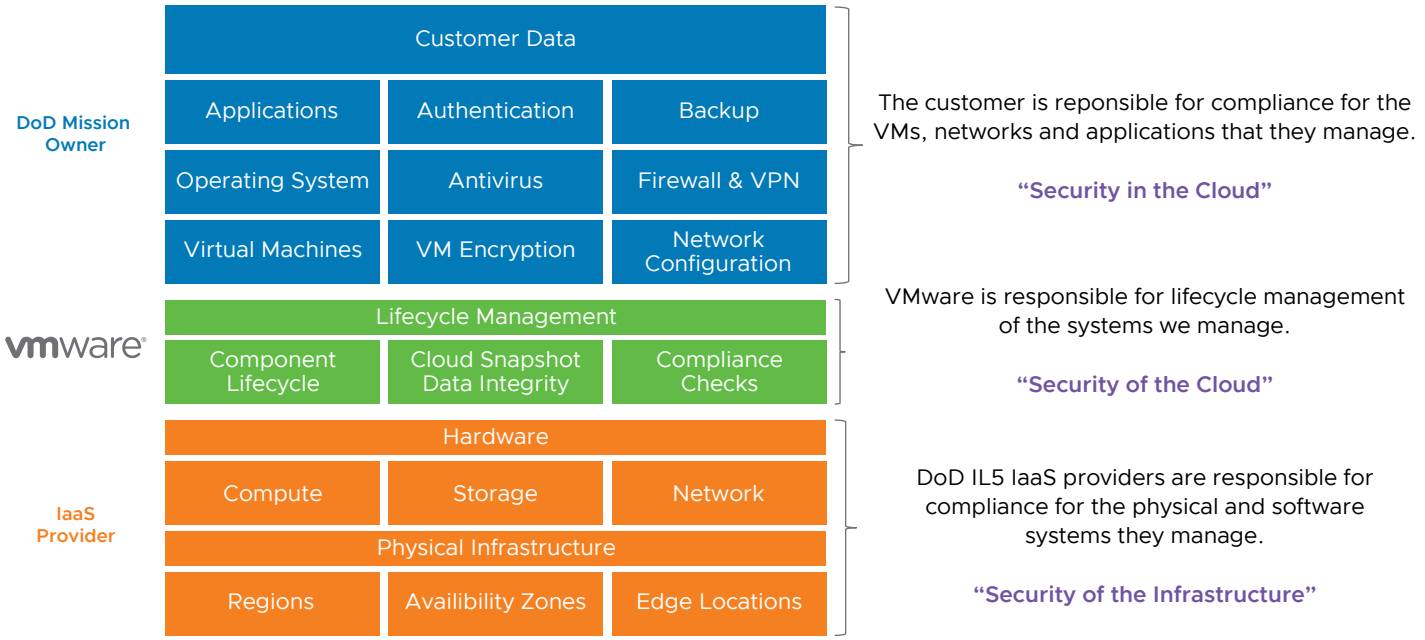

Figure 1: VMware shared responsibility model.

Mission Owner responsibility "Security in the Cloud" — Mission Owners are responsible for the deployment and ongoing configuration of their VMware service offerings. Mission Owners are also responsible for overseeing and managing certain controls pertaining to their security authorization boundary. Specific examples of these controls include configuration and patch management of virtual machines (VMs), management of VMware NSX firewall rulesets, role and credential management.

VMware responsibility "Security of the Cloud" — VMware is responsible for protecting the software and systems that make up the VMware service offerings. This software is composed of the compute, storage and networking needed to provided control plane services for the VMware CSOs made available in the VGS authorization boundary.

IaaS responsibility "Security of the Infrastructure" — The IaaS providers are responsible for the physical facilities, physical security, infrastructure and hardware underlying the entire service.

DoD cloud connectivity

A foundational element of enabling DoD Mission Owners to utilize cloud services is the establishment of a Cloud Access Point (CAP) connection between the Defense Information Systems Network (DISN) and the cloud environment. The CAP acts as a gateway that facilitates the secure transmission of data and communications between the DISN and cloud environments, ensuring compliance with DoD security and policy requirements.

The sections below describe the Defense Information Systems Agency (DISA) BCAP reference architecture and how VMware aligns with that architecture, leveraging the features of the VGS authorization boundary.

DISA BCAP reference architecture

The diagram below has been generated by DISA and serves as a reference architecture that can be leveraged by Cloud Service Providers (CSPs) as a blueprint for architecting cloud services that can be utilized by Mission Owners for DoD IL2, 4 and 5 workloads.

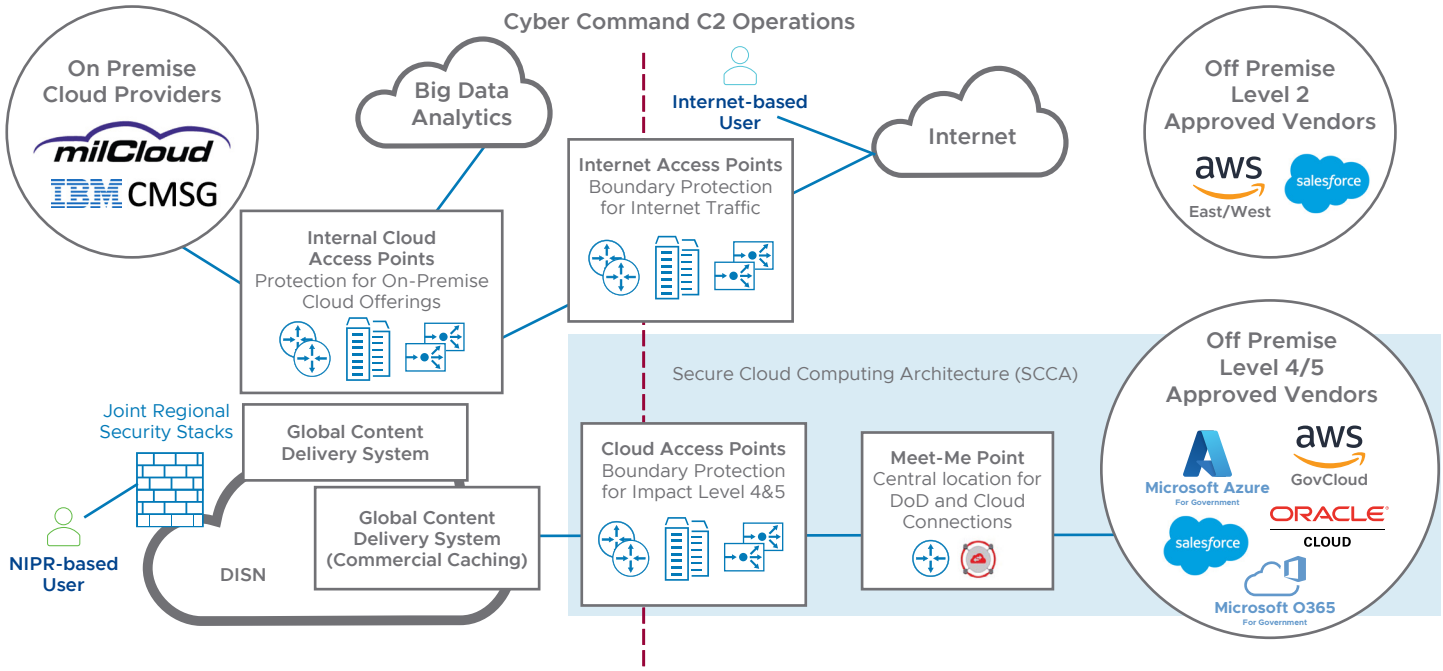

Figure 2: DISA BCAP reference architecture.

VGS BCAP reference architecture

The diagram below provides a visual depiction of the reference architecture utilized by VMware to establish a CAP connection between DoD Mission Owners and the service offerings provided as part of the VGS authorization boundary.

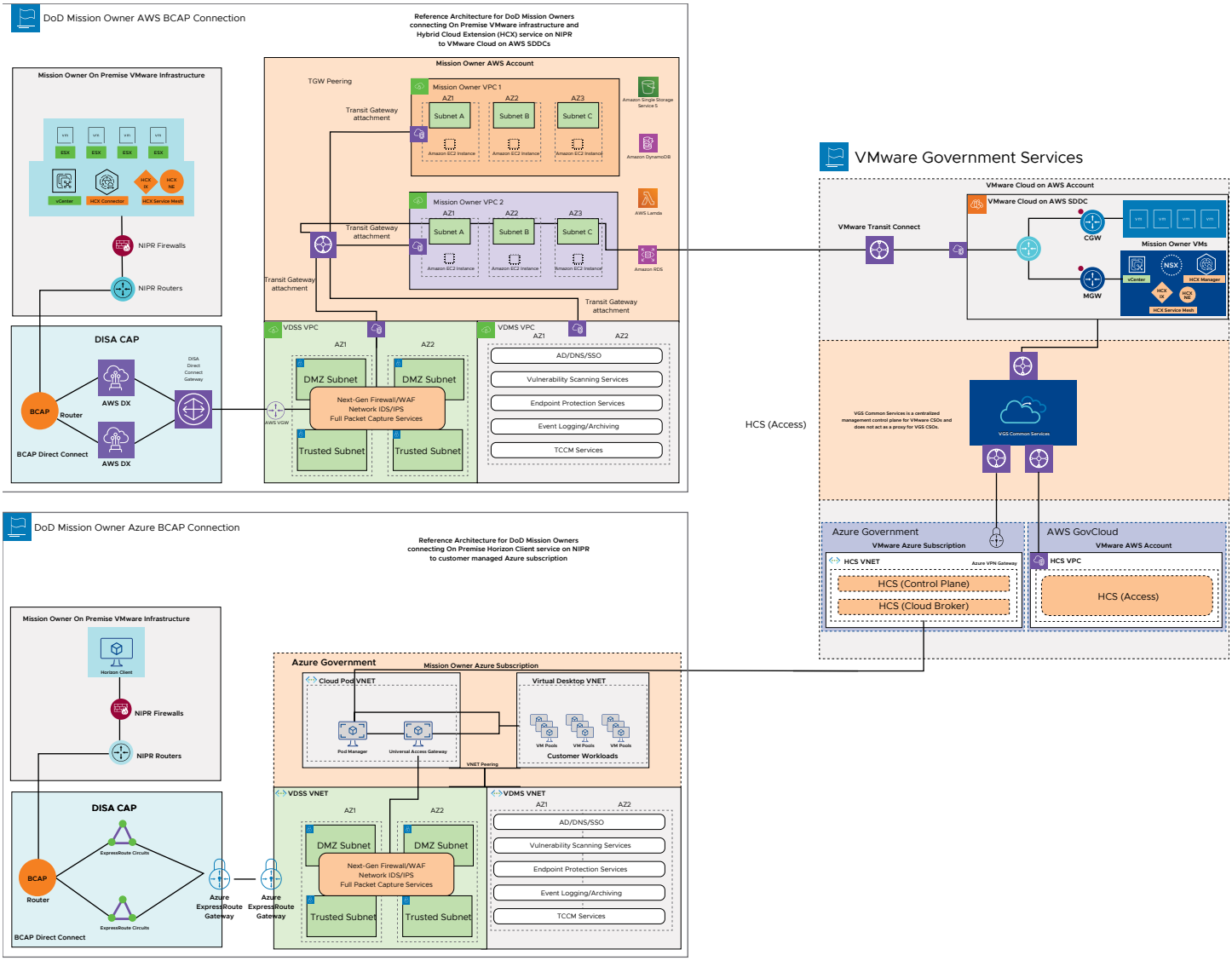

Figure 3: VGS BCAP reference architecture.

Tenant Configuration Guides

The following VMware Tenant Configuration Guides are designed to provide Mission Owners with fundamental security principles of VMware CSOs operating in the VGS authorization boundary and explore their specialized features to enable Mission Owners to run secure workloads utilizing security best practices.

VMware Cloud on AWS GovCloud (US)

The information documented below is intended for DoD Mission Owners who intend to use VMware Cloud on AWS GovCloud (US) to create a Software-Defined Data Center (SDDC) that has the networking and security infrastructure necessary to migrate workloads off premises and run them securely in the cloud. It was written for readers who have used vSphere in an on-premises environment are familiar with the fundamentals of IP networking using VMware NSX or another networking solution. In-depth knowledge of vSphere or Amazon Web Services (AWS) is not required.

VMware Cloud on AWS GovCloud (US) BCAP architecture

The diagram below provides a visual depiction of the reference architecture utilized by VMware Cloud on AWS GovCloud (US) to establish a CAP connection between DoD Mission Owners and their SDDCs. This includes VMware HCX, VMware Site Recovery Manager and customer workload traffic.

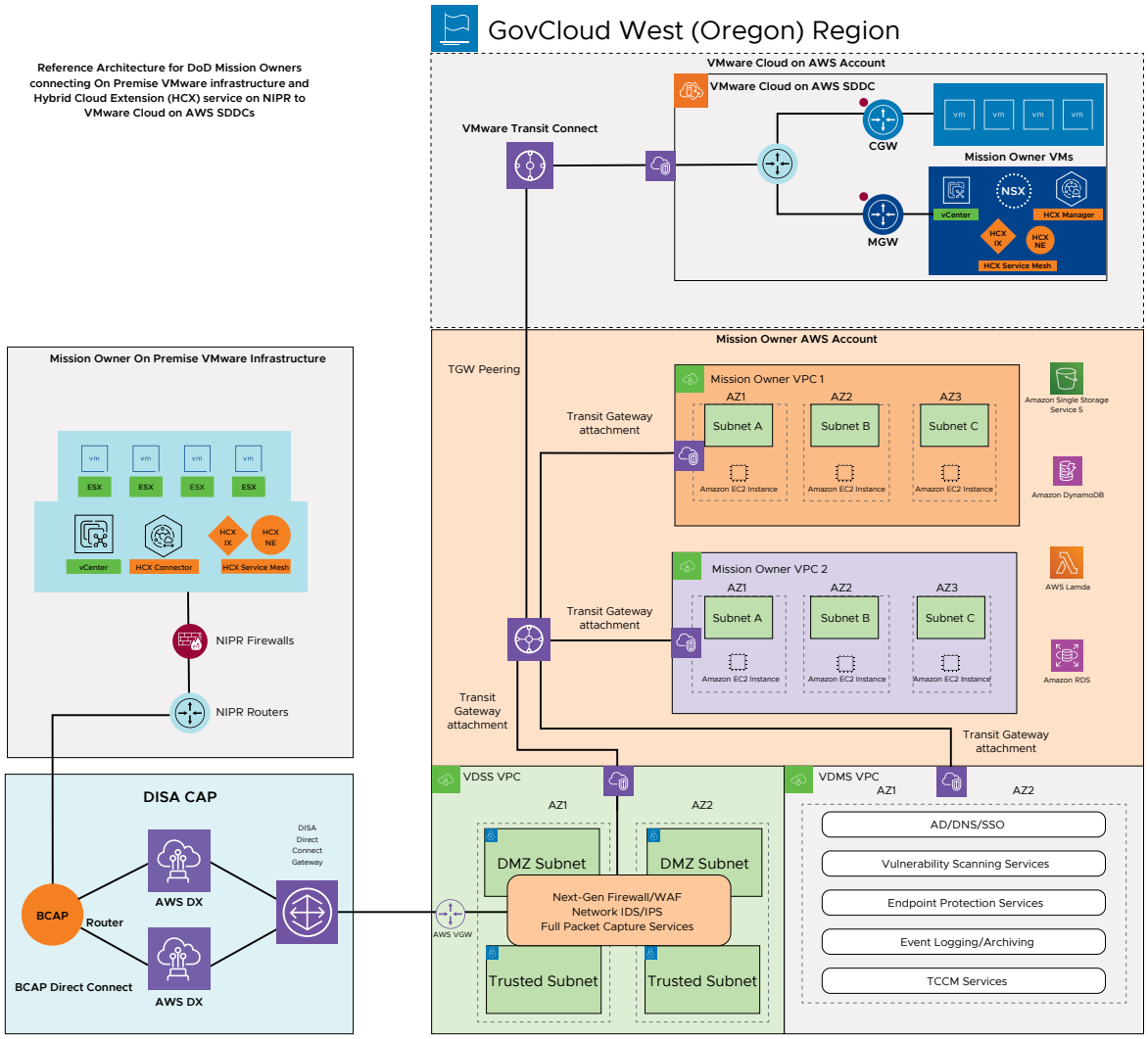

Figure 4: VMware Cloud on AWS GovCloud (US) BCAP reference architecture.

VMware Cloud on AWS GovCloud (US) secure network configuration

SDDCs utilize VMware NSX to create and manage SDDC networks. VMware NSX provides an agile software-defined infrastructure to build cloud-native application environments. Mission Owners have autonomy in defining the virtual networking within their SDDCs to support DoD IL2, 4 and 5 workloads.

Mission Owners shall ensure the following when establishing network configurations for their SDDC:

- All inbound/outbound Mission Owner SDDC communication shall flow through VMware Transit Connect.
- Transit Gateway Peering shall be configured between VMware Transit Connect and the Mission Owner's Transit Gateway or VPC attachment to Mission Owner's SCCA/VDSS.

VMware Cloud on AWS GovCloud (US) account management

VMware Cloud on AWS GovCloud (US) accounts are based on an organization which corresponds to each mission owner that subscribes to VMware Cloud Services. Organization roles specify the privileges that an organization member has over organization assets. Service roles specify the privileges that an organization member has when accessing VMware Cloud Services that the organization uses. All service roles can be assigned and changed by a user with organization owner privileges.

Mission Owners shall ensure the following when establishing service roles for their SDDC:

- Restrictive roles such as NSX Cloud Admin (Delete Restricted) or NSX Cloud Auditor shall be assigned along with the role of organization member to prevent modification.
- The NSX Cloud Admin role shall be limited to as few individuals as operationally possible to prevent unauthorized network configurations.
  - **NSX Cloud Auditor** — This role can view NSX service settings and events but cannot make any changes to the service.
  - **NSX Cloud Admin** — This role can perform all tasks related to deployment and administration of the NSX service.

The NSX Cloud Admin role can establish external connections to a Mission Owner SDDC. Mission Owners shall follow their internal access control, audit & accountability, configuration management, incident response and systems and communications protections policies and procedures to reduce the risk of unauthorized external connections.

Mission Owners shall restrict access to their Cloud Services Portal/VMware Cloud on AWS GovCloud (US) Console by setting up Allow/Block lists based on specific the IP ranges. This allows users to restrict access to CSP to only trusted IP address ranges. Additionally, DoD Mission Owners can implement a Remote Desktop or Bastion Host solution for remote access into the Cloud Services Portal (CSP). For more security, DoD Mission Owners shall enable whitelisting to limit CSP connections to only approved IP ranges.

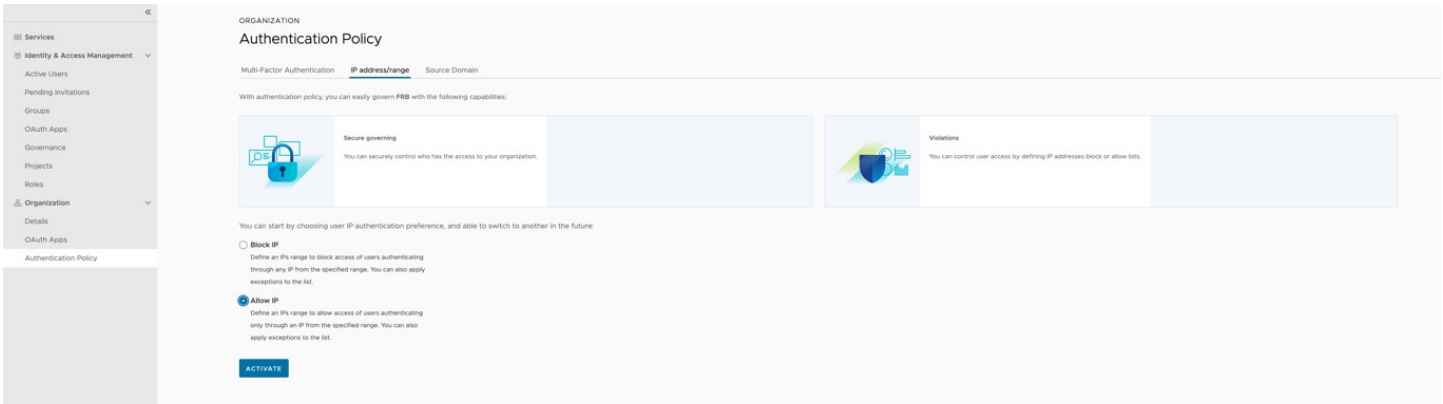

Figure 5: CSP Authentication Policy.

VMware Cloud on AWS GovCloud (US) audit & logging

Mission owner VMware Cloud on AWS GovCloud (US) Service Organizations and VMware Cloud on AWS GovCloud (US) SDDCs have access to Organization level activity logs for auditing as well as access to SDDC infrastructure level logs for monitoring and auditing SDDC infrastructure components. As VMware does not have access to Mission Owner workloads, Mission Owners shall ensure the following when establishing logging for their SDDC:

- Verify NSX Manager logs are sent to a centralized server and can be used as part of the organization's security incident tracking and analysis. VMware provides SDDC logs to Mission Owners via AWS S3 Buckets which can be ingested by DoD Mission Owners SIEM of choice.
- Verify that non-privileged users are prevented from executing privileged functions, including disabling, circumventing or altering implemented security safeguards/countermeasures.
- Verify NSX Manager audit records are off-loaded to a different system.
- Verify the capability for organization-identified individuals or roles to change the auditing to be performed based on all selectable event criteria within near-real time.
- Configure incident response monitoring and alerting to detect changes to SDDC networking.

VMware Horizon Cloud Service

A DoD Mission owner's Horizon Cloud environment consists of the VMware-hosted cloud service, DoD Mission Owner Microsoft Azure subscription and VMware software deployed into that capacity and connected to the cloud service. When the VMware software installed in that capacity is appropriately configured and connected to the cloud service, that configured entity is now a cloud-connected pod. Having at least one cloud-connected pod and completing the Active Directory registration process unlocks use of the cloud- and web-based Horizon Universal Console for management and administrative tasks involving those pods.

The Information documented below is intended for DoD Mission Owners who intend to use VMware's Horizon Cloud Service (HCS) to deliver virtual desktops and applications on Microsoft Azure.

VMware HCS BCAP Architecture

The diagram below provides a visual depiction of the reference architecture utilized by HCS to establish a CAP connection between DoD Mission Owners and their virtual workloads.

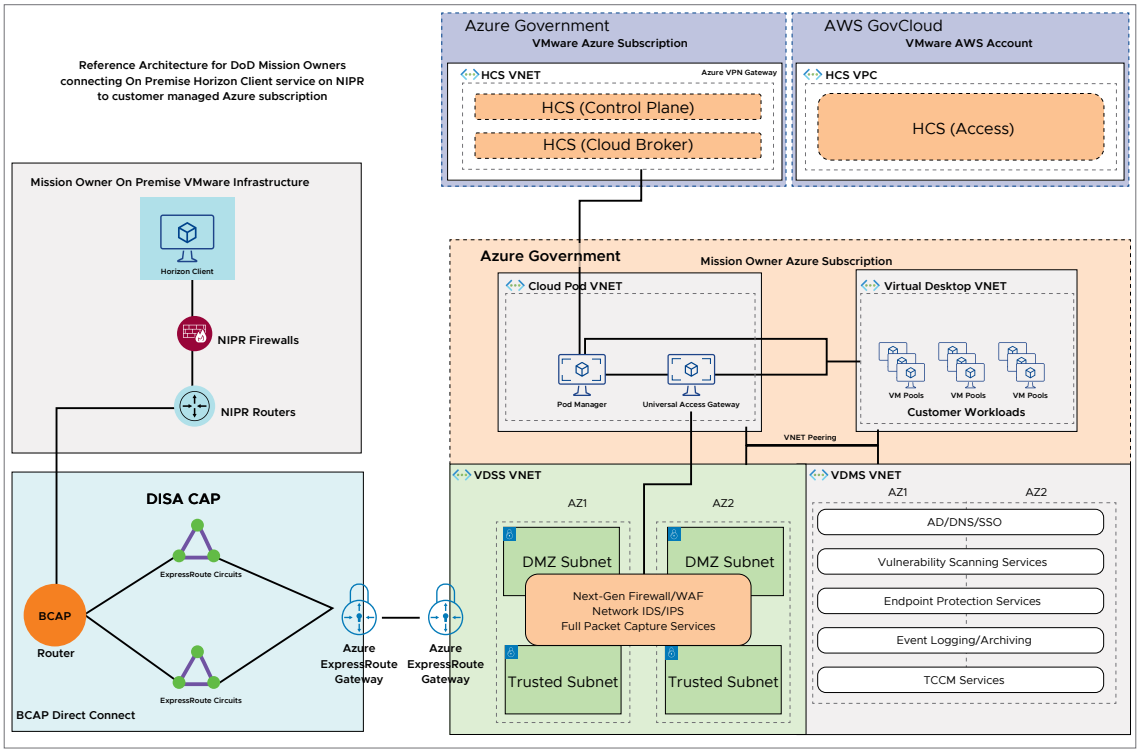

Figure 6: VMware Horizon Cloud Service BCAP Reference Architecture

VMware HCS secure network configuration

VMware Horizon Cloud Service (HCS) requires the customer to follow the Azure's Secure Azure Computing Architecture (SACA) to setup the BCAP connection to the customer's Azure subscription. DoD Mission Owners must follow Azure's guidance to ensure mission workloads are only accessible through the BCAP.

There is no HCS configuration required to establish this connectivity. All configurations are between the DoD BCAP and the Mission Owner's Azure Subscription.

VMware HCS account management

DoD Mission Owners shall securely configure and manage their identity and access to their Azure subscription and Azure resources. Owners shall federate Azure AD with their Identity Provider (IdP) and configure roles and permissions for user and system access to Azure resources in line with the Mission's identity and access management policy.

VMware HCS audit & logging

DoD Mission Owners shall configure Microsoft Azure to monitor applications, virtual machines, guest OSs, databases, security events, networking events and more. Alerting shall be configured by the Mission Owner within the Azure Monitor service to report any user activity that is not approved through mission procedures. These logs can also be exported from Azure Monitor into third-party solutions for alerting and correlation by the Mission Owner.

VMware HCS compute isolation

To ensure isolated computing, Mission Owner's shall deploy HCS virtualized desktops and applications onto Azure Dedicated Hosts. These hosts are available from Azure and provide physical servers that host one or more Azure virtual machines. These servers are dedicated to the mission and workloads—capacity isn't shared with other Azure customers.

Conclusion

VMware offers several essential advantages to DoD mission owners, encompassing adaptability, scalability and accelerated time-to-deployment. It furnishes an array of security solutions and functionalities that can be leveraged to oversee the safeguarding of your assets and data within the VMware environment. While VMware delivers a commendable service management framework for infrastructure and platform services, Mission Owners retain the obligation to ensure the secrecy, integrity and accessibility of their cloud-stored data, as well as fulfill distinct mission criteria for data security.

Contributors

The following VMware staff contributed to this document:

- Joe Witles, Director of Authorization Management, VMware Government Services
- Patrick O'Laughlin, Security Compliance Manager, VMware Government Services
- Jason Crocker, Staff VMware Cloud Solutions Architect, VMware Cloud
- Nic Hall, Staff Security Engineer, VMware Government Services
- Jeremy Soehnlin, Senior Information Security Engineer, VMware Government Services

Appendix

The above guidance is specific to DoD Mission Owner implementations. General configuration information is provided at the below links:

	Release date
Cloud Infrastructure Security Configuration & Hardening | VMware	06/13/2023
VMware Cloud on AWS GovCloud (US) Networking and Security	06/21/2022
VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist	04/27/2023
First-Gen Horizon Cloud on Microsoft Azure Deployments — Key Characteristics	06/17/2023
VMware Horizon Security	03/14/2023

Item No: VGS IL5 Tenant Configuration Guide 9/23