La arquitectura de computación en nube segura está lista AWS para el Departamento de Defensa de EE. UU.

AWS Orientación prescriptiva

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Orientación prescriptiva: La arquitectura de computación en nube segura está lista AWS para el Departamento de Defensa de EE. UU.

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Introducción 1
Destinatarios previstos 1
Descripción general del acelerador de zonas de aterrizaje 2
Planifique la implementación de la LZA en AWS 4
Componentes y requisitos del SCCA 5
Punto de acceso a la nube 7
Paquete de seguridad para centros de datos virtuales 8
Virtual Data Center Managed Services 17
Integración de servicios complementarios 24
Revisiones del sistema operativo 25
Administrador de credenciales en la nube de confianza 25
Conclusión y recursos 32
AWS recursos 32
Otros recursos de 32
Historial de documentos 33
..... xxxiv

La arquitectura de computación en nube segura está lista AWS para el Departamento de Defensa de EE. UU.

Rob Higareda y Rughved Gadgil, Amazon Web Services ()AWS

Marzo de 2024 (historial del documento)

El Departamento de Defensa (DoD) de EE. UU. segmenta la información de la nube en niveles de impacto (ILs). El nivel de impacto está asociado a la confidencialidad de la información y al riesgo de perder la confidencialidad, integridad o disponibilidad de esa información. IL4 aloja la información no clasificada controlada (CUI) del DoD y la información de la CUI del DoD y IL5 de los Sistemas de Seguridad Nacional (NSS). Esta guía está diseñada para ayudarte a construir una landing zone que sirva de apoyo IL4 e IL5 información.

Para crear una infraestructura IL4 de nube compatible o IL5 compatible, debe crear componentes específicos. La arquitectura segura de computación en nube (SCCA) de la Agencia de Sistemas de Información de Defensa (DISA) es una selección de servicios de administración y seguridad en la nube. Proporciona un enfoque estandarizado para crear un límite entre las nubes. La SCCA también incluye componentes de seguridad a nivel de aplicación para IL4 la IL5 información alojada en la nube.

Esta guía le ayuda a cumplir los requisitos de la SCCA al utilizar el acelerador de zonas de aterrizaje (LZA) activado. AWS La solución LZA implementa un conjunto básico de capacidades diseñadas para adaptarse a las AWS mejores prácticas y a varios marcos de cumplimiento globales. La LZA puede ayudarlo a crear muchos de los componentes necesarios para cumplir con la SCCA del DoD. Esta guía también recomienda cómo añadir componentes adicionales para cumplir con la SCCA y establecer una base segura para sus entornos de nube. AWS Si bien esta guía no incluye todas las situaciones posibles, proporciona orientación sobre cómo empezar y cuáles Servicios de AWS pueden ayudarle a cumplir los requisitos de la SCCA.

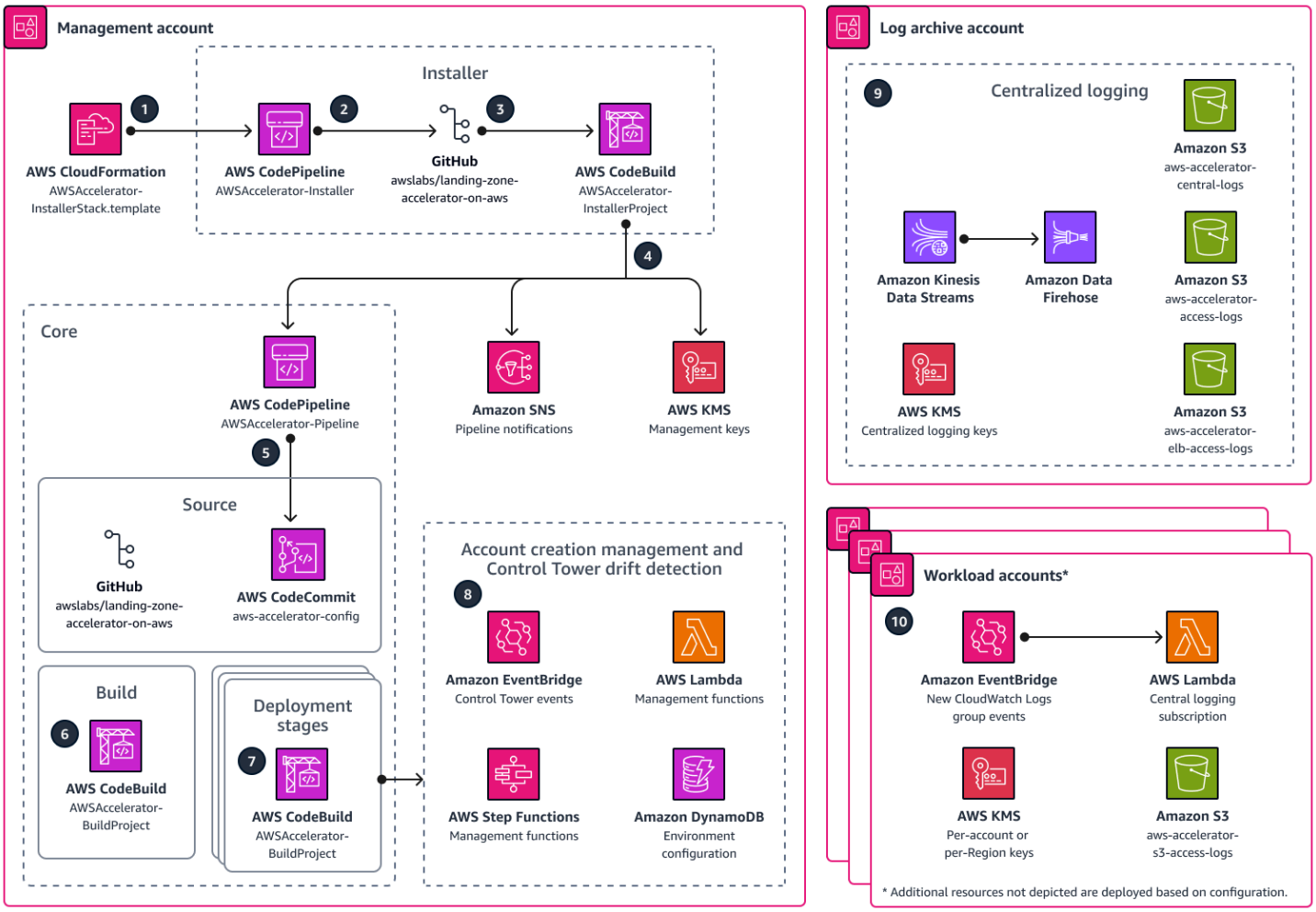
Destinatarios previstos

Esta guía está destinada a personas que necesitan cumplir con la arquitectura de computación en la nube segura del DoD para ayudar a proteger IL4 la IL5 información en el. Nube de AWS Si aún no lo ha hecho, consulte la Guía de requisitos de seguridad de la computación en nube de DISA antes de leer esta guía.

Descripción general del acelerador de zonas de aterrizaje

Para construir una landing zone AWS que se ajuste a la arquitectura segura de computación en nube (SCCA) de la Agencia de Sistemas de Información de Defensa (DISA), debes contar con ciertos elementos que te ayuden a cumplir con los requisitos mínimos. AWS ha creado el Landing Zone Accelerator (LZA) para ayudarte a desplegar una zona de aterrizaje que cumpla con los requisitos necesarios. Con la solución LZA, puede implementar el entorno mediante un conjunto de archivos de configuración. Estos archivos de configuración le ayudan a centrarse en la entrega de un entorno en lugar de aprender a cada individuo Servicio de AWS y cómo implementarlo.

La siguiente imagen muestra los servicios involucrados en la implementación de la LZA. Los números indican el flujo de trabajo, desde la modificación de los archivos de configuración hasta la configuración de las cuentas Servicios de AWS de carga de trabajo.



Esta solución está diseñada para alinearse con las AWS mejores prácticas y ajustarse a varios marcos de cumplimiento globales. Cuando se utiliza en coordinación con servicios como AWS Control Tower, por ejemplo, esta solución proporciona una solución integral Servicios de AWS y con poco código que abarca más de 35 funciones. En concreto, esta solución le ayuda a gestionar y gestionar un entorno de múltiples cuentas diseñado para soportar cargas de trabajo altamente reguladas y requisitos de conformidad complejos. LZA le ayuda a establecer la idoneidad de la plataforma con capacidades operativas, de seguridad y de conformidad. Esta guía incluye notas específicas sobre el uso de esta solución para respaldar la alineación con las directrices federales y del Departamento de Defensa (DoD) de los Estados Unidos (EE. UU.).

AWS proporciona la solución LZA como un proyecto de código abierto que se creó utilizando el. Kit de desarrollo de la nube de AWS (AWS CDK) Puede instalarla directamente en su entorno, lo que le brinda acceso total a la solución de infraestructura como código (IaC).

Mediante un conjunto simplificado de archivos de configuración, puede:

- Configurar funciones, barandas y servicios de seguridad adicionales, como reglas AWS Configadministradas y. AWS Security Hub CSPM
- Administre su topología de red fundamental a través de servicios como Amazon Virtual Private Cloud (Amazon VPC) y. AWS Transit GatewayAWS Network Firewall
- Genere cuentas de carga de trabajo adicionales mediante Account Factory AWS Control Tower .

No se requieren cargos adicionales ni compromisos por adelantado para utilizar Landing Zone Accelerator en. AWS Solo pagas por lo Servicios de AWS que enciendas para configurar tu plataforma y operar tus barandillas. Esta solución también admite AWS particiones no estándar, incluidas las AWS GovCloud (US) regiones AWS Secret y AWS Top Secret.

> **Important**
>
> La solución LZA, por sí sola, no hace que cumpla con las normas. Proporciona la infraestructura básica desde la que puede integrar soluciones complementarias adicionales. La información incluida en la guía de implementación de la LZA no es exhaustiva. Debe revisar, evaluar y aprobar la solución de conformidad con las características, herramientas y configuraciones de seguridad específicas de su organización. Es responsabilidad exclusiva de usted y de su organización determinar qué requisitos reglamentarios son aplicables y asegurarse de que cumplen con todos los requisitos. Si bien esta solución analiza los

requisitos técnicos y administrativos, no le ayuda a cumplir con los requisitos administrativos no técnicos.

Planifique la implementación de la LZA en AWS

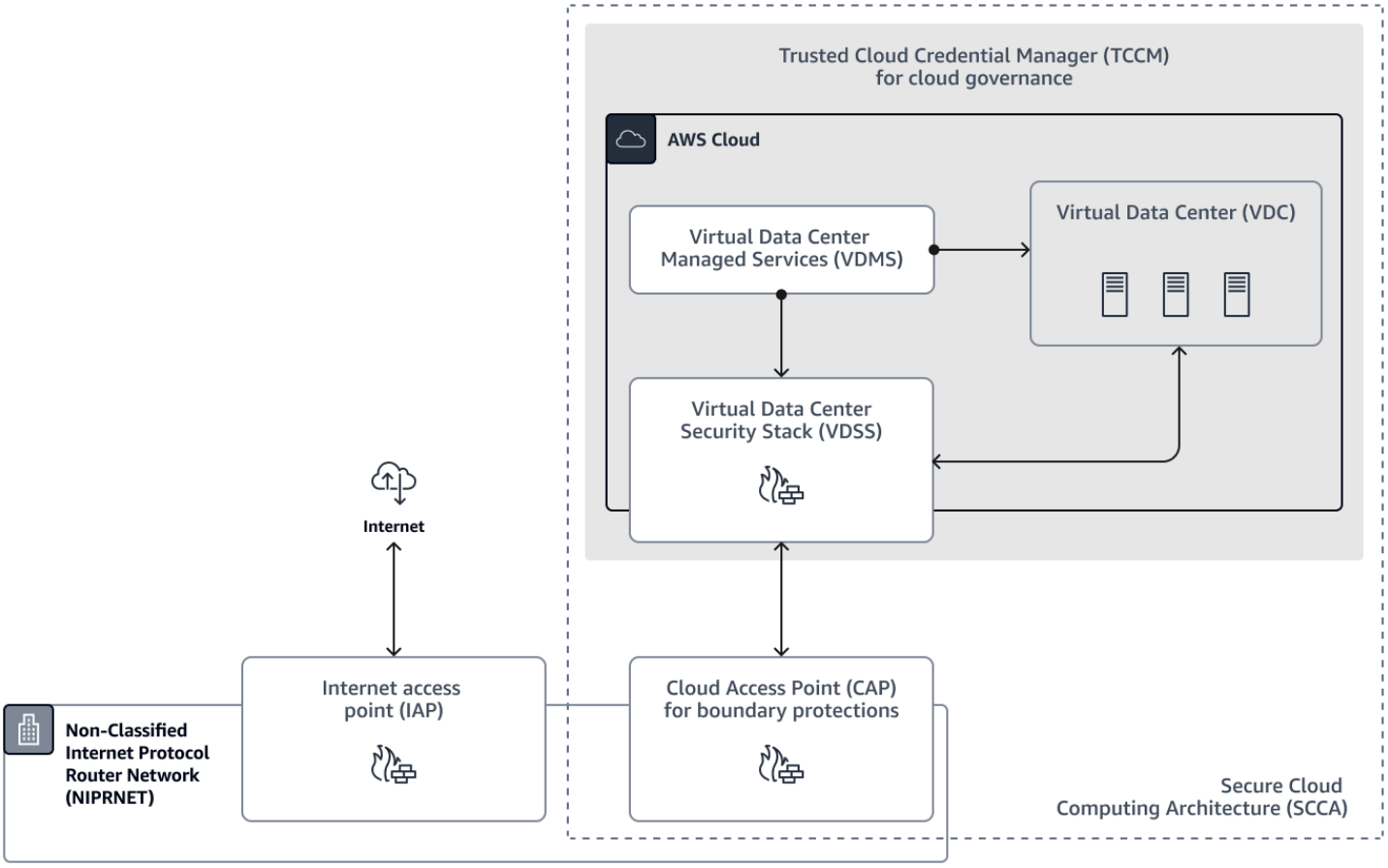
AWS ha creado una guía de implementación detallada para implementar la solución Landing Zone Accelerator (LZA) en. AWS Para ver un diagrama de arquitectura y una descripción general de los pasos de implementación, consulte el diagrama de arquitectura en la guía de implementación de Landing Zone Accelerator. AWS Su entorno debe cumplir los requisitos previos antes de implementar la solución. Con los requisitos del capítulo sobre los componentes y requisitos de la SCCA de esta guía, puede elegir entre las opciones de implementación que se describen en la guía de implementación de la LZA.

Componentes y requisitos del SCCA

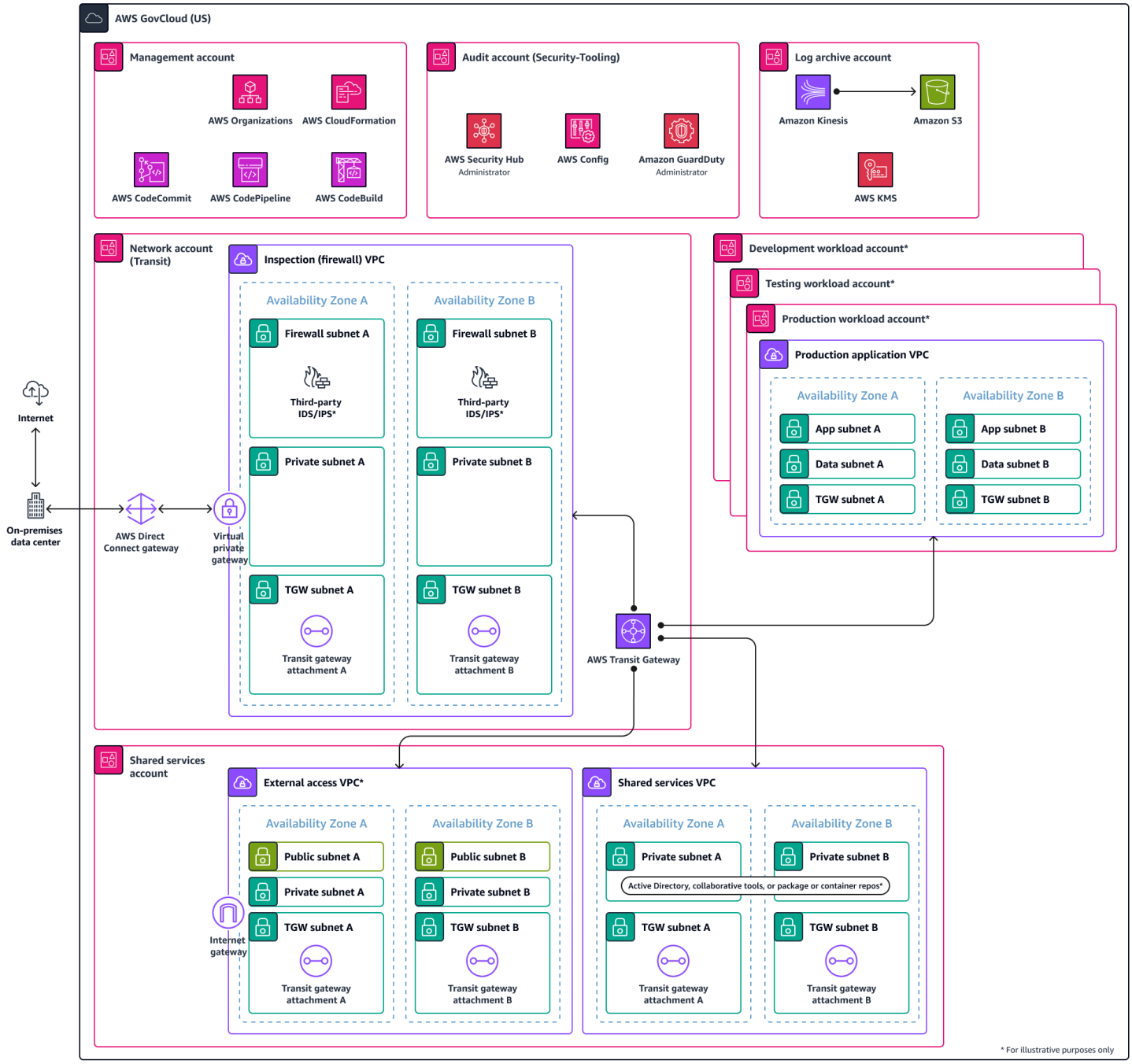
La arquitectura segura de computación en nube (SCCA) de la Agencia de Sistemas de Información de Defensa (DISA), adoptada por el Departamento de Defensa de los Estados Unidos (DoD), pretende ser un enfoque escalable y rentable para proteger las aplicaciones basadas en la nube bajo una arquitectura de seguridad común. Proporciona un enfoque estándar para proteger los datos de IL4 e IL5 en entornos de nube. Los componentes principales de la SCCA incluyen:

- Punto de acceso a la nube (CAP): proporciona acceso a la nube y protege las redes del DoD desde la nube. Protecciones simplificadas centradas en proteger los límites de la red.
- Paquete de seguridad para centros de datos virtuales (VDSS): seguridad de enclave de red virtual para proteger las aplicaciones y los datos en las ofertas de nube comercial.
- Virtual Data Center Managed Services (VDMS): seguridad de host de aplicaciones para el acceso de usuarios privilegiados en entornos comerciales.
- Trusted Cloud Credential Manager (TCCM): administrador de credenciales en la nube para aplicar el control de acceso basado en roles (RBAC) y el acceso con menos privilegios.

La siguiente imagen muestra estos componentes de la SCCA.



En esta sección se analiza cada componente en detalle y los componentes correspondientes de la LZA que pueden ayudarle a cumplir con el estándar de la Agencia de Sistemas de Información de Defensa (DISA). La siguiente imagen muestra la estructura de cuentas múltiples de la LZA que construye los componentes de la SCCA dentro de la. Nube de AWS Esta estructura de cuentas múltiples de la LZA es la base que le ayuda a lograr una arquitectura que cumpla totalmente con los requisitos de la SCCA de la DISA. Para ver un ejemplo de una arquitectura que le ayude a cumplir plenamente los requisitos de conformidad, consulte el diagrama SCCA sobre arquitectura. AWS GovCloud



Punto de acceso a la nube

Su organización predetermina el punto de acceso a la nube (BCAP) o el punto de acceso a la nube (CAP). Por lo tanto, no está incluido en el ámbito de esta guía. El CAP proporciona acceso a entornos de nube comerciales desde la Red de Sistemas de Información de Defensa (DISN). El CAP también protege los límites de la DISN desde la nube. En el límite de la DISN, incluye capacidades de ciberdefensa, como el firewall, los sistemas de detección de intrusos (IDS) y los sistemas de

prevención de intrusiones (IPS). Es habitual que las organizaciones utilicen el diseño de referencia del punto de acceso nativo de la nube del DoD para acceder. AWS

Paquete de seguridad para centros de datos virtuales

El objetivo del paquete de seguridad para centros de datos virtuales (VDSS) es proteger las aplicaciones alojadas en las misiones del Departamento de Defensa. AWS El VDSS proporciona un enclave para los servicios de seguridad. El VDSS realiza la mayor parte de las operaciones de seguridad en la SCCA. Este componente contiene servicios de seguridad y red, como la conectividad entrante, los controles de acceso y los servicios de protección perimetral, incluidos los firewalls de aplicaciones web, la protección contra DDOS, los equilibradores de carga y los recursos de enrutamiento de redes. El VDSS puede residir en la infraestructura de la nube o de forma local, en su centro de datos. AWS o los proveedores externos pueden proporcionar capacidades de VDSS a través de infraestructura como servicio (IaaS) o AWS pueden ofrecer estas capacidades a través de soluciones de software como servicio (SaaS). Para obtener más información sobre el VDSS, consulte la Guía de requisitos de seguridad de la computación en la nube del DoD.

La siguiente tabla contiene los requisitos mínimos del VDSS. En ella se explica si la LZA aborda cada requisito y cuál Servicios de AWS puede utilizar para cumplirlos.

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.1	El VDSS mantendrá una separación virtual de todo el tráfico de administración, usuarios y datos.	AWS Network Firewall Lista de control de acceso a la red (ACL) Grupos de seguridad para interfaces de red elásticas	Aísle las VPC	Cubierto
2.1.2.2	El VDSS permitirá el uso	Amazon VPC (cifrado del	Prácticas recomendadas	Cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
	del cifrado para la segmentac ión del tráfico de gestión.	tráfico entre instancias)	de cifrado para Amazon VPC	
2.1.2.3	El VDSS proporcionará una capacidad de proxy inverso para gestionar las solicitudes de acceso de los sistemas cliente.	N/A	Servir contenido mediante un proxy inverso totalmente gestionado	No está cubierto
2.1.2.4	El VDSS proporcionará la capacidad de inspeccio nar y filtrar las conversac iones de la capa de aplicación en función de un conjunto predefinido de reglas (incluida la HTTP) para identificar y bloquear el contenido malicioso.	AWS WAF Network Firewall	Inspección del organismo de solicitud web Inspección de tráfico TLS con Network Firewall	Cubierto parcialmente

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.5	El VDSS proporcionará una capacidad que pueda distinguir y bloquear el tráfico no autorizado de la capa de aplicación.	AWS WAF	Cómo usar Amazon GuardDuty y AWS WAF bloquear automáticamente los anfitriones sospechosos	¿No está cubierto
2.1.2.6	El VDSS proporcionará una capacidad que supervise las actividad es de la red y el sistema para detectar y denunciar las actividades maliciosas del tráfico que entra y sale de la red privada virtual del propietario de la misión. networks/ enclaves	Logs de flujo de VPC Amazon GuardDuty AWS Nitro Enclaves	AWS Talle r sobre Nitro Enclaves	Cubierto parcialmente

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.7	El VDSS proporcionará una capacidad que supervise las actividades de la red y el sistema para detener o bloquear las actividades maliciosas detectadas.	Network Firewall AWS WAF	N/A	Cubierto parcialmente
2.1.2.8	El VDSS inspeccionará y filtrará el tráfico que circule entre la red privada virtual del propietario de la misión. networks/ enclaves	Network Firewall	Implemente un filtrado de tráfico centralizado	Cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.9	El VDSS deberá analizar e inspeccionar el tráfico de SSL/TLS comunicaciones mediante la autenticación simple y doble del tráfico destinado a los sistemas alojados en el CSE.	Network Firewall	Modelos de implementación para Network Firewall	Cubierto
2.1.2.10	El VDSS proporcionará una interfaz para llevar a cabo las actividades de administración de puertos, protocolos y servicios (PPSM) a fin de proporcionar control a los operadores del MCD.	Network Firewall	Modelos de implementación para Network Firewall	Cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.11	El VDSS proporcionará una capacidad de monitoreo que capture archivos de registro y datos de eventos para el análisis de ciberseguridad.	Amazon CloudWatch AWS CloudTrail	Registro para la respuesta a incidentes de seguridad	Cubierto
2.1.2.12	El VDSS proporcionará o alimentará la información de seguridad y los datos de los eventos a un sistema de archivo asignado para que los usuarios privilegiados que realicen actividades de la CND de Boundary y Mission recopilen, almacenen y accedan a ellos de forma común.	Amazon CloudWatch Logs	Seguridad en CloudWatch los registros	Cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.13	El VDSS proporcionará un sistema de gestión de claves de cifrado FIPS-140-2 compatible para almacenar las credenciales de las claves de cifrado privadas del servidor generadas y asignadas por el DoD para su acceso y uso por parte del Web Application Firewall (WAF) en la ejecución de la SSL/TLS interrupción e inspección de las sesiones de comunicación cifradas.	AWS Secrets Manager AWS Key Management Service(AWS KMS)	Mejora la seguridad de Amazon CloudFront Origin con AWS WAF Secrets Manager AWS KMS administración de claves con FIPS 140-2	No está cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.14	El VDSS proporcionará la capacidad de detectar e identificar el secuestro de sesiones de la aplicación.	N/A	N/A	No está cubierto
2.1.2.15	El VDSS proporcionará una extensión DMZ del DoD para respaldar las aplicaciones orientadas a Internet (IFA).	N/A	N/A	No está cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.16	El VDSS proporcionará una capacidad de captura completa de paquetes (FPC) o una capacidad de FPC equivalente a un servicio en la nube para grabar e interpretar las comunicaciones transversales.	Network Firewall Logs de flujo de VPC	N/A	Cubierto
2.1.2.17	El VDSS proporcionará métricas y estadísticas del flujo de paquetes de la red para todas las comunicaciones transversales.	CloudWatch	Supervise el rendimiento de la red de los puntos finales de la interfaz de VPC mediante CloudWatch	Cubierto

ID	Requisito de seguridad del VDSS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.2.18	El VDSS se encargará de inspeccionar el tráfico que entra y sale de la red privada virtual del propietario de cada misión.	Network Firewall	Implemente un filtrado de tráfico centralizado	Cubierto

Hay componentes del CAP que usted define y que no se tratan en esta guía porque cada agencia tiene su propia conexión con el CAP AWS. Puede complementar los componentes del VDSS con el LZA para poder inspeccionar el tráfico entrante. AWS Los servicios que se utilizan en la LZA permiten analizar los límites y el tráfico interno para ayudar a proteger su entorno. Para seguir creando un VDSS, hay algunos componentes de infraestructura adicionales que no están incluidos en el LZA.

Al utilizar la nube privada virtual (VPC), puede establecer límites en cada uno de ellos Cuenta de AWS para cumplir con los estándares de la SCCA. Esto no está configurado como parte de la LZA porque las VPC, el direccionamiento IP y el enrutamiento son componentes que debe configurar según sea necesario para su infraestructura. Puede implementar componentes como las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) en Amazon Route 53. También puede añadir WAF comerciales AWS WAF o de terceros para ayudarle a alcanzar los estándares necesarios.

Además, para cumplir con el requisito 2.1.2.7 de la DISA SCCA, puede utilizar un Network GuardDutyFirewall para proteger y monitorear el entorno en busca de tráfico malicioso.

Virtual Data Center Managed Services

El propósito de Virtual Data Center Managed Services (VDMS) es proporcionar seguridad para el host y servicios de centro de datos compartidos. Las funciones del VDMS pueden ejecutarse en el centro de su SCCA o el propietario de la misión puede implementar partes de él por su cuenta.

Cuentas de AWS Este componente se puede proporcionar en su entorno. AWS Para obtener más información sobre el VDMS, consulte la Guía de requisitos de seguridad de la computación en la nube del DoD.

La siguiente tabla contiene los requisitos mínimos del VDMS. En ella se explica si la LZA cumple con cada requisito y cuál Servicios de AWS puede utilizar para cumplirlos.

ID	Requisito de seguridad de VDMS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.3.1	El VDMS proporcionará una solución de evaluación asegurada del cumplimiento (ACAS), o un equivalente aprobado, para llevar a cabo una supervisión continua de todos los enclaves del CSE.	AWS Config AWS Security Hub CSPM AWS Audit Manager Amazon Inspector	Escaneo de vulnerabilidades con Amazon Inspector	Cubierto parcialmente
2.1.3.2	El VDMS proporcionará un sistema de seguridad basado en el host (HBSS), o un equivalente aprobado, para gestionar la seguridad	N/A	N/A	No está cubierto

ID	Requisito de seguridad de VDMS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
	de los puntos finales en todos los enclaves del CSE.			
2.1.3.3	El VDMS proporcionará servicios de identidad para incluir un respondedor del Protocolo de estado de certificados en línea (oCloud Workload Security) para la autenticación de dos factores mediante la tarjeta de acceso común (CAC) del DoD remota de los usuarios con privilegios del DoD en los sistemas instanciados dentro del CSE.	Multi-factor autenticación (MFA) disponible a través de: AWS Identity and Access Management (IAM) AWS IAM Identity Center AWS Directory Service for Microsoft Active Directory AWS Autoridad de certificado privado	Configurar una tarjeta CAC para Amazon WorkSpaces	Cubierto parcialmente

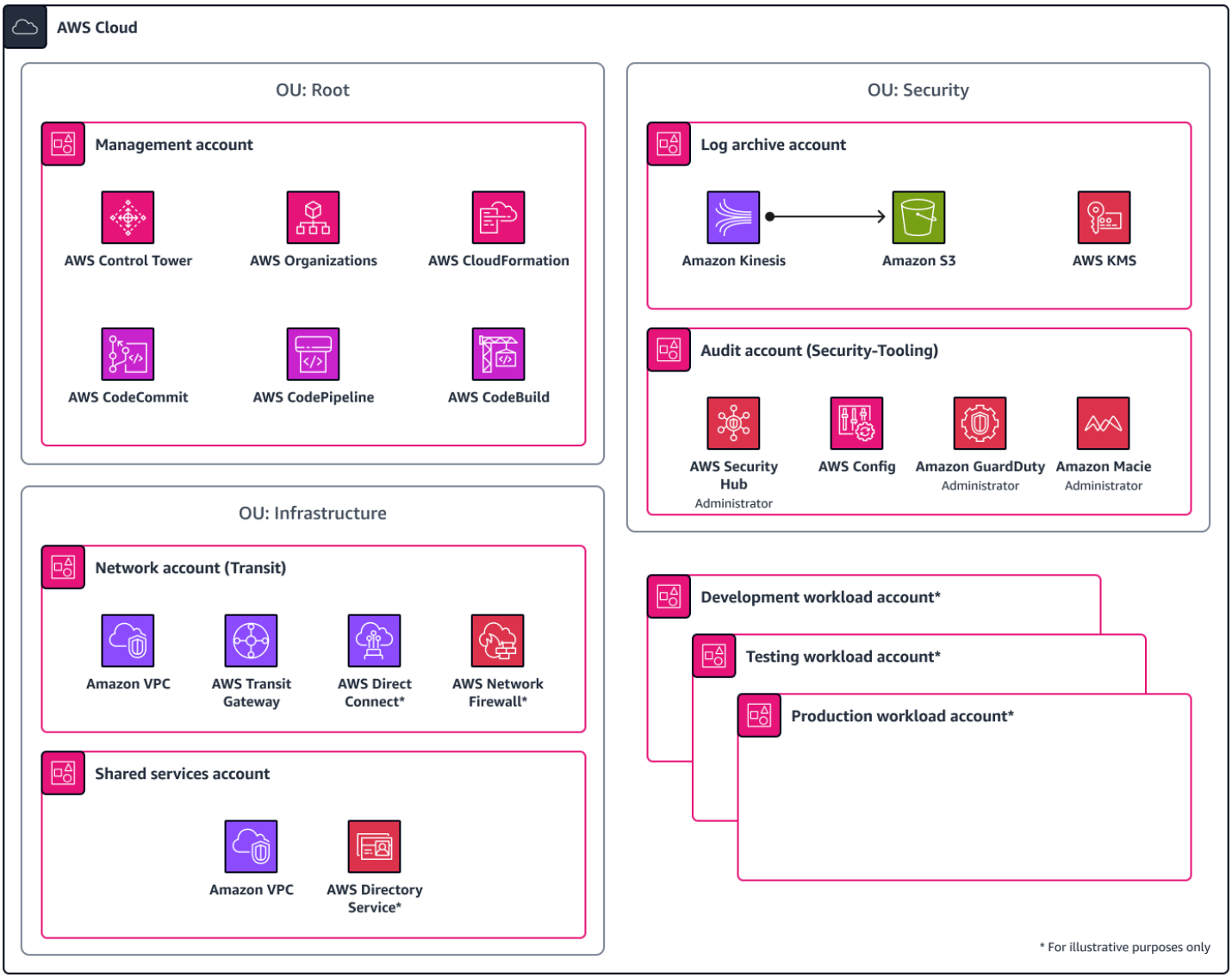
ID	Requisito de seguridad de VDMS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.3.4	El VDMS proporcionará un sistema de gestión de configuraciones y actualizaciones que sirva a los sistemas y aplicaciones de todos los enclaves del CSE.	AWS Systems Manager Patch Manager AWS Config	Automatizar la administración de parches con (vídeo) AWS Systems Manager YouTube	Cubierto parcialmente
2.1.3.5	El VDMS proporcionará servicios de dominio lógico que incluyan el acceso a los directorios, la federación de directorios, el protocolo de configuración dinámica de host (DHCP) y el sistema de nombres de dominio (DNS) para todos los enclaves del CSE.	AWS Managed Microsoft AD Amazon Virtual Private Cloud (Amazon VPC) Amazon Route 53	Configure los atributos de DNS para su VPC	Cubierto parcialmente

ID	Requisito de seguridad de VDMS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.3.6	El VDMS proporcionará una red para gestionar los sistemas y las aplicaciones dentro del CSE que esté separada lógicamente de las redes de usuarios y datos.	Amazon VPC Subredes de Amazon VPC	N/A	Cubierto

ID	Requisito de seguridad de VDMS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.3.7	El VDMS proporcionará un sistema de registro y archivado de eventos del sistema, la seguridad, las aplicaciones y la actividad del usuario para que los usuarios privilegiados que realicen actividades de BCP y MCP recopilen, almacenen y accedan a los registros de eventos de manera común.	AWS Security Hub CSPM AWS CloudTrail Amazon CloudWatch Logs Amazon Simple Storage Service (Amazon S3)	Registro centralizado con OpenSearch	Cubierto

ID	Requisito de seguridad de VDMS	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.3.8	El VDMS permitirá el intercambio de los atributos de autenticación y autorización de los usuarios con privilegios del DoD con el sistema de administración de identidad y acceso del CSP para permitir el aprovisio namiento, la implementación y la configura ción del sistema en la nube.	AWS Managed Microsoft AD	Mejore su configuración de seguridad AWS Managed Microsoft AD	No está cubierto
2.1.3.9	El VDMS implementará las capacidad es técnicas necesarias para ejecutar la misión y los objetivos de la función de TCCM.	AWS Managed Microsoft AD IAM Centro de identidades de IAM	N/A	Cubierto parcialmente

Como se muestra en la siguiente imagen, la LZA establece los componentes fundamentales para cumplir con los requisitos básicos del VDMS. Hay algunos componentes adicionales que debe configurar después de implementar la LZA para cumplir con los estándares del VDMS. En la tabla anterior, asegúrese de revisar los enlaces de la columna Recursos adicionales. Estos enlaces le ayudan a configurar estos elementos adicionales o proporcionan más mejoras de seguridad.



Integración de servicios complementarios

En la columna de recursos adicionales de la tabla anterior se enumeran los recursos que le ayudarán a ampliar la LZA para cumplir con los requisitos del VDMS. AWS Además, ofrece algunos materiales

de taller que le ayudarán a configurar una arquitectura de nube segura. Sin modificaciones, la LZA cumple con los IL4/IL5 requisitos, pero puede implementar servicios adicionales para mejorar la seguridad de su AWS entorno.

Por ejemplo, Amazon Inspector es un servicio de gestión de vulnerabilidades que analiza continuamente sus AWS cargas de trabajo en busca de vulnerabilidades de software y exposición no intencionada a la red. Puede usarlo para identificar e investigar vulnerabilidades en los sistemas operativos anfitriones, como Windows y Linux. Aunque es posible que Amazon Inspector no incorpore completamente todos los requisitos necesarios para un sistema de seguridad basado en host (HBSS), al menos proporciona una evaluación de vulnerabilidad de nivel básico de las instancias.

Revisiones del sistema operativo

La aplicación de parches al sistema operativo es un componente fundamental del funcionamiento de un entorno seguro. AWS ofrece y recomienda el uso del Administrador de parches, una capacidad que permite mantener bases de AWS Systems Manager referencia de parches consistentes y automatizar la implementación de parches. Patch Manager automatiza el proceso de parchear los nodos gestionados tanto con actualizaciones relacionadas con la seguridad como con otros tipos de actualizaciones.

Puede utilizar Patch Manager para aplicar parches a los sistemas operativos y a las aplicaciones. (En Windows Server, el soporte de aplicaciones se limita a las actualizaciones de las aplicaciones publicadas por Microsoft). Para obtener más información, consulte Cómo organizar procesos de parches personalizados y de varios pasos mediante AWS Systems Manager Patch Manager en el blog sobre operaciones y migraciones en la AWS nube.

Para obtener instrucciones paso a paso sobre el uso de Patch Manager, consulte el taller sobre herramientas AWS de gestión y gobierno.

Para obtener más información sobre cómo proteger las cargas de trabajo de Microsoft Windows en AWS, consulte el taller Cómo proteger las cargas de trabajo de Windows en el AWS taller.

Administrador de credenciales en la nube de confianza

El Trusted Cloud Credential Manager (TCCM) es un componente de la SCCA. Es responsable de la administración de credenciales. Al establecer la TCCM, es importante permitir el acceso de los menos privilegiados a la SCCA. Esto se puede lograr mediante el uso AWS de servicios de administración de identidad y acceso. Un componente adicional del TCCM es una conexión a Virtual

Data Center Managed Services (VDMS). Puede utilizar esta conexión según sea necesario para acceder al TCCM y administrar el TCCM Consola de administración de AWS .

El TCCM es una combinación de tecnologías y estándares que rigen el acceso a. AWS El TCCM se considera fundamental para la mayoría de las implementaciones porque controla los permisos de acceso. La función TCCM no pretende imponer requisitos exclusivos de gestión de identidades al proveedor de servicios en la nube (CSP) comercial. La TCCM tampoco prohíbe el uso de la federación CSP del DoD o de soluciones de agentes de identidad de terceros para proporcionar el control de identidad previsto.

Los componentes de la política de TCCM se basan en el entendimiento general de que los CSP ofrecen un sistema de gestión de identidad y acceso que permite controlar el acceso a los sistemas en la nube. Dichos sistemas pueden incluir los componentes de servicio de la consola de acceso, la API y la interfaz de línea de comandos (CLI) del CSP. En el nivel básico, el TCCM debe bloquear las credenciales que se pueden utilizar para crear redes y otros recursos no autorizados. El TCCM es nombrado por el oficial autorizado (AO) encargado de supervisar los sistemas de TI. Las políticas del TCCM establecen la necesidad de un modelo de acceso con privilegios mínimos. Estas políticas son responsables del suministro y el control de las credenciales de los usuarios privilegiados en la nube comercial. Esto es para mantener la coherencia con la Guía de requisitos de seguridad de la computación en la nube del DoD, que aborda la implementación de políticas, planes y procedimientos para administrar las credenciales de la cuenta del portal. Antes de conectarse a la Red de Sistemas de Información de Defensa (DISN), DISA valida la existencia del Plan de administración de credenciales en la nube (CCMP) como parte del proceso de aprobación de la conexión definido en la Guía del proceso de conexión.

La siguiente tabla contiene los requisitos mínimos para el TCCM. Explica si la LZA aborda cada requisito y cuál Servicios de AWS puede utilizar para cumplirlos.

ID	Requisitos de seguridad de TCCM	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.4.1	La TCCM desarrollará y mantendrá un plan de gestión de credencia les en la nube	N/A	N/A	No está cubierto

ID	Requisitos de seguridad de TCCM	AWS tecnologías	Recursos adicionales	Cubierto por LZA
	(CCMP) para abordar la implementación de las políticas , los planes y los procedimientos que se aplicarán a la gestión de las credenciales de las cuentas del portal de clientes del propietario de la misión.			
2.1.4.2	El TCCM recopilará, auditará y archivará todos los registros de actividad y alertas del Portal del Cliente.	AWS CloudTrail Amazon CloudWatch Logs	N/A	Cubierto

ID	Requisitos de seguridad de TCCM	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.4.3	El TCCM se asegurará de que los usuarios privilegiados del DoD que participan en actividades de MCP y BCP compartan las alertas del registro de actividades, las reenvíen o las puedan recuperar.	AWS CloudTrail CloudWatch Registros Amazon Simple Notification Service (Amazon SNS) CloudWatch Registra información	N/A	Cubierto

ID	Requisitos de seguridad de TCCM	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.4.4	Según sea necesario para el intercambio de información, el TCCM creará cuentas de acceso al repositorio de registros para que los usuarios privilegiados que realicen actividades tanto de MCP como de BCP puedan acceder a los datos del registro de actividades.	AWS CloudTrail CloudWatch Registros Amazon SNS CloudWatch Registra información	N/A	Cubierto
2.1.4.5	El TCCM recuperará y controlará de forma segura las credenciales de las cuentas del portal de clientes antes de conectar la aplicación a la DISN.	AWS IAM Identity Center	N/A	Cubierto

ID	Requisitos de seguridad de TCCM	AWS tecnologías	Recursos adicionales	Cubierto por LZA
2.1.4.6	El TCCM creará, emitirá y revocará, según sea necesario, las credenciales del portal de clientes menos privilegiados con acceso basado en roles para los administradores de aplicaciones y sistemas propietarios de la misión (es decir, los usuarios con privilegios del DoD).	AWS Identity and Access Management (IAM) AWS Directory Service for Microsoft Active Directory	N/A	Cubierto

Para permitir que el TCCM cumpla con los requisitos, la LZA utiliza el control programático de los recursos a través del servicio IAM. Además, puede combinar la IAM para implementar el inicio de sesión único AWS Managed Microsoft AD en otro directorio. Esto vincula el AWS entorno a la infraestructura local mediante la confianza de Active Directory. En la LZA, la implementación se implementa con funciones de IAM para un acceso temporal y basado en sesiones. Las funciones de IAM son credenciales efímeras que ayudan a la organización a cumplir los requisitos de TCCM necesarios.

Si bien la LZA implementa el acceso con privilegios mínimos y el acceso programático a corto plazo a AWS los recursos, revise las mejores prácticas de IAM para asegurarse de seguir las pautas de seguridad recomendadas.

Para obtener más información sobre la implementación AWS Managed Microsoft AD, consulte la AWS Managed Microsoft ADsección del taller del Día de Inmersión de Active Directory en AWS.

El modelo de responsabilidad AWS compartida se aplica a la TCCM y a la LZA. La LZA desarrolla los aspectos fundamentales del control de acceso, pero cada organización es responsable de la configuración de sus controles de seguridad.

Conclusión y recursos

Para el Departamento de Defensa de los EE. UU. (DoD), esta guía explica cuáles son los requisitos de la Agencia de Sistemas de Información de Defensa (DISA) para implementar una arquitectura de computación en nube segura (SCCA). Al utilizar el acelerador de zonas de aterrizaje (LZA) AWS, puede implementar las AWS ofertas y eliminar el trabajo pesado e indiferenciado. Esto le ayuda a centrarse en su misión de crear una infraestructura de nube que IL4 cumpla o IL5 cumpla con las normas.

AWS recursos

- AWS Servicios incluidos en el ámbito de aplicación del programa de AWS cumplimiento (conformidad)
- Guía de requisitos de seguridad de la computación en la nube del Departamento de Defensa (AWS cumplimiento)
- AWS Guías de cumplimiento para clientes (AWS cumplimiento)
- Landing Zone Accelerator activado AWS (biblioteca de AWS soluciones)
- Guía de implementación de Landing Zone Accelerator on AWS
- SCCA en el diagrama de arquitectura AWS GovCloud
- Infraestructura en la nube del Departamento de Defensa como código (IaC) para AWS ()AWS Marketplace

Otros recursos de

- Diseño de referencia del punto de acceso nativo en la nube (CNAP) del Departamento de Defensa (DoD) (sitio web del DoD)
- DOW Cloud iAC (sitio web de DISA)

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	12 de marzo de 2024

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.