

Análisis de una implementación de firewall seguro en MCD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Antecedentes](#)

[Supervisión de la implementación](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo monitorear una implementación de Multicloud Defense usando los registros del sistema disponibles para validar que la implementación está progresando.

Prerequisites

Esto se aplica a entornos de nube como AWS, Azure, GCP u Oracle para permitir una integración perfecta en el conector de nube seguro y el FirePOWER Management Center (cdFMC) implementado en la nube

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Flujos de trabajo de implementación de Defensa multinube (MCD)
- Conceptos de conectividad de red de nube y conector de nube seguro (SCC)
- Supervisión FMC y validación del estado para implementaciones en la nube

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Defensa multicloud
- Entorno AWS
- Firepower Management Center implementado en la nube (cdFMC)
- Conector de nube seguro (SCC)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Defensa multicloud
- Conector de nube seguro (SCC)
- Firepower Management Center implementado en la nube (cdFMC)

Antecedentes

Al implementar un dispositivo en una plataforma de nube mediante MCD, hay varios lugares que revisar para garantizar que la implementación progresa correctamente. Estas herramientas ayudan a supervisar la implementación y proporcionan contexto adicional cuando se produce un error. Los mismos principios de supervisión se aplican a las implementaciones de AWS, Azure y GCP.

Los registros del sistema son la fuente principal de visibilidad de la implementación en MCD. Este es el mejor lugar para revisar los eventos de creación de clústeres, la actividad de creación de puertas de enlace, los inicios de instancias y cualquier excepción encontrada durante el flujo de trabajo de implementación. El CSP también emite alertas cuando falla un paso de registro o implementación, lo que ayuda a reducir el área a investigar.



Consejo: Si se agota el tiempo de espera del registro, compruebe los registros del sistema MCD antes de solucionar problemas del entorno en sí. Los registros a menudo

identifican el paso fallido.

Supervisión de la implementación

Revise los registros del sistema en MCD para confirmar que la implementación está avanzando en las etapas esperadas. Este es el primer lugar y el más útil para comprobar el estado de la implementación, la creación del gateway, la actividad de inicio de la instancia y cualquier error registrado.

Navegue hasta:

Defensa de varias nubes > Investigar > Registros del sistema

En el ejemplo se muestra la creación correcta de la puerta de enlace y dónde se inician las instancias de clúster. En este caso, las instancias del gateway se alojan en la región US-east-2 y en la zona de disponibilidad us-east-2b.

AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	FTDv instance i-0bdd9ff657...
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	Gateway Enabled for Gateway mcd-lab-cluster. Newly created instances in this gateway are 1 in region us-east-2 availability zone us-east-2b
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	
			Gateway Enabled for Gatew...

Utilice la página Registros del Sistema para verificar que la implementación se está moviendo a través del ciclo esperado y para recopilar mensajes de error detallados cuando falla un paso.

Compruebe el FMC en busca de errores de implementación cuando se informa de un tiempo de espera de registro o de un evento de implementación fallido. El FMC puede proporcionar una alerta de alto nivel que indique que la implementación no se ha completado correctamente.

Las comprobaciones recomendadas incluyen:

1. Verifique la conectividad entre la red en la nube y el conector de nube seguro (SCC).
2. Confirme que se ha completado cada paso de la implementación de la guía de implementación.
3. Valide que el rol IAM correcto esté configurado y en uso.

Register	Registration ciscomcd-mcd-lab-cluster-gcrpxvxq: Established secure connection	27s
Register	Registration ciscomcd-mcd-lab-cluster-gcrpxvxq: Registration timed out. Please check connectivity and registration id	2m 6s X
Register	Registration ciscomcd-mcd-lab-cluster-dfmnhqfi: Established secure connection	2m 32s



Precaución: Un error de registro puede ocurrir una o más veces antes de que se complete un registro correcto. Este comportamiento puede ser causado por el comportamiento del temporizador de la nube y no es necesariamente un problema permanente.

Si el FMC del SCC informa de un tiempo de espera de registro, los registros del sistema suelen incluir más detalles sobre el fallo específico. En la mayoría de los casos, el problema es una combinación de problemas de conectividad, IAM o configuración, y los registros son la mejor fuente para reducir el paso fallido.

Confirme que la implementación se ha completado correctamente mediante la revisión del evento de éxito final en los registros del sistema MCD. Cuando la implementación se realiza correctamente, los registros pueden mostrar un evento de finalización correcta.

System Logs

UTC Local Refresh

Quick Filters Advanced

Last 1 Hour

CSP Account	Gateway	Severity	Sub Type	Message
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info		FTDv instance i-0e880723d9ce7772f policy deployment is done with Multicloud defense configurations. Marking as health_check pending
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info		FTDv instance i-0e880723d...

Una implementación correcta también puede verse en el FMC, donde los dispositivos implementados muestran un estado de conexión y los indicadores de estado aparecen en verde.

Device Management			
Devices		New device management UI	Migrate Deployment history
3		Normal 3	
Q Type to search		Total: 3	
☐ Name	Version	Model	
☐ mcd-lab-cluster 2			
☐ ✓ cisco-mcd-lab-cluster-dfmmhqi N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	
☐ ✓ cisco-mcd-lab-cluster-gcrpxvq N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	

Esto confirma que el clúster se ha creado correctamente y que el dispositivo está funcionando en el entorno esperado.

Verificación

Hay algunos lugares para verificar que la implementación de AWS sea correcta:

- Los registros del sistema muestran una actividad de implementación normal y ningún error de bloqueo.
- El dispositivo o la puerta de enlace se crean en la región esperada y en la zona de disponibilidad.
- El FMC indica que el dispositivo está conectado y en buen estado.
- No se agota el tiempo de espera para el registro ni permanecen advertencias de implementación erróneas en los registros.

Cuando todas estas condiciones son verdaderas, la implementación de MCD se puede considerar exitosa.

Troubleshoot

Si la implementación no alcanza un estado correcto:

- Revise los registros del sistema MCD para conocer el paso exacto que ha fallado.
- Compruebe el FMC para ver si hay alertas de registro o de conectividad.
- Confirme la red en la nube y la conectividad del conector de nube seguro.
- Valide el rol IAM y todos los requisitos previos de la guía de implementación.
- Confirme que el clúster se está implementando en la región y zona de disponibilidad esperadas.

Información Relacionada

- [Guía de arquitectura de defensa de Cisco Multicloud](#)
- [Informe técnico de Cisco Multicloud Defense](#)
- [Guía del usuario de Cisco Multicloud Defense: Registros del sistema](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).