centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-666

INFRAESTRUCTURA CENTRALIZADA EN APLICACIONES (CISCO ACI)

SEPTIEMBRE 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-20-186-9

Fecha de Edición: septiembre de 2020
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

septiembre de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

El actual uso de tecnologías emergentes que permiten la virtualización de los sistemas de las Tecnologías de la Información y la Comunicación (TIC), en adelante Sistemas, se ha hecho crítica con la extensión del empleo de dichas tecnologías a todos los ámbitos.

Las amenazas asociadas a un sistema, que pueden afectar a la confidencialidad, integridad y disponibilidad de la información manejada, o a la propia integridad y disponibilidad del sistema, son tenidas en cuenta a la hora de establecer los requisitos de seguridad mínimos, de tal manera, que las medidas de protección que se implementan tienen por objeto hacer frente a dichas amenazas reduciendo la superficie de exposición y minimizando el impacto de las mismas.

La seguridad se tratará desde la fase de diseño del sistema, donde se definirán las salvaguardas a implementar, permitiendo de esta manera que el análisis y gestión de riesgos de seguridad estén presentes en el proceso de desarrollo del sistema.

La Política STIC determina que todos los sistemas que requieran manejar información clasificada deberán ser previamente acreditados, de acuerdo con el procedimiento que, para tal fin, apruebe la Autoridad de Acreditación de Seguridad (AAS).

El procedimiento de acreditación de seguridad, entre otros requisitos, confirmará que las medidas de seguridad que satisfacen los requisitos STIC se encuentran implementadas en los Sistemas antes de manejar información clasificada.

3. OBJETO

El objeto de esta instrucción técnica es establecer los requisitos STIC mínimos, que deben realizarse en los sistemas CIS que contemplen la implementación de una infraestructura centralizada en aplicaciones de Cisco (ACI), cuando manejen información clasificada.

El presente informe proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad y buenas prácticas necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestas las arquitecturas virtuales sobre las que se implementa un sistema que va a manejar información clasificada.

Por su parte, a los sistemas del Sector Público que no traten información clasificada les será de aplicación el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), de conformidad con lo dispuesto en la Ley 40/2015, de Régimen Jurídico del Sector Público y atendiendo a lo señalado en la Ley 39/2019, de Procedimiento Administrativo Común de las Administraciones Públicas, ambas de 1 de octubre.

4. ALCANCE

El propósito del presente documento es realizar un análisis general de los mecanismos y la configuración de seguridad destinada a proporcionar una serie de recomendaciones de seguridad para la protección de los datos, comunicaciones e información que almacenan los sistemas con implementaciones Cisco ACI.

En los Sistemas que manejen información clasificada, se determinarán las autoridades y responsables relacionados con la seguridad de los mismos a lo largo de su ciclo de vida (determinación de la necesidad, diseño, desarrollo, implantación, operación, mantenimiento y retirada).

Dichas autoridades tendrán en cuenta los requisitos STIC a implementar en las diferentes fases del ciclo de vida debiendo constar y estar presentes en la documentación de seguridad asociada al Sistema.

La Autoridad de Acreditación de Seguridad podrá determinar la aplicación de esta instrucción técnica a cualquier otro tipo de Sistema bajo su responsabilidad.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de recomendaciones seguridad, es conveniente explicar el proceso de refuerzo de seguridad de una infraestructura centralizada en aplicaciones de Cisco (ACI). Dicho proceso estará basado en las recomendaciones de seguridad establecidas por el fabricante que ofrecen la posibilidad de mantener una infraestructura de red de forma centralizada con el uso de su tecnología.

En función de su arquitectura, la metodología de aplicación de las recomendaciones de seguridad establecidas en el presente documento, podrán variar, es por ello que, las recomendaciones de seguridad están dirigidas a la tecnología Cisco ACI en sí, y no a la totalidad de las soluciones de implementación de una infraestructura de red centralizada.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

La guía ha sido desarrollada con el objetivo de dotar a la aplicación Cisco ACI, con la seguridad adecuada, dependiendo del entorno sobre el que se aplique, teniendo en consideración el ámbito y nivel de seguridad de la información a tratar. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas, y por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, roles o características deseadas.

El espíritu de estas guías no está dirigido a remplazar políticas de seguridad consolidadas y probadas de las organizaciones, sino a servir como línea base de seguridad.

Esta línea deberá ser adaptada a las necesidades propias de cada organización, pero sin desviarse de la seguridad mínima necesaria para el manejo de información clasificada.

6. CARACTERÍSTICAS DE LA SOLUCIÓN CISCO ACI

Cisco ACI (Infraestructura Centrada en Aplicaciones) es la implementación SDN de Cisco. Es una solución basada en políticas que integra el software y el hardware. Arquitectura integral, con automatización centralizada y perfiles de aplicaciones basados en políticas e integrado en un entorno fundamentado en APIs estandarizadas y abiertas. Gracias al controlador Cisco APIC se consigue controlar la conectividad L2/L3 y las políticas de seguridad entre diferentes Grupos de Seguridad (EPGs).

Las características más significativas de ACI como arquitectura son:

a) Cisco APIC: Es el único punto de gestión de toda la Red (física y virtual).

b) Escalabilidad: Los nuevos nodos se añaden automáticamente al Fabric.

c) Seguridad: Todo el Fabric actúa como un Router + Firewall.

d) Gestión sencilla: Actualizaciones, identificación avanzada de problemas, diagnóstico…etc.

Los componentes de Cisco ACI son:

a) Controlador APIC (Application Policy Infraestructure Controler): Como el único punto de gestión de toda la Red (física y virtual), que actúa como un repositorio central de todas las políticas y tiene la capacidad de desplegar bajo demanda los recursos de red según la necesidad.

b) ACI Fabric: Familia switches Cisco Nexus 9000 formando la arquitectura tipo Leaf-Spine.

c) Ecosistema de partners: Hipervisores y servicios L4-L7.

El diseño de Cisco ACI se ha hecho en conformidad con Open Source y Open APIs. Dentro de ACI todo se representa como un objeto, y cada objeto se puede manipular utilizando REST API (POST, GET, UPDATE, DELETE) y Python, permitiendo así varios tipos de orquestación, automatización y disposición de recursos de red a otras plataformas tales como OpenStack, Puppet, Ansible, etc.

6.1 EVOLUCIÓN DE LAS SOLUCIONES SDN

SDN (Software-defined network) define a una arquitectura de red con gestión centralizada basada en software que se caracteriza por ser una arquitectura escalable, flexible, programable y automatizable. Con este propósito, se distinguen y separan los dos niveles de funcionamiento:

a) El plano de control (control plane), referido a la lógica de control o inteligencia del hardware y que no es otra cosa que proporcionar la información de enrutamiento tanto de capa 2 como de capa 3 a dispositivos de red que requieran de esta información para el reenvío de paquetes. En el modelo centralizado que propone una tecnología SDN, el controlador es el encargado de distribuir esta información mediante las tablas MAC y FIB.

b) El plano de datos (data plane), que permanece en los dispositivos de red (todos los nodos como routers, switches y firewalls). En una SDN, el plano de datos reenvía el tráfico de datos al siguiente salto en función de la información obtenida, motivo por el cual requiere poca potencia de cálculo.

Al utilizar un software centralizado independiente del hardware, el plano de control puede definirse con mayor libertad puesto que se puede programar la decisión de priorización del tráfico, así como la administración de red es mucho más flexible.

Para que el software en el plano de control pueda enviar las instrucciones a los nodos de la red que participan en el flujo del tráfico de datos, se necesita una interfaz específica de comunicación entre el plano de control y el de datos. La solución más extendida es OpenFlow, (Gestionado por la Open Networking Foundation (ONF), y está considerado como la primera interfaz estandarizada entre los planos de control y de datos en una arquitectura SDN). En muchas redes definidas por software, OpenFlow reemplaza a las diferentes interfaces integradas en los dispositivos, con lo que se limita la dependencia respecto a fabricantes de hardware.

Una vez que se establece la comunicación entre el software y el hardware, el propio software SDN en el plano de control se encarga de centralizar y facilitar al administrador la gestión de los nodos de la red, permitiéndole así, dirigir los flujos de datos de una forma mucho más eficiente que en las redes tradicionales en las que cada uno de los distintos nodos cuenta con su propia lógica de control, lo que facilita en gran medida la virtualización y el escalado de recursos. A esto se suma que los datos de enrutamiento y topología se envían todos a un mismo lugar central que es el controlador.

6.1.1 ARQUITECTURAS SDN

Aunque están en una continua evolución y cambio, las principales arquitecturas de SDN se pueden dividir en:

a) Switch-based SDN (SDN basado en Switches): La idea del SDN se basó originalmente en el modelo basado en Switches, que procesan paquetes con un sistema como OpenFlow, que dicta el comportamiento de los nodos de la red. Esto proporciona un punto de control central que gestiona cómo los nodos manejan el tráfico de la red (pueden ser virtuales o físicos, siempre que sean compatibles con OpenFlow).

b) SDN overlay (Superposición de SDN): El modelo de superposición de SDN crea túneles virtuales a través de la red física para ejecutar múltiples topologías de red virtual (VN) sobre una infraestructura existente. Esto permite que una VN sea una red de capa 2 o capa 3, y que una red física sea de capa 2 o capa 3, según el tipo de superposición.

c) Hybrid SDN (SDN híbrido): Un modelo hibrido de SDN combina protocolos tradicionales de las redes Legacy y SDN. Un administrador de red, por ejemplo, puede configurar el plano de control de la SDN para gestionar flujos de tráfico específicos, mientras que los protocolos de red tradicionales gestionan los demás flujos de tráfico de la red. La SDN híbrida utiliza diversos tipos de redes, como VPN, Ethernet, MPLS, entre otras, para conectar múltiples lugares y trabajadores. El enfoque de la SDN híbrida proporciona flexibilidad al utilizar las tecnologías más recientes de SDN para satisfacer las demandas de cada lugar.

6.1.2 MODELOS DE DESPLIEGUE DE SDN (REACTIVA, PROACTIVA Y PREDICTIVA)

Cuando un flujo llega a un nodo de la red (switch) se realiza un mapeo de la tabla de flujos y en caso de no existir una entrada se realiza una consulta al controlador para recibir información. Se detallan los tres modos:

En el modo reactivo, el controlador actúa después de recibir estas peticiones y se ajustan constantemente creando una regla en la tabla de flujos para el paquete correspondiente, ya que los cambios se hacen inmediatamente como reacción a las condiciones actuales de la red (generalmente se asocia con SDN y OpenFlow). Este es el modelo básico de gestión de la volatilidad en el que hay una alta tasa de cambio en la ubicación de los puntos finales (normalmente máquinas virtuales) y OpenFlow se utiliza para actualizar continuamente la ubicación y el camino a través de la red hasta cada punto final.

En el modo proactivo anticipan los problemas de la red e intentan abordarlos antes de que se conviertan en un problema real (lo que requeriría una reacción). El modo proactivo crea una tabla de flujos para cada posible coincidencia de tráfico en ese nodo de la red (Switch) dando así solución a conocer el camino que deberá tomar el tráfico de datos.

El modo predictivo es el modelo híbrido que combina el modo reactivo y proactivo beneficiando en las ventajas de ambos, que utiliza datos históricos sobre el rendimiento de la red para ajustar las rutas y los flujos periódicamente. Este enfoque es menos perturbador, ya que se produce con menos frecuencia, pero aun así, permite que las tendencias en el flujo y el volumen de datos informen las rutas apropiadas.

6.2 OBJETIVOS Y VENTAJAS DE SDN

Se podría decir que la finalidad de una solución SDN es facilitar la implementación y posterior implantación de servicios de red de una manera sencilla, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel.

La idea principal reside en el hecho de gestionar las redes separando el plano de control del plano de datos. Esta separación entre el software y el hardware hace que este último se pueda desprender de parte de sus procesos, consiguiendo así ser más eficiente en las tareas de conmutación.

Es decir, SDN es una manera de enfrentarse a la creación de redes en la cual el control se desprende del hardware y se le da a una aplicación de software, llamada controlador. Esto permite a un administrador de red modificar el tráfico desde una consola de control centralizada. El administrador puede cambiar cualquier regla de los switches de red cuando sea necesario, es decir, le permite tener más control que nunca sobre el flujo del tráfico de red.

A continuación, se exponen de forma resumida, algunas de las principales ventajas que puede aportar una solución SDN

a) **Agilidad y flexibilidad**. SDN permite a los administradores de red desplegar servicios, aplicaciones e infraestructuras de forma rápida permitiendo así alcanzar los objetivos marcados en el menor tiempo posible.

b) **Permite innovación**. Los entornos SDN permiten crear nuevos tipos de aplicaciones y modelos de negocio por parte de las empresas.

c) **Reduce el gasto operacional**. La tecnología SDN permite el control de elementos de red mediante el uso de programas, como switches/routers. En consecuencia, permite una reducción del tiempo de gestión por parte de los administradores y reduce considerablemente la probabilidad de un error humano.

d) **Reduce el gasto en hardware**. Los entornos SDN permiten reutilizar el hardware existente, alargando así su vida útil. Además, permite a los administradores de redes disponer de hardware de diferentes fabricantes siempre que sea posible la integración de dicho fabricante con la tecnología SDN.

Dado que se centraliza la administración de la red, el controlador, se convierte en el centro de control y de toma de decisión de la red, por lo tanto, hay que protegerlo y asegurarlo, ya que un problema en el controlador afectará a toda la red.

Los principales riesgos del controlador en un entorno SDN son:

a) **Escalabilidad**: Un aumento repentino, o no programado de trabajo puede provocar que el controlador se transforme en un "cuello de botella" o incluso llegar a "saturarse", y de esta manera afectar a toda la red.

b) **Seguridad**: los ataques al controlador podrían afectar al funcionamiento de toda la red. Para su protección se pueden utilizar las herramientas de seguridad que se aplican en las redes convencionales y también mecanismos de seguridad específicos para SDN.

6.3 COMPONENTES DE CISCO ACI

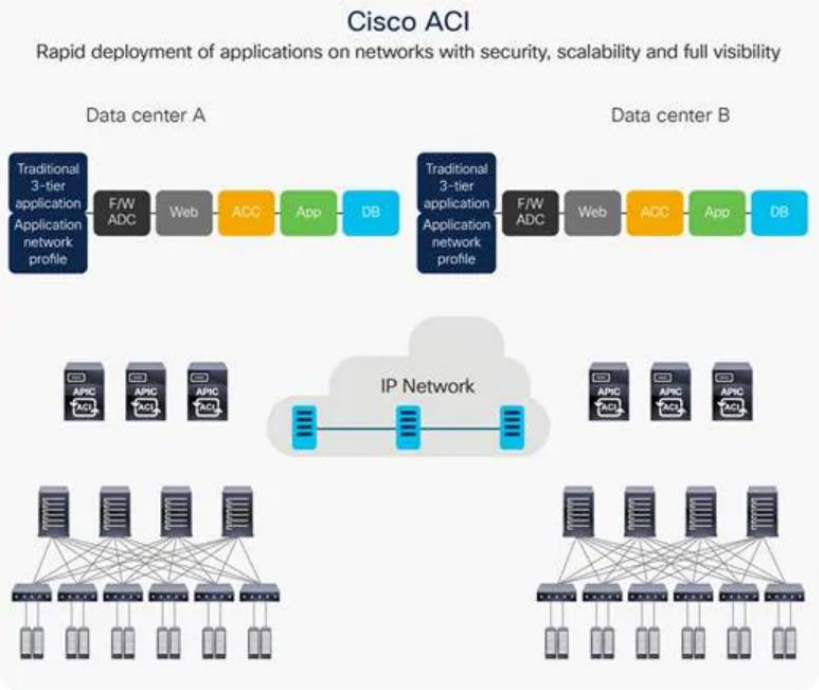
La solución Cisco ACI consta de los siguientes componentes principales:

a) **Cisco Application Policy Infrastructure Controller (APIC)**, (Controlador de infraestructura de políticas de aplicaciones de Cisco), es el componente principal de la arquitectura de la solución Cisco ACI. es un controlador en clúster centralizado que optimiza el rendimiento, puede admitir cualquier aplicación desde cualquier lugar y unifica el funcionamiento de entornos físicos y virtuales. El controlador gestiona y opera un fabric de Cisco ACI con capacidad de ampliación y varios clientes.

   Cisco APIC se ha diseñado, para ofrecer una administración centralizada y en función del programa. Cisco APIC cuenta con una API ascendente mediante XML y JSON, y dispone de una interfaz de línea de comandos (CLI) y una interfaz de usuario gráfica (GUI) que usa esta API para administrar el fabric. El sistema también ofrece una API descendente de código abierto que permite a los proveedores de servicios de red de terceros implementar un control de políticas de los dispositivos suministrados a través de Cisco APIC.

b) **Perfiles de redes de aplicaciones** (en el fabric), es un conjunto de grupos de terminales (una agrupación lógica de terminales similares que representan un nivel de aplicaciones o un conjunto de servicios que requieren una política semejante), sus conexiones y las políticas que definen dichas conexiones. Se trata de la representación lógica de todos los componentes de la aplicación y sus interdependencias en el fabric de la aplicación.

c) **Fabric de Cisco ACI**: cartera de Cisco Nexus (Switches Cisco Nexus 9000 para Cisco ACI), ofrecen configuraciones de 1, 10 o 40 Gigabit Ethernet fijas y modulares diseñadas para funcionar tanto con Cisco NX-OS, y ofrecer así compatibilidad y coherencia con los switches Cisco Nexus actuales.



Bloques de construcción arquitectónicos de Cisco ACI

6.3.1 CARACTERÍSTICAS DEL CONTROLADOR DE INFRAESTRUCTURA DE POLÍTICAS DE APLICACIONES CISCO

El controlador de infraestructura es el principal componente arquitectónico de la solución Cisco ACI. Es el punto unificado de automatización y administración para el fabric Cisco ACI, la aplicación de políticas y la monitorización de estado. El dispositivo APIC es un controlador centralizado y agrupado que optimiza el rendimiento y unifica el funcionamiento de los entornos físicos y virtuales. El controlador administra y opera un multitenant escalable de Cisco ACI fabric.

El controlador de infraestructura de políticas de aplicaciones de Cisco ofrece las siguientes ventajas:

a) Gestión centralizada basada en políticas:

   i. Integración de redes virtuales y físicas.

   ii. Reducción del tiempo de entrega de servicios.

   iii. Despliegue y configuración automática del tejido con un único punto de gestión.

b) Suministro automatizado de redes y servicios de red:

i. Ampliación a solicitud y eliminación de los servicios de red para una alineación dinámica con las necesidades de las aplicaciones.

ii. La red y los servicios están estrechamente ligados a los despliegues de aplicaciones específicas.

iii. Promoción de políticas y servicios coherentes.

iv. Visibilidad de la red en tiempo real, telemetría y resultados de la salud de las aplicaciones.

v. Control centralizado en tiempo real de las redes físicas, virtuales y sus servicios.

vi. Visibilidad continua del rendimiento de las aplicaciones.

vii. Solución de problemas más rápida e integrada con enfoque centrado en la aplicación.

c) Agilidad en las aplicaciones:

i. Despliegue de la aplicación independiente de la infraestructura subyacente para facilitar despliegue, gestión y migración.

ii. Política de redes centrada en la aplicación para una mayor integración entre la aplicación y Equipos de TI.

d) Seguridad abierta y completa de extremo a extremo:

i. API y estándares abiertos para permitir la flexibilidad del software.

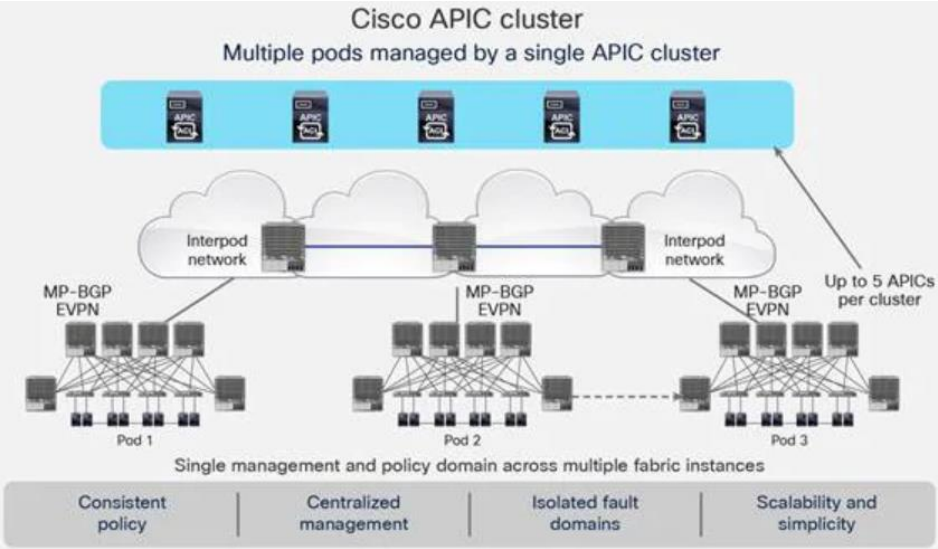
ii. Auditoria de todos los cambios de configuración y soluciones de seguimiento del cumplimiento.

iii. Control de acceso detallado basado en roles (RBAC) y red separación basada en el contexto.

iv. Reglas de reenvío basadas en la lista blanca (sólo las políticas explícitamente establecidas en el perfil de la aplicación permiten el reenvío de los flujos).

6.3.2 CISCO APIC CLÚSTER

El dispositivo APIC se implementa como un clúster. Se configuran un mínimo de tres controladores de infraestructura en un clúster para proporcionar control de escalamiento horizontal de Cisco ACI fabric. El tamaño final del clúster de controladores es directamente proporcional al tamaño de la implementación de Cisco ACI y se basa en los requisitos de velocidad de transacción. Cualquier controlador en el clúster puede atender a cualquier usuario para cualquier operación, y un controlador se puede agregar o eliminar de forma transparente del clúster.



Ejemplo Cisco APIC clúster

6.4 SEGURIDAD CISCO ACI

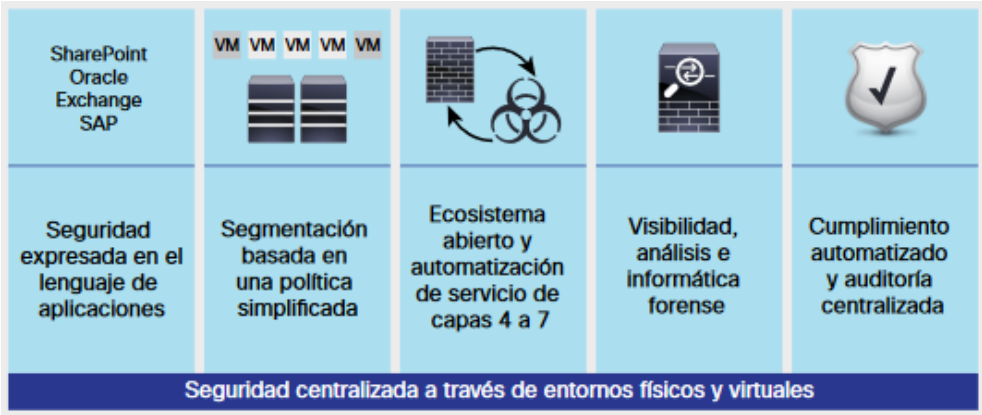
Un escenario como el actual, en el que las organizaciones están migrando sus sistemas a entornos de nube y centros de datos de próxima generación, se requiere la automatización de políticas de seguridad para soportar el aprovisionamiento y la escalabilidad dinámica de las aplicaciones.

Las cargas de trabajo de la aplicación se agregan, modifican y trasladan en un entorno de centro de datos dinámico, por lo que, las políticas de seguridad deben residir en los terminales de la aplicación. La creación y la eliminación de políticas dinámicas son necesarias para asegurar el tráfico transversal y para manejar la movilidad de la aplicación. La visibilidad del tráfico es importante para identificar y mitigar las nuevas amenazas y para asegurar los tenants.

La solución de seguridad Cisco ACI busca hacer uso de un enfoque integral, basado en sistemas, a fin de cubrir las necesidades de seguridad para los entornos Cloud y de centros de datos de próxima generación.

Cisco ACI aborda, de manera exclusiva, las necesidades de seguridad del centro de datos de próxima generación, mediante el uso de un enfoque centrado en aplicaciones y un modelo operativo común basado en políticas, y al mismo tiempo, permite garantizar el cumplimiento y reducir el riesgo de infracciones a la seguridad.

La seguridad Cisco ACI permite una administración unificada del ciclo de vida de la política de seguridad con capacidad para hacer cumplir las políticas en cualquier lugar del centro de datos a través de cargas de trabajo físicas y virtuales. Ofrece automatización completa de las políticas de seguridad de la capa 4 a la 7 y admite una estrategia de defensa profunda con un amplio soporte de ecosistema a la vez que posibilita alta visibilidad, cumplimiento automatizado de políticas y detección y mitigación aceleradas de las amenazas.



6.4.1 FUNCIONES DE SEGURIDAD CISCO ACI

La seguridad de Cisco ACI incluye los siguientes beneficios y funciones principales:

a) Modelo de política centrada en la aplicación: Cisco ACI brinda un nivel más alto de abstracción mediante el uso de grupos terminales (EPG) y contratos, permitiendo definir con mayor facilidad las políticas con un lenguaje de aplicaciones en lugar de una topología de red. El enfoque de política basada en lista blanca de Cisco ACI respalda un modelo de confianza cero, por lo que no permite el tráfico entre los EPG a menos que una política lo permita explícitamente.

b) Administración unificada de política de seguridad de capas 4 a 7: con Cisco ACI, se automatizan y administran de manera centralizada las políticas de seguridad de capas 4 a 7 en el contexto de una aplicación mediante un modelo de política unificado y centrado en la aplicación que funciona a través de los límites físicos y virtuales, así como también en dispositivos de terceros. Así, se logra reducir la complejidad operativa y se aumenta la agilidad de TI sin comprometer la seguridad.

c) Segmentación basada en políticas: con Cisco ACI, se permite una segmentación detallada y flexible de los nodos físicos y virtuales basada en políticas de grupo, lo que reduce el alcance del cumplimiento y mitiga los riesgos de seguridad.

d) Cumplimiento automatizado: Cisco ACI permite garantizar que la configuración de la estructura siempre coincida con la política de seguridad. Las API de Cisco se pueden usar para extraer la política y auditar los registros del Controlador de infraestructura de políticas de la aplicación de Cisco (APIC) y crear informes de cumplimiento. Esta función permite la evaluación de riesgos de TI en tiempo real y reduce el riesgo de que se produzca una falta de cumplimiento en las organizaciones.

e) Seguridad integrada de capa 4 para el tráfico transversal: la estructura de Cisco ACI incluye un firewall independiente de capa 4, distribuido e integrado, para asegurar el tráfico transversal entre los componentes de la aplicación.

f) Marco de seguridad abierto: Cisco ACI ofrece un marco de seguridad abierto (que incluye API y el protocolo de OpFlex) para admitir la incorporación de servicios avanzados para los servicios críticos de seguridad de capas 4 a 7, como sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), además de servicios de firewall de próxima generación en el flujo de la aplicación, independientemente de su ubicación en el centro de datos. Esta función permite una estrategia de seguridad de defensa profunda y la protección de las inversiones.

g) Alta visibilidad y detección acelerada de ataques: Cisco ACI reúne datos de tráfico de red con marca de tiempo y admite contadores atómicos para ofrecer inteligencia de red en tiempo real y alta visibilidad a través de los límites de red física y virtual. Gracias a esta función, se permite una detección de manera acelerada y temprana de los ataques.

h) Respuesta automatizada ante incidentes: Cisco ACI admite la respuesta automatizada ante amenazas identificadas en la red ya que permite la integración con las plataformas de seguridad mediante las API ascendentes.

6.5 PRINCIPALES CAMBIOS VERSIÓN 4

Se presentan los principales cambios de la versión 4.0. detallando ciertos comportamientos conocidos por el fabricante, la compatibilidad con opciones de virtualización y las principales pautas a seguir para la configuración e implementación de la tecnología de una manera eficiente.

6.5.1 COMPORTAMIENTOS CONOCIDOS

Se muestra la siguiente tabla con distintos comportamientos que pueden aparecer dependiendo de su infraestructura desde la versión 4.0 (3).

ID	DESCRIPCIÓN	VERSIONADO
CSCuu17314	CDP no está habilitado en las interfaces de administración para los switches leaf y los switches spine.	4.0 (3c) y posterior
CSCvd43548	Las estadísticas para una regla de cambio de hoja dada no se pueden ver si se hace doble clic en una regla.	4.0 (3c) y posterior
CSCve84297	No se puede llegar a un servicio utilizando la administración fuera de banda APIC que existe dentro de la subred 172.17.0.0/16.	4.0 (3c) y posterior
CSCvf70411	Se anunciará una ruta, pero no contendrá el valor de etiqueta establecido en la política de etiqueta de ruta VRF.	4.0 (3c) y posterior
CSCvg70246	Al configurar un L3Out bajo un “tenant” de usuario que está asociado con una instancia de VRF que está bajo el “tenant” común, una política de temporizador BGP personalizada que se adjunta a la instancia de VRF no se aplica al L3Out (par BGP) en el “tenant” del usuario.	4.0 (3c) y posterior
CSCvh59843	Habilitar la multidifusión bajo el VRF en uno o más dominios puente es difícil debido a cómo está diseñado el menú desplegable. Esta es una solicitud de mejora para hacer que se pueda buscar en el menú desplegable.	4.0 (3c) y posterior

ID	DESCRIPCIÓN	VERSIONADO
CSCvi41092	Los archivos de registro APIC son extremadamente grandes, lo que lleva una cantidad considerable de tiempo para cargar, especialmente para usuarios w	4.0 (3c) y posterior
CSCvi80543	Esta es una mejora que permite ordenar la conmutación por error, categorizar enlaces ascendentes como activos o en espera, y categorizar enlaces ascendentes no utilizados para cada EPG en dominios VMware del APIC.	4.0 (3c) y posterior
CSCvi82903	Cuando se autentica con Cisco APIC usando ISE (TACACS), todos los inicios de sesión de más de 31 caracteres fallan.	4.0 (3c) y posterior
CSCvj89771	El proceso de Virtual Machine Manager (vmmmgr) se bloquea y genera un archivo central.	4.0 (3c) y posterior
CSCvj91789	Cisco APIC M5 usa solo 2 de 4 puertos en una nueva NIC.	4.0 (3c) y posterior
CSCvk04072	No hay registro de quién reconoció una falla en Cisco APIC, ni cuándo ocurrió el reconocimiento.	4.0 (3c) y posterior
CSCvm63668	Un solo usuario puede enviar consultas para sobrecargar la puerta de enlace API.	4.0 (3c) y posterior
CSCvm88517	Se pueden observar problemas con dominios puente, subredes y programación de instancias VRF en la ruta de datos.	4.0 (3c) y posterior
CSCvm89559	El proceso svc_ifc_policye consume el 100% de los ciclos de la CPU. Los siguientes mensajes se observan en svc_ifc_policymgr.bin.log: 8816||18-10-12 11:04:19.101||route_control||ERROR||co=doer:255:127:0xff00000000c42ad2:11||Route entry order exceeded max for st10960-2424833-any-2293761-33141-shared-svc-int Order:18846Max:17801||	4.0 (3c) y posterior
CSCvn00576	Un CSA SHA2 para el certificado HTTPS ACI no se puede configurar en la GUI APIC.	4.0 (3c) y posterior
CSCvn79128	Al actualizar desde algunas versiones 3.2 o 3.1 a 4.0, algunos o todos los grupos de mantenimiento del “leaf switch” comenzarán a actualizarse inmediatamente sin ser activados por el usuario. Este problema ocurre tan pronto como los APIC terminan de actualizarse.	4.0 (3c) y posterior
CSCvo04679	Es posible que las pantallas de exploración de utilización de recursos y medio ambiente no muestren datos para ciertos nodos después de desmantelar un APIC de Cisco.	4.0 (3c) y posterior
CSCvp25660	Después de actualizar los APIC de una versión anterior a la 4.0 a 4.0 o posterior, los modificadores de hoja no se actualizarán, o los modificadores se actualizarán y luego volverán automáticamente a la versión anterior.	4.0 (3c) y posterior

ID	DESCRIPCIÓN	VERSIONADO
CSCvp38627	Algunos “tenants” dejan de recibir actualizaciones de su estado en el APIC. Los registros de ayuda al objetivo tienen mensajes similares al siguiente ejemplo: “An unexpected error has occurred while reconciling tenant tn-prj_...: long int too large to convert to float”	4.0 (3c) y posterior
CSCvp57131	Después de que un VC se desconectó y se volvió a conectar al APIC, se eliminaron los fallos operativos (por ejemplo, la falta de coincidencia de descubrimiento entre APIC y VC), incluso si todavía existía la condición defectuosa.	4.0 (3c) y posterior
CSCvp79454	Syslog no se envía con ningún cambio en la estructura. Los eventos se generan correctamente, pero no se envía Syslog desde los puertos oobmgmt de ninguno de los APIC.	4.0 (3c) y posterior
CSCvp94085	El APIC Licensemgr genera un archivo central mientras analiza una respuesta XML.	4.0 (3c) y posterior
CSCvp95407	Los encabezados de control de acceso no están presentes en las solicitudes no válidas.	4.0 (3c) y posterior
CSCvp97092	Los tenants que comienzan con la palabra "infra" son tratados como el tenant "infra" predeterminado.	4.0 (3c) y posterior
CSCvp99430	El asistente de solución de problemas no responde en el APIC.	4.0 (3c) y posterior
CSCvp99508	La GUI es lenta cuando se accede a las políticas de acceso. Esta es una solicitud de mejora para agregar paginación para resolver este problema.	4.0 (3c) y posterior
CSCvq04110	La API y la CLI de APIC permiten la configuración de varias VLAN nativas en la misma interfaz. Cuando un puerto de switch leaf tiene más de una VLAN nativa configurada (que es una configuración incorrecta) en su lugar, y un usuario intenta configurar un encap de VLAN nativa en otro puerto en el mismo switch leaf, se genera un error de validación que indica un problema con el puerto mal configurado. Este error ocurrirá incluso si el puerto de destino actual no tiene configuraciones incorrectas en su lugar.	4.0 (3c) y posterior
CSCvq14177	El agente de Hyper-V está en estado DETENIDO. Los registros del agente de Hyper-V indican que el proceso se está deteniendo en el comando "Set-ExecutionPolicy Unrestricted".	4.0 (3c) y posterior
CSCvq31358	"show external-l3 interfaces node <id> detail" mostrará "missing" tanto para "Oper Interface" como para "Oper IP", a pesar de que L3Out funciona como se esperaba.	4.0 (3c) y posterior
CSCvq39764	Cuando hace clic en Reiniciar para el agente del Administrador de máquina virtual (SCVMM) de Microsoft System Center en una configuración escalada, el servicio puede detenerse. Puede reiniciar el agente haciendo clic en Inicio.	4.0 (3c) y posterior

ID	DESCRIPCIÓN	VERSIONADO
CSCvq39922	Las combinaciones específicas del sistema operativo y la versión del navegador no se pueden utilizar para iniciar sesión en la GUI APIC. Algunos navegadores que se sabe que tienen este problema incluyen (pero no se limitan a) Google Chrome versión 75.0.3770.90 y Apple Safari versión 12.0.3 (13606.4.5.3.1).	4.0 (3c) y posterior
CSCvq43101	Al abrir una subred externa, un usuario no puede ver las casillas de verificación Exportar / Importar agregadas establecidas en la GUI aunque ya estén configuradas.	4.0 (3c) y posterior
CSCvq45710	El error F3206 para "Error en la configuración de la política uni / infra / nodeauthpol-default, debido a un error de EPg o errorVlan está vacío" aparece en la estructura cuando se usa la política de autenticación de nodo 802.1x predeterminada en el Grupo de políticas de switch. En este escenario, la EPG y la VLAN Fail-auth no se han configurado, ya que la característica 802.1x no está en uso.	4.0 (3c) y posterior
CSCvq58304	Los fallos relacionados con el inventario de VMM se generan para el inventario de VMware vCenter, que VMM no administra.	4.0 (3c) y posterior
CSCvq61877	El proceso SNMP se bloquea repetidamente en los APIC. El clúster y los fragmentos se ven en buen estado y no tienen problemas de uso de CPU o memoria.	4.0 (3c) y posterior
CSCvq63491	Cuando se usa Open vSwitch, que se usa como parte de la integración de ACI con Kubernetes o Red Hat Open Shift, hay algunos casos en que el consumo de memoria de Open vSwitch crece con el tiempo.	4.0 (3c) y posterior
CSCvq74727	Al realizar un cambio de configuración a un L3Out (como la eliminación o adición de un contrato), las aletas pares BGP o el objeto bgpPeerP se eliminan del Switch leaf. En los rastreos de elementos de política de cambio de hoja, 'isClassic = 0, wasClassic = 1' se establece después de la actualización desde el APIC de Cisco.	4.0 (3c) y posterior
CSCvq86573	Bajo un caso de esquina, la base de datos del clúster APIC de Cisco puede divergir parcialmente después de actualizar a una versión que introduce nuevos servicios. Una nueva versión que introduce un nuevo servicio DME (como el domainmgr en la versión 2.3) podría no recibir la actualización del vector de fragmentos de tamaño completo en la primera ventana de dos minutos, lo que hace que el nuevo archivo de bandera de servicio se elimine antes de que todo el líder local los fragmentos pueden iniciarse en el modo de campo verde. Esto da como resultado que la base de datos del clúster APIC de Cisco se desvíe parcialmente.	4.0 (3c) y posterior

ID	DESCRIPCIÓN	VERSIONADO
CSCvr30815	Los objetos vmmPLInf se crean con epgKey y DN que tienen nombres EPG truncados (truncados en ".").	4.0 (3c) y posterior
CSCvr36851	La opción descendente no funcionará para la tabla Puertos estáticos. Incluso cuando el usuario hace clic en descendente, el orden predeterminado es ascendente.	4.0 (3c) y posterior
CSCvr41750	Las políticas pueden tardar mucho tiempo (más de 10 minutos) en programarse en los switches leaf. Además, el APIC extrae inventario de VMware vCenter repetidamente, en lugar de seguir el intervalo habitual de 24 horas.	4.0 (3c) y posterior
CSCvr85515	Al intentar rastrear una dirección IP de punto final AVE, ejecutar el comando "show “endpoint” ip xxxx" en la CLI de Cisco APIC para ver la dirección IP y verificar la dirección IP en el punto final EP en la GUI muestra nombres de VPC incorrectos o múltiples.	4.0 (3c) y posterior
CSCvr92169	El alcance de las rutas de host debe ser configurable; sin embargo, la opción para definir el alcance no está disponible.	4.0 (3c) y posterior
CSCvr98638	Al migrar un dominio AVS VMM a Cisco ACI Virtual Edge, el Cisco ACI Virtual Edge que se implementa se configura en modo VLAN en lugar de modo VXLAN. Debido a esto, se pueden observar fallos para las EPG con el siguiente mensaje de error: "No hay un identificador de encapsulación válido asignado para el epg".	4.0 (3c) y posterior
CSCvs10076	Se genera un error al crear una imagen de contenedor ACI debido a un conflicto con el paquete /opt/ciscoaci-tripleo-heat-templates/tools/build_openstack_aci_containers.py.	4.0 (3c) y posterior
CSCvm32345	No se puede cambiar el nombre de un grupo de puertos. Esta es una solicitud de mejora para habilitar el cambio de nombre de los grupos de puertos.	4.0 (3c) y posterior
CSCvo42420	Después de cambiar la asociación de la instancia VRF de un dominio de puente de servicios compartidos, una ruta de servicios compartidos todavía está presente en la antigua instancia VRF.	4.0 (3c) y posterior
CSCvq38191	Se genera un archivo core eventmgr cuando un usuario ejecuta el comando de depuración syslog "logit".	4.0 (3c) y posterior
CSCuo52668	Cisco APIC no valida las direcciones IP duplicadas que se asignan a dos grupos de dispositivos. La comunicación a los dispositivos o la configuración de los dispositivos de servicio pueden verse afectados.	4.0 (3c) y posterior
CSCuo79243	En algunos de los datos estadísticos de 5 minutos, el recuento de muestras de diez segundos es 29 en lugar de 30.	4.0 (3c) y posterior

ID	DESCRIPCIÓN	VERSIONADO
CSCuo79250	La política de ID de nodo se puede replicar desde un dispositivo antiguo que está fuera de servicio cuando se une a un clúster.	4.0 (3c) y posterior
CSCup47703	El valor DSCP especificado en un grupo de punto final externo no tiene efecto en las reglas de filtro en el “leaf switch”.	4.0 (3c) y posterior
CSCup79002	La resolución del nombre de host del servidor syslog falla en los switches leaf y spine sobre la conectividad en banda.	4.0 (3c) y posterior
CSCuq21360	Después de un FEX o una recarga del interruptor, las etiquetas de interfaz configuradas ya no se configuran correctamente.	4.0 (3c) y posterior
CSCur39124	Los switches se pueden degradar a una versión 1.0 (1) si la configuración importada consiste en una política de firmware con una versión deseada establecida en 1.0 (1).	4.0 (3c) y posterior
CSCur71082	Si el APIC de Cisco se reinicia usando el reinicio de energía CIMC, el sistema entra en fsck debido a un disco dañado.	4.0 (3c) y posterior
CSCus15627	El servicio APIC de Cisco (ApicVMMService) se muestra como detenido en el Administrador de servicios de Microsoft (services.msc en el panel de control> herramientas de administración> servicios). Esto sucede cuando una cuenta de dominio no tiene el privilegio correcto en el dominio para reiniciar el servicio automáticamente.	4.0 (3c) y posterior
CSCut51929	El tráfico destinado a un grupo de puntos finales del proveedor de servicios compartidos elige una ID de clase incorrecta (PcTag) y se descarta.	4.0 (3c) y posterior
CSCuu09236	El tráfico de una red externa de Capa 3 se permite cuando se configura como parte de un consumidor vzAny (una colección de grupos de puntos finales dentro de un contexto).	4.0 (3c) y posterior
CSCuu61998	Las configuraciones de EPG de microsegmento recién agregadas deben eliminarse antes de pasar a una versión de software que no lo admite.	4.0 (3c) y posterior
CSCuu64219	La degradación de la estructura que comienza con el switch leaf provocará fallas como el fallo de implementación de política con el código de falla F1371.	4.0 (3c) y posterior
CSCva32534	Crear o eliminar una política fabricSetupP da como resultado un estado inconsistente.	4.0 (3c) y posterior

ID	DESCRIPCIÓN	VERSIONADO
CSCva60439	Después de que se crea un pod y se agregan nodos en el pod, al eliminar el pod se obtienen entradas obsoletas del pod que están activas en la estructura. Esto ocurre porque Cisco APIC utiliza DHCP de código abierto, lo que crea algunos recursos que Cisco APIC no puede eliminar cuando se elimina un pod.	4.0 (3c) y posterior
CSCva86794	Cuando se está actualizando un clúster de Cisco APIC, el clúster de Cisco APIC puede entrar en el estado minoritario si hay problemas de conectividad. En este caso, los inicios de sesión de los usuarios pueden fallar hasta que la mayoría de los APIC de Cisco finalicen la actualización y el clúster salga de la minoría.	4.0 (3c) y posterior
CSCva97082	Al bajar a una versión 2.0 (1), los “spines” y sus interfaces deben moverse de infra L3out2 a infra L3out1. Después de que aparezca Infra L3out1, elimine L3out2 y su configuración relacionada, y luego baje a una versión 2.0 (1).	4.0 (3c) y posterior
CSCvb39702	No se genera ninguna falla al usar la misma VLAN de encapsulación en un dispositivo de copia en tenant común, a pesar de que se debe generar una falla.	4.0 (3c) y posterior
CSCvg41711	En el modo hoja, el comando "template route group <group-name> tenant <tenant-name>" falla, declarando que el tenant pasado no es válido.	4.0 (3c) y posterior
CSCvg79127	Cuando la seguridad del primer salto está habilitada en un dominio de puente, el tráfico se interrumpe.	4.0 (3c) y posterior
CSCvg81856	Los pares BGP de Cisco ACI Multi-Site Orchestrator están inactivos y se genera un error por un rtrId en conflicto en el objeto administrado fvRtdEpP durante la configuración de L3extOut.	4.0 (3c) y posterior
CSCvh76076	Es posible que los detalles de la PSU SPROM no se muestren en la CLI tras la extracción e inserción del switch.	4.0 (3c) y posterior
CSCvh93612	Si se programan dos reglas de rechazo intra-EPG, una con la prioridad class-eq-deny y otra con la prioridad class-eq-filter, cambiar la acción de la segunda regla para "denegar" hace que la segunda regla sea redundante y tenga sin efecto. El tráfico todavía se niega, como se esperaba.	4.0 (3c) y posterior
CSCvj26666	El comando "show run leaf | spine <nodeId>" puede producir un error para configuraciones ampliadas.	4.0 (3c) y posterior
CSCvm71833	Las actualizaciones del switch fallan con el siguiente error: Versión no compatible.	4.0 (3c) y posterior

6.5.2 COMPATIBILIDAD DE VIRTUALIZACIÓN

En esta sección se enumerará la información de compatibilidad de virtualización para el software APIC de Cisco. Desde esta versión se admiten las siguientes tecnologías o funcionalidades:

a) Esta versión es compatible con VMM Integration y VMware Distributed Virtual Switch (DVS) 6.5.x.

Nota: Para obtener más información sobre las pautas para actualizar VMware DVS de 5.xa 6.x y la integración de VMM, consulte la Guía de virtualización de Cisco ACI, versión 4.0 (3) en la siguiente URL: https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

b) Esta versión admite las versiones acumulativas de actualizaciones 9, 10 y 11 de Microsoft System Center Virtual Machine Manager (SCVMM) 2012 y las actualizaciones acumulativas de actualizaciones 9, 10 y 11 de Microsoft Windows Azure Pack.

c) Esta versión es compatible con las versiones acumulativas de actualizaciones 1, 2, 2.1 y 3 de Microsoft SCVMM para SCVMM 2016 y Microsoft Hyper-V 2016.

d) Si usa Microsoft vSwitch y desea degradar a Cisco APIC versión 2.3 (1) de una versión posterior, primero debe eliminar cualquier EPG de microsegmento configurado con el filtro Match All.

e) Esta versión es compatible con el paquete de dispositivo de dispositivo de seguridad adaptable (ASA) versión 1.2.5.5 o posterior. Si está ejecutando una versión del dispositivo virtual de seguridad adaptable de Cisco (ASA) anterior a la versión 9.3 (2), debe configurar el cifrado SSL como “aes128-sha1”.

Se muestra a continuación la tabla comparativa que muestra desde la versión 3.0(1) las tecnologías virtuales que son compatibles y en qué versión. Las versiones que se encuentren con un aspa en la fila de esa tecnología, representa la incompatibilidad de la misma.

Producto de virtualización / lanzamiento de ACI	3.0(1)	3.0 (2)	3.1 (1)	3.1 (2)	3.2 (1)	3.2 (2)	3.2 (3)	3.2 (4) al 3.2 (6)	3.2 (7) al 3.2 (9)	4.0 (1)	4.0 (2) - 4.0 (3)	4.1 (1) - 4.1 (2)	4.2 (1) al 4.2 (3)
VMware vSphere 5.1													
VMware vSphere 5.5													
VMware vSphere 6.0													
VMware vSphere 6.5													
VMware vSphere 6.7	X	X	X	X	X								
VMware vRealize													
VMware vRealize 7.0													
VMware vRealize 7.1													
VMware vRealize 7.2													
VMware vRealize 7.3													
VMware vRealize 7.4	X	X	X	X	X								

Producto de virtualización / lanzamiento de ACI	3.0(1)	3.0 (2)	3.1 (1)	3.1 (2)	3.2 (1)	3.2 (2)	3.2 (3)	3.2 (4) al 3.2 (6)	3.2 (7) al 3.2 (9)	4.0 (1)	4.0 (2) - 4.0 (3)	4.1 (1) - 4.1 (2)	4.2 (1) al 4.2 (3)
VMware vRealize 7.5	X	X	X	X	X								
VMware vRealize 7.6	X	X	X	X	X	X	X	X	X	X	X	X	
VMware vSphere Web Client 5.5 o superior													
Cisco AVS 5.2 (1) SUV3 (2.1) y (2.1a)													
Cisco AVS 5.2 (1) SUV3 (2.2) y (2.2a)													
Cisco AVS 5.2 (1) SUV3 (2.5)													
Cisco AVS 5.2 (1) SUV3 (2.6) y (2.6a)													
Cisco AVS 5.2 (1) SUV3 (2.7)													
Cisco AVS 5.2 (1) SUV3 (2.14)													
Cisco AVS 5.2 (1) SUV3 (3.2)													
Cisco AVS 5.2 (1) SUV3 (3.3)													
Cisco AVS 5.2 (1) SUV3 (3.4) y (3.4a)													
Cisco AVS 5.2 (1) SUV3 (3.5) y (3.5a)													
Cisco AVS 5.2 (1) SUV3 (3.10)													
Cisco AVS 5.2 (1) SUV3 (3.11)	X												
Cisco AVS 5.2 (1) SUV3 (3.20)	X	X											
Cisco AVS 5.2 (1) SUV3 (3.21)	X	X	X										
Cisco AVS 5.2 (1) SUV3 (3.25)	X	X	X	X									
Cisco AVS 5.2 (1) SUV3 (3.27)	X	X	X	X	X								
Cisco AVS 5.2 (1) SUV3 (3.28)	X	X	X	X	X	X							
Cisco AVS 5.2 (1) SUV3 (3.29)	X	X	X	X	X	X	X						
Cisco AVS 5.2 (1) SUV3 (3.35)	X	X	X	X	X	X	X	X	X				

Producto de virtualización / lanzamiento de ACI	3.0(1)	3.0 (2)	3.1 (1)	3.1 (2)	3.2 (1)	3.2 (2)	3.2 (3)	3.2 (4) al 3.2 (6)	3.2 (7) al 3.2 (9)	4.0 (1)	4.0 (2) - 4.0 (3)	4.1 (1) - 4.1 (2)	4.2 (1) al 4.2 (3)
Cisco AVS 5.2 (1) SUV3 (3.40)	X	X	X	X	X	X	X	X	X	X			
Cisco AVS 5.2 (1) SUV3 (3.50)	X	X	X	X	X	X	X	X	X	X	X		
Cisco AVS 5.2 (1) SUV3 (3.80)	X	X	X	X	X	X	X	X	X	X	X		
Cisco AVS 5.2 (1) SUV3 (4.11)	X	X	X	X	X	X	X	X	X	X	X	X	
Cisco ACI Virtual Edge 1.1 (1a)	X	X											
Cisco ACI Virtual Edge 1.1 (1b)	X	X											
Cisco ACI Virtual Edge 1.1 (2a)	X	X	X										
Cisco ACI Virtual Edge 1.2 (1a)	X	X	X	X									
Cisco ACI Virtual Edge 1.2 (2a)	X	X	X	X	X								
Cisco ACI Virtual Edge 1.2 (3a)	X	X	X	X	X	X							
Cisco ACI Virtual Edge 1.2 (3b)	X	X	X	X	X	X							
Cisco ACI Virtual Edge 1.2 (4a)	X	X	X	X	X	X	X						
Cisco ACI Virtual Edge 2.0 (1a)	X	X	X	X	X	X	X	X	X				
Cisco ACI Virtual Edge 2.0 (2a)	X	X	X	X	X	X	X	X	X	X			
Cisco ACI Virtual Edge 2.1 (1a)	X	X	X	X	X	X	X	X	X	X	X		
Cisco ACI Virtual Edge 2.2 (2a)	X	X	X	X	X	X	X	X	X	X	X	X	
Cisco ACI Virtual Edge 2.2 (3a)	X	X	X	X	X	X	X	X	X	X	X	X	
SCVMM 2012 y WAP 2.0 Plugin													
SCVMM y WAP Update Rollup 11													
SCVMM 2019	X	X	X	X	X	X	X	X	X	X	X	X	
Red Hat Virtualization 4.1.6 o posterior	X	X											
Red Hat OSP 7	X	X	X	X	X	X	X	X	X	X	X	X	X

Producto de virtualización / lanzamiento de ACI	3.0(1)	3.0 (2)	3.1 (1)	3.1 (2)	3.2 (1)	3.2 (2)	3.2 (3)	3.2 (4) al 3.2 (6)	3.2 (7) al 3.2 (9)	4.0 (1)	4.0 (2) - 4.0 (3)	4.1 (1) - 4.1 (2)	4.2 (1) al 4.2 (3)
Red Hat OSP 8	X	X	X	X	X	X	X	X	X	X	X	X	X
Red Hat OSP 9		X	X	X	X	X	X	X	X	X	X	X	X
Red Hat OSP 10													
Red Hat OSP 11													
Red Hat OSP 12	X	X	X	X									
Red Hat OSP 13	X	X	X	X	X	X	X						
Canonical Kilo	X	X	X	X	X	X	X	X	X	X	X	X	X
Canonical Liberty	X	X	X	X	X	X	X	X	X	X	X	X	X
Canonical Mitaka		X	X	X	X	X	X	X	X	X	X	X	X
Canonical Newton													
Canonical Ocata													
Canonical Pike	X	X	X	X									
Canonical Queens	X	X	X	X	X								
OpenShift 3.6	X	X			X	X	X	X	X	X	X	X	X
OpenShift 3.9	X	X	X	X	X								
OpenShift 3.10	X	X	X	X	X					X	X		
OpenShift 3.11	X	X	X	X	X					X	X		
Kubernetes Upstream 1.6				X	X	X	X	X	X	X	X	X	X
Kubernetes Upstream 1.7	X	X			X	X	X	X	X	X	X	X	X
Kubernetes Upstream 1.9	X	X	X	X				X	X	X	X	X	X
Kubernetes Upstream 1.10	X	X	X	X							X	X	X
Kubernetes Upstream 1.11	X	X	X	X	X							X	X
Kubernetes Upstream 1.12	X	X	X	X	X								X
Kubernetes Upstream 1.13	X	X	X	X	X					X	X		
Kubernetes Upstream 1.14	X	X	X	X	X	X	X	X	X	X	X	X	
Kubernetes Upstream 1.15	X	X	X	X	X	X	X	X	X	X	X	X	
Kubernetes Upstream 1.16	X	X	X	X	X	X	X	X	X	X	X	X	

Producto de virtualización / lanzamiento de ACI	3.0(1)	3.0 (2)	3.1 (1)	3.1 (2)	3.2 (1)	3.2 (2)	3.2 (3)	3.2 (4) al 3.2 (6)	3.2 (7) al 3.2 (9)	4.0 (1)	4.0 (2) - 4.0 (3)	4.1 (1) - 4.1 (2)	4.2 (1) al 4.2 (3)
Docker Enterprise 2.1 (UCP 3.1)	X	X	X	X	X	X	X	X	X	X	X	X	
Docker Enterprise 3.0 (UCP 3.2)	X	X	X	X	X	X	X	X	X	X	X	X	
LACP mejorado (eLACP)	X	X	X	X	X	X	X	X					

Tabla de compatibilidades 1

Nota: Todas las actualizaciones de VMware vSphere son compatibles a menos que se mencione explícitamente. La alta disponibilidad (HA) con múltiples vRO no es compatible en todas las versiones. Además, El complemento Cisco ACI CNI es compatible con las siguientes soluciones de contenedor:

- Kubernetes canónicos en Ubuntu 18.04
- Red Hat Openshift en RHEL 7
- Docker Enterprise en RHEL 7

6.5.3 PAUTAS DE VIRTUALIZACIÓN, CONFIGURACIÓN Y USO

Se enumeran a continuación, algunas pautas, configuraciones a tener en cuenta y uso, del software APIC de Cisco, asociadas a distintos escenarios:

6.5.3.1 VIRTUALIZACIÓN PARA EL SOFTWARE APIC DE CISCO

Se enumeran a continuación, las pautas de uso relacionadas con la virtualización para el software APIC de Cisco:

a) No se deberán separar los nodos miembros del canal de puerto virtual (vPC) en diferentes zonas de configuración. Si los nodos están en diferentes zonas de configuración, los modos de los vPC no coinciden si las políticas de la interfaz se modifican y se implementan solo en uno de los nodos miembros de vPC.

b) Si está actualizando VMware vCenter 6.0 a vCenter 6.7, primero se debe eliminar la siguiente carpeta en VMware vCenter: C:\ProgramData\cisco_aci_plugin. Si no se elimina la carpeta y se intenta registrar una estructura nuevamente después de la actualización, se mostrará el siguiente mensaje de error:

Error al guardar la configuración en "C:\ProgramData\cisco_aci_plugin\<usuario>_<dominio>".

c) Cuando el usuario, es el usuario que actualmente ha iniciado sesión en vSphere Web Client, y el dominio, es el dominio al que pertenece el usuario, se puede registrar una estructura, no obstante, no tiene permisos para anular la configuración que se creó en el antiguo VMware vCenter. Para cualquier cambio en la configuración de Cisco APIC se deberá reiniciar VMware vCenter e intentarlo nuevamente después.

d) Si la comunicación entre Cisco APIC y VMware vCenter se ve afectada, algunas funciones pueden dejar de funcionar. Cisco APIC se basa en extraer información de inventario, actualizar la configuración de VDS y recibir notificaciones de eventos de VMware vCenter para realizar ciertas operaciones.

e) Después de migrar máquinas virtuales utilizando un centro de datos cruzados VMware vMotion en el mismo VMware vCenter, es posible que encuentre una entrada de máquina virtual obsoleta en el DVS de origen. Esta entrada obsoleta puede causar problemas, como un fallo en la eliminación del host. La solución para este problema es habilitar "Start monitoring port state“ en el vNetwork DVS. Consulte el tema "Actualización de la información del estado del puerto para un switch virtual distribuido vNetwork" en el sitio web de VMware para obtener instrucciones.

f) Al crear un dominio vPC entre dos “leaf switches”, ambos switches deben de ser de la misma generación de switches. Los switches que no son de la misma generación no son pares vPC compatibles. Las generaciones son las siguientes:

   i. Generación 1: switches de plataforma Cisco Nexus 9200 y 9300 (sin "EX" al final del nombre del switch); por ejemplo, Cisco Nexus 93120TX.

   ii. Generación 2: switches de plataforma Cisco Nexus 9300-EX y FX; por ejemplo, Cisco Nexus 93108TC-EX.

g) Se aplican las siguientes pautas de Red Hat Virtualization (RHV):

   i. Se recomienda la utilización de la versión 4.1.6 o posterior.

   ii. Solo un controlador (compCtrlr) puede asociarse con un centro de datos de Red Hat Virtualization Manager (RHVM).

   iii. La inmediatez de implementación solo se admite como pre-aprovisionamiento.

   iv. El aislamiento de IntraEPG, las micro EPG y los contratos de IntraEPG no son compatibles.

   v. El uso de nodos de servicio dentro de un dominio RHV no ha sido validado.

6.5.3.2 GUI Y EL CLI PARA EL SOFTWARE APIC DE CISCO

Por otra parte, las pautas de uso relacionadas con la GUI y el CLI para el software APIC de Cisco serían las siguientes:

a) El icono en el APIC de Cisco abre el menú para los módulos “**Show Me How**“, que proporcionan ayuda paso a paso a través de configuraciones específicas.

   i. Si se cambia de ruta mientras está en progreso un módulo Show Me How, ya no podrá continuar.

   ii. Debe tener IPv4 habilitado para usar los módulos Show Me How.

b) La GUI de Cisco APIC incluye una versión en línea de la Guía de inicio rápido que incluye demostraciones en video.

c) Para llegar a la CLI APIC de Cisco desde la GUI: elija Sistema> Controladores, resalte un controlador, haga clic con el botón derecho y elija "iniciar SSH". Para obtener la lista de comandos, presione la tecla de escape dos veces.

d) El modo GUI básico está en desuso. No se recomienda utilizar el modo básico APIC de Cisco para la configuración. Sin embargo, si se desea usar el modo básico APIC de Cisco, se puede usar ingresando en la siguiente URL: “APIC_URL /indexSimple.html”.

e) Los comandos “show” ejecutados en la CLI de estilo NX-OS está sujeta a cambios en futuras versiones de software. No se recomienda la utilización de los comandos “show” para la automatización.

f) La CLI solo es compatible con usuarios con privilegios de inicio de sesión administrativo.

g) Si FIPS está habilitado en las configuraciones de Cisco ACI, entonces el soporte SHA256 es obligatorio en el Cliente SSH. Además, para tener compatibilidad con SHA256, el cliente OpenSSH debe ejecutar la versión 6.6.1 o superior.

6.5.3.3 CAPA 2 Y CAPA 3 SEGÚN MODELO OSI

En cuanto a la configuración de la capa 2 y capa 3 según modelo OSI, se enumeran a continuación las principales pautas a seguir para el software Cisco APIC:

a) Para las redes externas de Capa 3 creadas a través de la API o GUI y actualizadas a través de la CLI, los protocolos deben habilitarse globalmente en la red externa a través de la API o GUI, y el perfil de nodo para todos los nodos participantes debe agregarse a través de la API o GUI antes de hacer más actualizaciones a través de la CLI.

b) Al configurar dos redes externas de Capa 3 en el mismo nodo, los bucles deben configurarse por separado para ambas redes de Capa 3.

c) Todos los grupos de punto final (EPG), incluidas las EPG de aplicación y las EPG externas de capa 3 requieren un dominio. Los grupos de políticas de interfaz también deben estar asociados con un perfil de entidad adjunta (AEP) y el AEP debe estar asociado con dominios. En función de la asociación de EPG a dominios y de los grupos de políticas de interfaz a dominios, se validan las VLAN de puertos que utiliza EPG. Esto se aplica a todas las EPG, incluidas las capas 2 externas en puente y las capas 3 enrutadas fuera de las EPG. Para obtener más información, consulte la siguiente URL:

   https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/L2_config/b_Cisco_APIC_Layer_2_Configuration_Guide.html.

Nota: Al crear rutas estáticas para aplicaciones EPG o Capa 2 / Capa 3 fuera de EPG, no se requiere el dominio físico. La actualización sin el dominio físico genera un error en la EPG que indica "configuración de ruta no válida".

d) No se necesita crear una política de supervisión personalizada para cada “tenant”. Por defecto, un “tenant” comparte la política común bajo “tenant” común. Cisco APIC crea automáticamente una política de monitorización predeterminada y común. Puede modificar la política predeterminada en “tenant” común según los requisitos de su estructura.

e) Cisco APIC no proporciona servicios de IPAM para cargas de trabajo de “tenants”.

f) Debe configurar correctamente las entradas del filtro de Control Plane Policing (CoPP). Las entradas del filtro de CoPP pueden afectar la conectividad a configuraciones de múltiples pods, “leaf switches” remotos e implementaciones de Cisco ACI Multi-Site.

g) No puede usar “leaf switches” remotos con Cisco ACI Multi-Site.

6.5.3.4 DIRECCIONES IP

Para el uso relacionado con las direcciones IP, se enumeran a continuación las principales pautas a seguir para el software Cisco APIC:

a) Para los siguientes servicios, se deberá usar un nombre de host basado en DNS con conectividad de administración fuera de banda. Las direcciones IP se pueden usar con conectividad de administración dentro y fuera de banda.
   i. Servidor Syslog
   ii. Llame al servidor SMTP de inicio
   iii. Servidor de exportación de soporte técnico
   iv. Servidor de exportación de configuración
   v. Servidor de exportación de estadísticas

b) El rango de la dirección IP de la infraestructura no debe solaparse con otras direcciones IP utilizadas en la estructura para redes dentro y fuera de banda.

c) Si se configura una dirección IP en uno de los dos “endpoint’s” para los que está configurando una política, debe usar una política basada en IP y no una política basada en “endpoint”.

d) Una implementación “multi-pod” requiere que el sistema Global IP Outside (GIPo) se encuentre configurado con la ip 239.255.255.240 en la red pod (IPN) como un rango PIM BIDIR. Esta configuración de rango 239.255.255.240 PIM BIDIR en los dispositivos IPN se puede evitar mediante el uso de Infra GIPo como característica del sistema GIPo. La función Infra GIPo como sistema GIPo debe habilitarse solo después de actualizar todos los switches en la estructura Cisco ACI, incluidos los “leaf switches” y los “spine switches” a la última versión de Cisco APIC.

e) Cisco ACI no admite una dirección de clase E como una dirección VTEP.

6.5.3.5 PAUTAS GENERALES RECOMENDADAS PARA EL SOFTWARE CISCO APIC

Finalmente se enumeran las pautas generales recomendadas para el software Cisco APIC:

a) Las contraseñas ser deben cumplir con los siguientes criterios:
   i. La longitud mínima es de 8 caracteres.
   ii. La longitud máxima es de 64 caracteres.
   iii. Menos de tres caracteres repetidos consecutivos.
   iv. Al menos tres de los siguientes tipos de caracteres: minúsculas, mayúsculas, dígitos, símbolos.
   v. No se debe usar una contraseña que se pueda adivinar fácilmente.
   vi. No puede ser el nombre de usuario o el reverso del nombre de usuario
   vii. No debe usarse para la contraseña ninguna variación de "cisco", "isco", ni ninguna permutación de estos caracteres o variantes obtenida cambiando la mayúscula de las letras.

b) Si definió varios dominios de inicio de sesión, se puede elegir el dominio de inicio de sesión que desea utilizar al iniciar sesión en un APIC de Cisco. De manera predeterminada, la lista desplegable de dominios está vacía, y si no elige un dominio, el dominio "DefaultAuth" se usa para la autenticación. Esto puede provocar un error de inicio de sesión si el nombre de usuario no está en el dominio de inicio de sesión "DefaultAuth". Como tal, debe ingresar las credenciales basadas en el dominio de inicio de sesión elegido.

c) Un grupo de mantenimiento de firmware debe contener un máximo de 80 nodos.

d) Cuando los contratos no están asociados con un grupo de "endpoint", el DSCP no es compatible con un VRF con un "vzAny". DSCP se envía a un "leaf switch" junto con la regla "actrl", pero un "vzAny" no tiene una regla actrl. Por lo tanto, el valor DSCP no se puede enviar.

e) Los APIC de Cisco deben tener 1 SSD y 2 HDD, y ambos volúmenes RAID deben estar en buen estado antes de actualizar a la última versión. Cisco APIC podría no iniciarse si la SSD no está instalada.

f) En una configuración "multi-pod", si se agrega un nuevo "spine switch" a un pod, primero debe conectarse al menos a un "leaf switch" en el pod. Entonces el "spine switch" realizará un descubrimiento para la unión.

Nota: Si se instalan enlaces de 1 Gigabit Ethernet (GE) o 10GE entre los "leaf switch" y los "spine switch", existe el riesgo de que se pierdan paquetes en lugar de reenviarse debido a un ancho de banda inadecuado. Para evitar el riesgo, use enlaces 40GE o 100GE entre los "leaf switch" y los "spine switch".

g) Para una consulta de API APT REST de Cisco de registros de eventos, el sistema APIC de Cisco limita la respuesta a un máximo de 500,000 registros de eventos. Si la respuesta es más de 500,000 eventos, devuelve un error. Por tanto, se recomienda usar filtros para acotar las consultas.

h) Los nombres alternativos del sujeto (SAN) contienen uno o más nombres alternativos y utilizan cualquier variedad de formularios de nombres para la entidad vinculada por la Autoridad de certificación (CA) a la clave pública certificada. Estos nombres alternativos se denominan "Nombres alternativos de sujeto" (SAN). Los posibles nombres incluyen:

   i. Nombre DNS

   ii. Dirección IP

i) Si un nodo tiene perfiles de puerto implementados, algunas configuraciones de puerto no se eliminan si retira el nodo. Debe eliminar manualmente las configuraciones después de desmantelar el nodo para que los puertos vuelvan al estado predeterminado. Para hacer esto, inicie sesión en el switch, ejecute el script "setup-clean-config.sh", espere a que se complete el script, luego ingrese el comando reload.

j) Al utilizar la función de agregación de capturas SNMP, si retira los APIC de Cisco, el servidor de reenvío de capturas recibirá capturas redundantes.

k) Si no realiza la configuración "over-provisioning" del SSD en los "spine switches" Cisco N9K-C9364C y N9K-C9336C-FX2, Cisco APIC genera el fallo F2972. la configuración "over-provisioning" del SSD se aplica automáticamente durante el proceso de arranque del switch después de responder al fallo. la configuración "over-provisioning" del SSD puede tardar hasta una hora por spine switch en completarse. Después de que el switch se vuelve a cargar, no es necesario que realice ninguna otra acción para solventar el fallo.

l) Si se actualizó desde una versión anterior a la versión 3.2 (1) de Cisco APIC y éste poseía alguna aplicación instalada antes de la actualización, las aplicaciones ya no funcionarán. Para usar las aplicaciones nuevamente, debe desinstalarlas y reinstalarlas.

m) Los filtros de conectividad quedaron en desuso en la versión 3.2 (4). La degradación de la función implica que no se han realizado más pruebas y que Cisco recomienda eliminar todas y cada una de las configuraciones que utilizan esta función. El uso de filtros de conectividad puede dar como resultado una resolución inesperada de la política de acceso, que en algunos casos llevará a que las VLAN se eliminen / reprogramen en las interfaces de los "leaf switch". Puede buscar la existencia de filtros de conectividad utilizando los siguientes comandos en el APIC:

   i. > moquery -c infraConnPortBlk
   ii. > moquery -c infraConnNodeBlk
   iii. > moquery -c infraConnNodeS
   iv. > moquery -c infraConnFexBlk
   v. > moquery -c infraConnFexS

n) Los puertos de conectividad de estructura pueden funcionar a velocidades de 10G o 25G (según el modelo del servidor APIC) cuando se conectan a las interfaces de host del "leaf switch". Se recomienda conectar dos "uplinks" por cada "leaf switch" separado o por cada par de "leaf switches" vPC.

o) Para APIC-M3 / L3, la tarjeta de interfaz virtual (VIC) 1445 tiene cuatro puertos (puerto-1, puerto-2, puerto-3 y puerto-4 de izquierda a derecha). El puerto 1 y el puerto 2 forman un solo par correspondiente a eth2-1 en el servidor APIC; port-3 y port-4 forman otro par correspondiente a eth2-2 en el servidor APIC. Solo se permite una única conexión para cada par. Por ejemplo, puede conectar un cable al puerto 1 o al puerto 2 y otro cable al puerto 3 o al puerto 4, pero no 2 cables a ambos puertos en el mismo par. Conectar 2 cables a ambos puertos en el mismo par crea inestabilidad en el servidor APIC. Todos los puertos deben configurarse para la misma velocidad: 10G o 25G.

p) Cuando crea un selector de puerto de acceso en un archivo de "leaf switch", la propiedad "fexId" se configura con un valor predeterminado de 101 a pesar de que un "FEX" no está conectado y la interfaz no es una interfaz "FEX". La propiedad "fexId" solo se usa cuando el selector de puerto está asociado con un objeto administrativo "infraFexBndlGrp".

7. CONFIGURACIÓN DE UNA INFRAESTRUCTURA SEGURA CISCO ACI

En este apartado se van a dar directrices de configuración para la aplicación, así como, configuraciones de seguridad comenzando desde la instalación.

7.1 CONFIGURACIÓN DE ROLES Y PERMISOS DE ACCESO

El APIC proporciona acceso de acuerdo con el rol del usuario a través del control de acceso basado en roles (RBAC). Cada usuario tiene asociadas las siguientes características:

a) Un conjunto de roles

b) Para cada rol, un tipo de privilegio: sin acceso, solo lectura o lectura-escritura

c) Una o más etiquetas de dominio de seguridad que identifican las partes del árbol de información de administración (MIT) a las que puede acceder un usuario

La estructura ACI gestiona los privilegios de acceso en el nivel de objeto gestionado (MO). Un privilegio es un MO que habilita o restringe el acceso a una función particular dentro del sistema.

Un rol es una colección de bits de privilegio. Por ejemplo, debido a que un rol de "administrador" está configurado con privilegios para "estructura de fabric" y "seguridad de tenant", el rol de "administrador" tiene acceso a todos los objetos que contienen a los mismos.

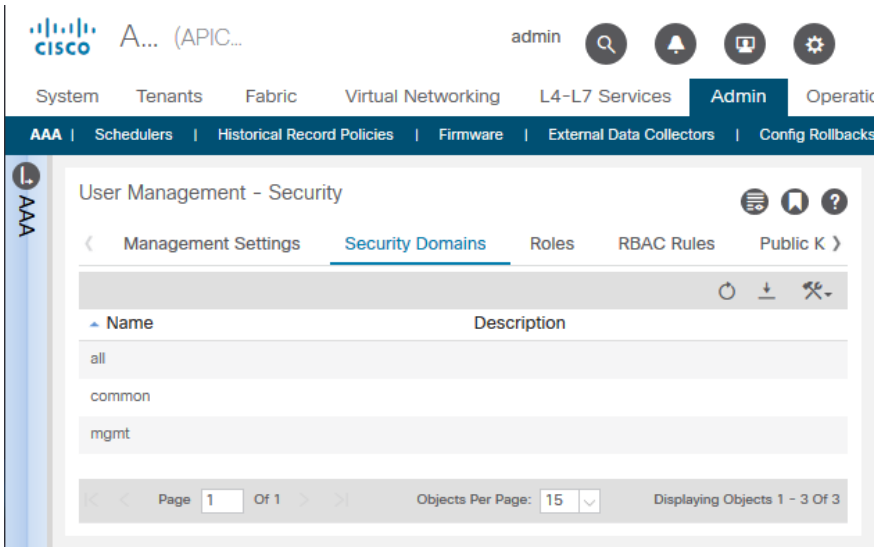
Un dominio de seguridad es una etiqueta asociada con un determinado subárbol en la jerarquía de objetos ACI MIT. Por ejemplo, el tenant predeterminado "common" tiene una etiqueta de dominio “common”. Del mismo modo, la etiqueta de dominio especial “all” incluye todo el árbol de objetos MIT. Un administrador puede asignar etiquetas de dominio personalizadas a la jerarquía de objetos MIT. Por ejemplo, un administrador podría asignar la etiqueta de dominio "dominio1" al tenant llamado dominio1. Dentro del MIT, solo ciertos objetos se pueden etiquetar como dominios de seguridad. Por ejemplo, un tenant se puede etiquetar como un dominio de seguridad, pero los objetos dentro de él no.

Crear un usuario y asignarle un rol a ese usuario no habilita los derechos de acceso. Es necesario asignar también al usuario a uno o más dominios de seguridad. Por defecto, ACI fabric incluye dos dominios pre-creados especiales:

a) ALL: permite el acceso a todo el MIT

b) Infra: permite el acceso a objetos/subárboles de infraestructura de fabric, como las políticas de acceso.

Los dominios de seguridad por defecto en el apartado de Administración AAA serían “all”, “common” y “mgmt”.



Se puede asociar un conjunto de clases de objetos gestionados predefinidos con dominios. Estas clases no deben tener una contención superpuesta. Los ejemplos de clases que admiten la asociación de dominio son los siguientes:

a) Objetos gestionados en red de capa 2 y capa 3

b) Perfiles de red (como físico, capa 2, capa 3, gestión)

c) Políticas de QoS

Cuando se crea un objeto que puede asociarse con un dominio, el usuario debe asignar dominio(s) al objeto dentro de los derechos de acceso del usuario. La asignación de dominio se puede modificar en cualquier momento.

Si un dominio de administración de máquina virtual (VMM) se etiqueta como un dominio de seguridad, los usuarios contenidos en el dominio de seguridad pueden acceder al dominio VMM etiquetado correspondientemente. Por ejemplo, si un tenant llamado “tenant01” está etiquetado con el dominio de seguridad llamado “dominio1” y un dominio VMM también está etiquetado con el dominio de seguridad llamado “dominio1”, entonces los usuarios del tenant “tenant01” pueden acceder al dominio VMM de acuerdo con sus derechos de acceso.

A partir de la versión 4.2 (4), puede impedir que un usuario pueda iniciar sesión después de que el usuario falle un número configurado de intentos de inicio de sesión. Puede especificar cuántos intentos fallidos de inicio de sesión puede tener el usuario dentro de un período de tiempo específico. Si el usuario no puede iniciar sesión demasiadas veces, entonces ese usuario no podrá iniciar sesión durante un período de tiempo específico.

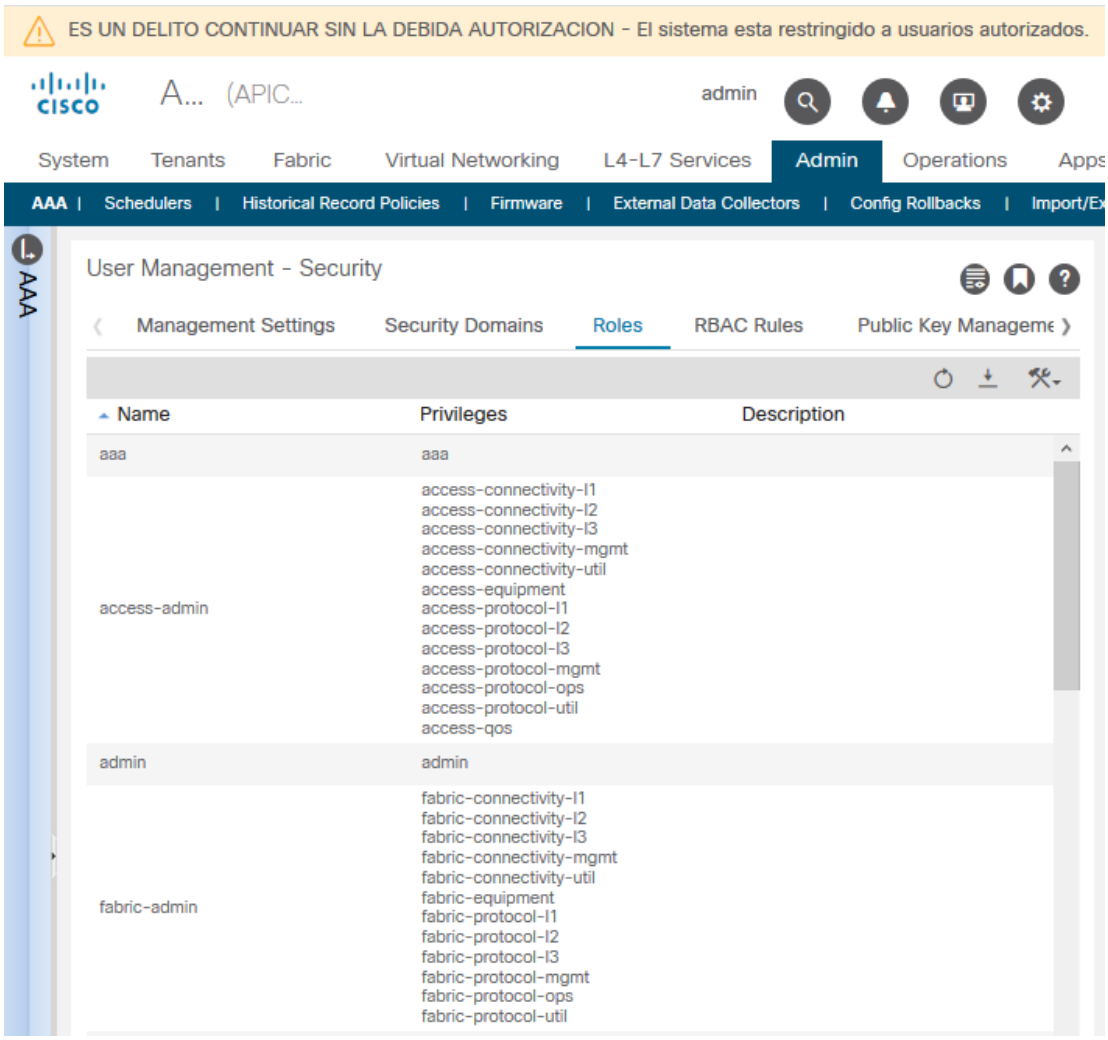
Esta característica cuenta los intentos fallidos de inicio de sesión tanto para usuarios locales que se encuentran en la base de datos de la Infraestructura céntrica de aplicaciones de Cisco (ACI) como para usuarios remotos que se autentican con servidores de autenticación externos, como RADIUS, LDAP, TACACS +, DUO Proxy, SAML o RSA. Un usuario remoto que está bloqueado debido a fallos consecutivas de autenticación usando un tipo de servidor de autenticación externo será bloqueado de todos los tipos de servidores de autenticación externos. Por ejemplo, un usuario que está bloqueado después de no poder iniciar sesión con un servidor RADIUS también se bloqueará cuando use un servidor LDAP. Los fallos de autenticación que se produzcan con motivo de que un servidor AAA es inaccesible o se encuentra inactivo, no se cuenta para el bloqueo de un usuario.

Un usuario que quede bloqueado de un nodo del Controlador de Infraestructura de Política de Aplicaciones de Cisco (APIC) en el clúster será bloqueado de todos los nodos del clúster, incluidos los “leaf switch” y los “spine switch”. Un usuario local que no existe en la base de datos Cisco ACI no puede ser bloqueado debido a esta característica.

7.1.1 ROLES Y PRIVILEGIOS DE AAA RBAC

En cisco ACI se requiere de dependencias de flujo de trabajo para garantizar una segregación en los derechos de acceso, un ejemplo de ello son las reglas RBAC de Cisco Application Centric Infrastructure (ACI). Éstas, permiten o restringen el acceso a parte o todo el “fabric”. Por ejemplo, para configurar un leaf switch para el acceso al servidor, el administrador registrado debe tener derechos para el dominio infra. Por defecto, un administrador de “tenant” no tiene derechos para el dominio infra. En este caso, un administrador de “tenants” que planea utilizar un servidor “bare metal” conectado a un leaf switch no podría completar todos los pasos necesarios para hacerlo.

El administrador del “tenant” tendría que coordinarse con un administrador del “fabric” que tenga derechos sobre el dominio infra. El administrador del “fabric” configuraría las políticas del switch que el administrador del “tenant” utilizaría para implementar una política de aplicación que utiliza el servidor conectado a un leaf switch ACI. Se pueden revisar los roles y privilegios que proporciona el Application Policy Infrastructure Controller (APIC) en “Admin”>AAA>”Security”>”Roles”.



Se muestra a continuación la tabla con los roles y privilegio:

Rol	Privilegio	Descripción
aaa	aaa	Se utiliza para configurar las políticas de autenticación, autorización, contabilidad e importación / exportación.
admin	admin	Proporciona acceso completo a todas las características de la tela. El privilegio de administrador se puede considerar como una unión de todos los demás privilegios.
access-admin	access-connectivity-l1	Se utiliza para la configuración de la Capa 1 bajo infra. Ejemplo: selectores y configuraciones de política de Capa 1 de puerto.

Rol	Privilegio	Descripción
access-admin	access-connectivity-l2	Se utiliza para la configuración de Capa 2 bajo infra. Ejemplo: configuraciones de encapsulado en selectores y entidad adjunta.
	access-connectivity-l3	Se utiliza para la configuración de la Capa 3 en configuraciones de ruta estática e infrarroja en L3Out de un tenant.
	access-connectivity-mgmt	Se utiliza para la gestión de políticas infra.
	access-connectivity-util	Se utiliza para las políticas de tenants ERSPAN.
	access-equipment	Se utiliza para la configuración del puerto de acceso.
	access-protocol-l1	Se usa para configuraciones de protocolo de Capa 1 bajo infra.
	access-protocol-l2	Se usa para configuraciones de protocolo de Capa 2 bajo infra.
	access-protocol-l3	Se usa para configuraciones de protocolo de Capa 3 bajo infra.
	access-protocol-mgmt	Se utiliza para políticas de todo el tejido para NTP, SNMP, DNS y gestión de imágenes.
	access-protocol-ops	Se utiliza para políticas de acceso relacionadas con las operaciones, como la política de clúster y las políticas de firmware.
	access-qos	Se utiliza para cambiar las políticas relacionadas con CoPP y QoS.
fabric-admin	fabric-connectivity-l1	Se utiliza para la configuración de la Capa 1 debajo de fabric. Ejemplo: selectores y política de Capa 1 de puerto y protección de vPC.
	fabric-connectivity-l2	Se utiliza en las políticas de implementación y firmware para generar advertencias para estimar el impacto de la implementación de políticas.
	fabric-connectivity-l3	Utilizado para la configuración de la Capa 3 debajo de la tela. Ejemplo: grupos de protección Fabric IPv4, IPv6 y MAC.
	fabric-connectivity-mgmt	Se utiliza para contadores atómicos y políticas de diagnóstico en los “switches leaf” y en los “switches spine”
	fabric-connectivity-util	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	fabric-equipment	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	fabric-protocol-l1	Se utiliza para configuraciones de protocolo de Capa 1 debajo de fabric.

Rol	Privilegio	Descripción
fabric-admin	fabric-protocol-l2	Se utiliza para configuraciones de protocolo de Capa 2 debajo de fabric.
	fabric-protocol-l3	Se utiliza para configuraciones de protocolo de Capa 3 debajo de fabric.
	fabric-protocol-mgmt	Se utiliza para políticas de todo el tejido para NTP, SNMP, DNS y gestión de imágenes.
	fabric-protocol-ops	Se utiliza para ERSPAN y políticas de puntaje de salud.
	fabric-protocol-util	Se utiliza para la gestión de firmware de traceroute y políticas de seguimiento de puntos finales.
	tenant-connectivity-util	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	tenant-connectivity-l2	Se utiliza para cambios de conectividad de Capa 2, incluidos dominios de puente y subredes.
	tenant-connectivity-l3	Se utiliza para los cambios de conectividad de Capa 3, incluidos los VRF.
	tenant-protocol-ops	Se utiliza para las políticas de traceroute de tenants.
nw-svc-admin	nw-svc-device	Se utiliza para administrar dispositivos de servicio de Capa 4 a Capa 7.
	nw-svc-devshare	Se utiliza para administrar dispositivos de servicio de Capa 4 a Capa 7 compartidos.
	nw-svc-policy	Se utiliza para administrar la orquestación de servicios de red de Capa 4 a Capa 7.
nw-svc-params	nw-svc-params	Se utiliza para administrar las políticas de servicio de Capa 4 a Capa 7.
ops	ops	Se utiliza para ver las políticas configuradas, incluidas las políticas de solución de problemas.
read-all	access-connectivity-l1	Se utiliza para la configuración de la Capa 1 bajo infra. Ejemplo: selectores y configuraciones de política de Capa 1 de puerto.
	access-connectivity-l2	Se utiliza para la configuración de Capa 2 bajo infra. Ejemplo: configuraciones de Encap en selectores y entidad adjunta.
	access-connectivity-l3	Se utiliza para la configuración de la Capa 3 en configuraciones de ruta estática e infra en L3Out de un tenant.
	access-connectivity-mgmt	Se utiliza para la gestión de políticas infra.
	access-connectivity-util	Se utiliza para las políticas de tenants ERSPAN.

Rol	Privilegio	Descripción
read-all	access-equipment	Se utiliza para la configuración del puerto de acceso.
	access-protocol-l1	Se usa para configuraciones de protocolo de Capa 1 bajo infra.
	access-protocol-l2	Se usa para configuraciones de protocolo de Capa 2 bajo infra.
	access-protocol-l3	Se usa para configuraciones de protocolo de Capa 3 bajo infra.
	access-protocol-mgmt	Se utiliza para políticas de todo el tejido para NTP, SNMP, DNS y gestión de imágenes.
	access-protocol-ops	Se utiliza para políticas de acceso relacionadas con las operaciones, como la política de clúster y las políticas de firmware.
	access-qos	Se utiliza para cambiar las políticas relacionadas con CoPP y QoS.
	fabric-connectivity-l1	Se utiliza para la configuración de la Capa 1 debajo de fabric. Ejemplo: selectores y política de Capa 1 de puerto y protección de vPC.
	fabric-connectivity-l2	Se utiliza en las políticas de implementación y firmware para generar advertencias para estimar el impacto de la implementación de políticas.
	fabric-connectivity-l3	Utilizado para la configuración de la Capa 3 debajo de la tela. Ejemplo: grupos de protección Fabric IPv4, IPv6 y MAC.
	fabric-protocol-l1	Se utiliza para configuraciones de protocolo de Capa 1 debajo de fabric.
	fabric-protocol-l2	Se utiliza para configuraciones de protocolo de Capa 2 debajo de fabric.
	fabric-protocol-l3	Se utiliza para configuraciones de protocolo de Capa 3 debajo de fabric.
	nw-svc-device	Se utiliza para administrar dispositivos de servicio de Capa 4 a Capa 7.
	nw-svc-devshare	Se utiliza para administrar dispositivos de servicio de Capa 4 a Capa 7 compartidos.
	nw-svc-params	Se utiliza para administrar las políticas de servicio de Capa 4 a Capa 7.
	nw-svc-policy	Se utiliza para administrar la orquestación de servicios de red de Capa 4 a Capa 7.
	ops	Se utiliza para ver las políticas configuradas, incluidas las políticas de solución de problemas.
	tenant-connectivity-util	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”

Rol	Privilegio	Descripción
read-all	tenant-connectivity-l2	Se utiliza para cambios de conectividad de Capa 2, incluidos dominios de puente y subredes.
	tenant-connectivity-l3	Se utiliza para los cambios de conectividad de Capa 3, incluidos los VRF.
	tenant-connectivity-mgmt	Se utiliza para configuraciones de conectividad de administración de tenants dentro y fuera de banda y para políticas de depuración / monitoreo tales como contadores atómicos y puntaje de salud.
	tenant-epg	Se utiliza para administrar configuraciones de tenants, como eliminar / crear grupos de puntos finales, VRF y dominios de puente.
	tenant-ext-connectivity-l1	Se utiliza para las políticas de firmware de acceso de escritura.
	tenant-ext-connectivity-l2	Se utiliza para administrar configuraciones de tenants L2Out.
	tenant-ext-connectivity-l3	Se usa para administrar configuraciones de tenants L3Out.
	tenant-ext-connectivity-mgmt	Se utiliza como acceso de escritura para políticas de firmware.
	tenant-ext-connectivity-util	Se utiliza para depurar / monitorear / observar políticas como traceroute, ping, oam y eptrk.
	tenant-ext-protocol-l1	Se usa para administrar los protocolos externos de Capa 1 del tenant. Generalmente solo se usa para acceso de escritura para políticas de firmware.
	tenant-ext-protocol-l2	Se usa para administrar protocolos externos de Capa 2 para tenants. Generalmente solo se usa para acceso de escritura para políticas de firmware.
	tenant-ext-protocol-l3	Se usa para administrar protocolos externos de Capa 3 de tenants como BGP, OSPF, PIM e IGMP.
	tenant-ext-protocol-mgmt	Se utiliza como acceso de escritura para políticas de firmware.
	tenant-ext-protocol-util	Se utiliza para depurar / monitorear / observar políticas como traceroute, ping, oam y eptrk.
	tenant-network-profile	Se utiliza para administrar configuraciones de tenants, como eliminar y crear perfiles de red, y eliminar y crear grupos de puntos finales.
	tenant-protocol-l1	Se usa para administrar configuraciones para protocolos de Capa 1 bajo un tenant.
	tenant-protocol-l2	Se usa para administrar configuraciones para protocolos de Capa 2 bajo un tenant.

Rol	Privilegio	Descripción
read-all	tenant-protocol-l3	Se usa para administrar configuraciones para protocolos de Capa 3 bajo un tenant.
	tenant-protocol-mgmt	Solo se utiliza como acceso de escritura para las políticas de firmware.
	tenant-protocol-ops	Se utiliza para las políticas de traceroute de tenants.
	tenant-QoS	Se utiliza para configuraciones relacionadas con la calidad del servicio para un tenant.
	tenant-security	Se utiliza para configuraciones relacionadas con contratos para un tenant.
	vmm-connectivity	Se usa para leer todos los objetos en el inventario VMM de APIC necesarios para la conectividad de la máquina virtual.
	vmm-ep	Se usa para leer puntos finales de máquina virtual e hipervisor en el inventario VMM de APIC.
	vmm-policy	Se utiliza para administrar políticas para redes de máquinas virtuales.
	vmm-protocol-ops	No utilizado por las políticas de VMM.
	vmm-security	Se usa para administrar políticas de autenticación para VMM, como el nombre de usuario y la contraseña para VMware vCenter.
tenant-admin	aaa	Se utiliza para configurar las políticas de autenticación, autorización, registro e importación / exportación.
	access-connectivity-l1	Se utiliza para la configuración de la Capa 1 bajo infra. Ejemplo: selectores y configuraciones de política de Capa 1 de puerto.
	access-connectivity-l2	Se utiliza para la configuración de Capa 2 bajo infra. Ejemplo: configuraciones de Encap en selectores y entidad adjunta.
	access-connectivity-l3	Se utiliza para la configuración de la Capa 3 en configuraciones de ruta estática e infrarroja en L3Out de un tenant.
	access-connectivity-mgmt	Se utiliza para la gestión de políticas infra.
	access-connectivity-util	Se utiliza para las políticas de tenants ERSPAN.
	access-equipment	Se utiliza para la configuración del puerto de acceso.
	access-protocol-l1	Se usa para configuraciones de protocolo de Capa 1 bajo infra.
	access-protocol-l2	Se usa para configuraciones de protocolo de Capa 2 bajo infra.

Rol	Privilegio	Descripción
tenant-admin	access-protocol-l3	Se usa para configuraciones de protocolo de Capa 3 bajo infra.
	access-protocol-mgmt	Se utiliza para políticas de todo el tejido para NTP, SNMP, DNS y gestión de imágenes.
	access-protocol-ops	Se utiliza para políticas de acceso relacionadas con las operaciones, como la política de clúster y las políticas de firmware.
	access-qos	Se utiliza para cambiar las políticas relacionadas con CoPP y QoS.
	fabric-connectivity-l1	Se utiliza para la configuración de la Capa 1 debajo de fabric. Ejemplo: selectores y política de Capa 1 de puerto y protección de vPC.
	fabric-connectivity-l2	Se utiliza en las políticas de implementación y firmware para generar advertencias para estimar el impacto de la implementación de políticas.
	fabric-connectivity-l3	Utilizado para la configuración de la Capa 3 debajo de la tela. Ejemplo: grupos de protección Fabric IPv4, IPv6 y MAC.
	fabric-connectivity-mgmt	Se utiliza para contadores atómicos y políticas de diagnóstico en los “switches leaf” y en los “switches spine”
	fabric-connectivity-util	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	fabric-equipment	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	fabric-protocol-l1	Se utiliza para configuraciones de protocolo de Capa 1 debajo de fabric.
	fabric-protocol-l2	Se utiliza para configuraciones de protocolo de Capa 2 debajo de fabric.
	fabric-protocol-l3	Se utiliza para configuraciones de protocolo de Capa 3 debajo de fabric.
	fabric-protocol-mgmt	Se utiliza para políticas de todo el tejido para NTP, SNMP, DNS y gestión de imágenes.
	fabric-protocol-ops	Se utiliza para ERSPAN y políticas de puntaje de salud.
	fabric-protocol-util	Se utiliza para la gestión de firmware de traceroute y políticas de seguimiento de puntos finales.
	nw-svc-device	Se utiliza para administrar dispositivos de servicio de Capa 4 a Capa 7.
	nw-svc-devshare	Se utiliza para administrar dispositivos de servicio de Capa 4 a Capa 7 compartidos.

Rol	Privilegio	Descripción
tenant-admin	nw-svc-params	Se utiliza para administrar las políticas de servicio de Capa 4 a Capa 7.
	nw-svc-policy	Se utiliza para administrar la orquestación de servicios de red de Capa 4 a Capa 7.
	ops	Se utiliza para ver las políticas configuradas, incluidas las políticas de solución de problemas.
	tenant-connectivity-util	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	tenant-connectivity-l2	Se utiliza para cambios de conectividad de Capa 2, incluidos dominios de puente y subredes.
	tenant-connectivity-l3	Se utiliza para los cambios de conectividad de Capa 3, incluidos los VRF.
	tenant-connectivity-mgmt	Se utiliza para configuraciones de conectividad de administración de tenants dentro y fuera de banda y para políticas de depuración / monitoreo tales como contadores atómicos y puntaje de salud.
	tenant-epg	Se utiliza para administrar configuraciones de tenants, como eliminar / crear grupos de puntos finales, VRF y dominios de puente.
	tenant-ext-connectivity-l1	Se utiliza para las políticas de firmware de acceso de escritura.
	tenant-ext-connectivity-l2	Se utiliza para administrar configuraciones de tenants L2Out.
	tenant-ext-connectivity-l3	Se usa para administrar configuraciones de tenants L3Out.
	tenant-ext-connectivity-mgmt	Se utiliza como acceso de escritura para políticas de firmware.
	tenant-ext-connectivity-util	Se utiliza para depurar / monitorear / observar políticas como traceroute, ping, oam y eptrk.
	tenant-ext-protocol-l1	Se usa para administrar los protocolos externos de Capa 1 del tenant. Generalmente solo se usa para acceso de escritura para políticas de firmware.
	tenant-ext-protocol-l2	Se usa para administrar protocolos externos de Capa 2 para tenants. Generalmente solo se usa para acceso de escritura para políticas de firmware.
	tenant-ext-protocol-l3	Se usa para administrar protocolos externos de Capa 3 de tenants como BGP, OSPF, PIM e IGMP.

Rol	Privilegio	Descripción
tenant-admin	tenant-ext-protocol-mgmt	Se utiliza como acceso de escritura para políticas de firmware.
	tenant-ext-protocol-util	Se utiliza para depurar / monitorear / observar políticas como traceroute, ping, oam y eptrk.
	tenant-network-profile	Se utiliza para administrar configuraciones de tenants, como eliminar y crear perfiles de red, y eliminar y crear grupos de puntos finales.
	tenant-protocol-l1	Se usa para administrar configuraciones para protocolos de Capa 1 bajo un tenant.
	tenant-protocol-l2	Se usa para administrar configuraciones para protocolos de Capa 2 bajo un tenant.
	tenant-protocol-l3	Se usa para administrar configuraciones para protocolos de Capa 3 bajo un tenant.
	tenant-protocol-mgmt	Solo se utiliza como acceso de escritura para las políticas de firmware.
	tenant-protocol-ops	Se utiliza para las políticas de traceroute de tenants.
	tenant-QoS	Se utiliza para configuraciones relacionadas con la calidad del servicio para un tenant.
	tenant-security	Se utiliza para configuraciones relacionadas con contratos para un tenant.
	vmm-connectivity	Se usa para leer todos los objetos en el inventario VMM de APIC necesarios para la conectividad de la máquina virtual.
	vmm-ep	Se usa para leer puntos finales de máquina virtual e hipervisor en el inventario VMM de APIC.
	vmm-policy	Se utiliza para administrar políticas para redes de máquinas virtuales.
	vmm-protocol-ops	No utilizado por las políticas de VMM.
	vmm-security	Se usa para administrar políticas de autenticación para VMM, como el nombre de usuario y la contraseña para VMware vCenter.
tenant-ext-admin	tenant-connectivity-util	Se utiliza para políticas de contador atómico, diagnóstico y gestión de imágenes en los “switches leaf” y en los “switches spine”
	tenant-connectivity-l2	Se utiliza para cambios de conectividad de Capa 2, incluidos dominios de puente y subredes.
	tenant-connectivity-l3	Se utiliza para los cambios de conectividad de Capa 3, incluidos los VRF.

Rol	Privilegio	Descripción
tenant-ext-admin	tenant-connectivity-mgmt	Se utiliza para configuraciones de conectividad de administración de tenants dentro y fuera de banda y para políticas de depuración / monitoreo tales como contadores atómicos y puntaje de salud.
	tenant-epg	Se utiliza para administrar configuraciones de tenants, como eliminar / crear grupos de puntos finales, VRF y dominios de puente.
	tenant-ext-connectivity-l1	Se utiliza para las políticas de firmware de acceso de escritura.
	tenant-ext-connectivity-l2	Se utiliza para administrar configuraciones de tenants L2Out.
	tenant-ext-connectivity-l3	Se usa para administrar configuraciones de tenants L3Out.
	tenant-ext-connectivity-mgmt	Se utiliza como acceso de escritura para políticas de firmware.
	tenant-ext-connectivity-util	Se utiliza para depurar / monitorear / observar políticas como traceroute, ping, oam y eptrk.
	tenant-ext-protocol-l1	Se usa para administrar los protocolos externos de Capa 1 del tenant. Generalmente solo se usa para acceso de escritura para políticas de firmware.
	tenant-ext-protocol-l2	Se usa para administrar protocolos externos de Capa 2 para tenants. Generalmente solo se usa para acceso de escritura para políticas de firmware.
	tenant-ext-protocol-l3	Se usa para administrar protocolos externos de Capa 3 de tenants como BGP, OSPF, PIM e IGMP.
	tenant-ext-protocol-mgmt	Se utiliza como acceso de escritura para políticas de firmware.
	tenant-ext-protocol-util	Se utiliza para depurar / monitorear / observar políticas como traceroute, ping, oam y eptrk.
	tenant-network-profile	Se utiliza para administrar configuraciones de tenants, como eliminar y crear perfiles de red, y eliminar y crear grupos de puntos finales.
	tenant-protocol-l1	Se usa para administrar configuraciones para protocolos de Capa 1 bajo un tenant.
	tenant-protocol-l2	Se usa para administrar configuraciones para protocolos de Capa 2 bajo un tenant.
	tenant-protocol-l3	Se usa para administrar configuraciones para protocolos de Capa 3 bajo un tenant.
	tenant-protocol-mgmt	Solo se utiliza como acceso de escritura para las políticas de firmware.

Rol	Privilegio	Descripción
tenant-ext-admin	tenant-protocol-ops	Se utiliza para las políticas de traceroute de tenants.
	tenant-QoS	Se utiliza para configuraciones relacionadas con la calidad del servicio para un tenant.
	tenant-security	Se utiliza para configuraciones relacionadas con contratos para un tenant.
	vmm-connectivity	Se usa para leer todos los objetos en el inventario VMM de APIC necesarios para la conectividad de la máquina virtual.
	vmm-ep	Se usa para leer puntos finales de máquina virtual e hipervisor en el inventario VMM de APIC.
	vmm-policy	Se utiliza para administrar políticas para redes de máquinas virtuales.
	vmm-protocol-ops	No utilizado por las políticas de VMM.
	vmm-security	Se usa para administrar políticas de autenticación para VMM, como el nombre de usuario y la contraseña para VMware vCenter.
vmm-admin	vmm-connectivity	Se usa para leer todos los objetos en el inventario VMM de APIC necesarios para la conectividad de la máquina virtual.
	vmm-ep	Se usa para leer puntos finales de máquina virtual e hipervisor en el inventario VMM de APIC.
	vmm-policy	Se utiliza para administrar políticas para redes de máquinas virtuales.
	vmm-protocol-ops	No utilizado por las políticas de VMM.
	vmm-security	Se usa para administrar políticas de autenticación para un VMM, como el nombre de usuario y la contraseña para VMware vCenter.

7.1.2 CREACIÓN DE UN USUARIO LOCAL CON CERTIFICADO USANDO LA GUI APIC

En el script de configuración inicial, la cuenta de administrador está configurada y el administrador (admin) es el único usuario cuando se inicia el sistema. El APIC admite un sistema de control de acceso granular basado en roles donde las cuentas de usuario se pueden crear con varios roles, incluidos los usuarios no administrativos con menos privilegios.

Para una correcta configuración se deberán de revisar ciertas configuraciones inicialmente:

a) El ACI fabric está instalado, los controladores APIC están en línea y el clúster APIC está formado y en buen estado.

b) Según corresponda, se deberán definir los dominios de seguridad a los que accederá el usuario. Por ejemplo, si la nueva cuenta de uso se limitará a acceder a un tenant, el dominio del tenant se etiquetará en consecuencia.

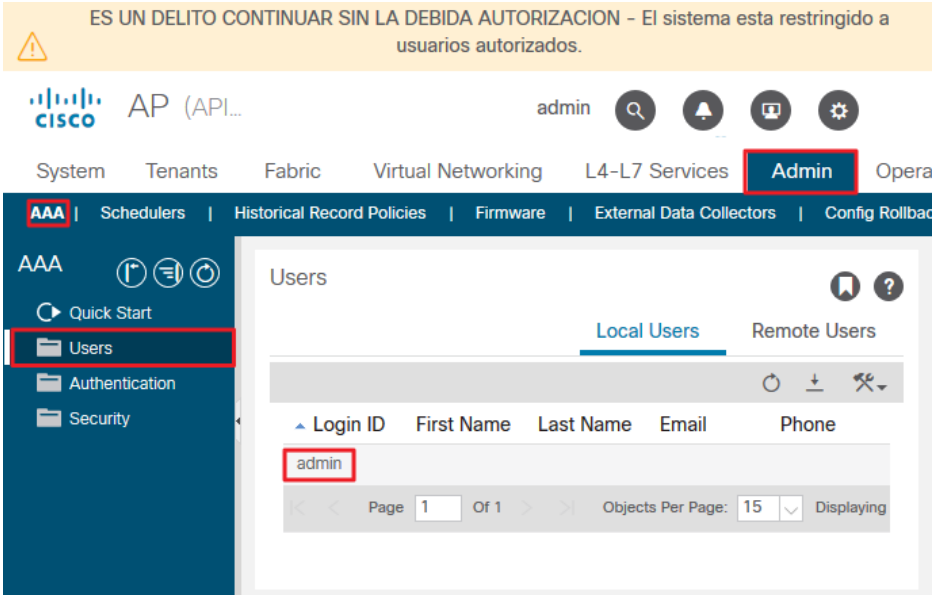
c) El APIC contiene una cuenta de usuario y está habilitada con los siguientes permisos:

   i. Creación de un proveedor TACACS +.

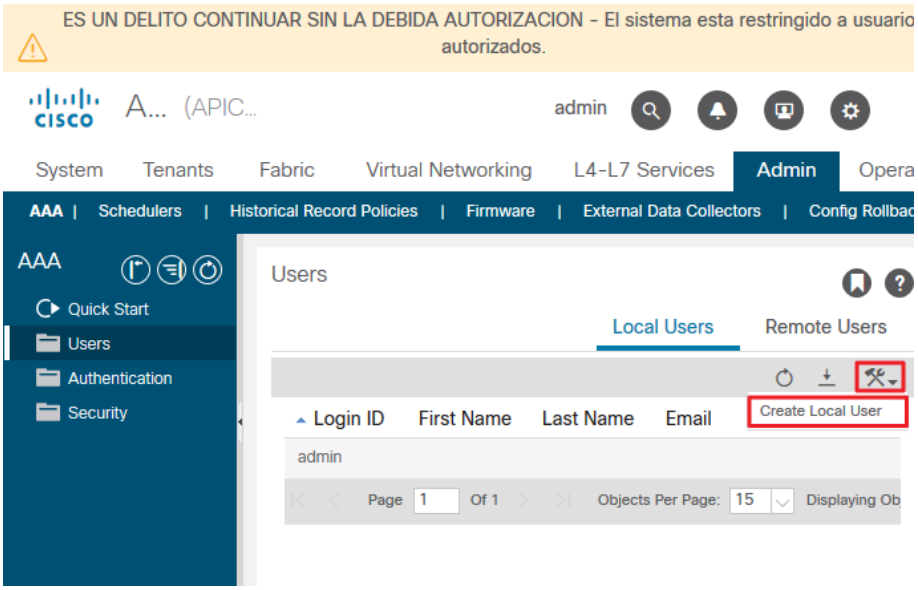
d) Creación de cuentas de usuario local en los dominios de seguridad de destino. Si el dominio de destino es “all”, la cuenta de inicio de sesión utilizada para crear el nuevo usuario local debe ser un administrador de toda la estructura al que tenga acceso “all”. Si el dominio de destino es un “tenant”, la cuenta de inicio de sesión utilizada para crear el nuevo usuario local debe ser un administrador de “tenants” que tenga derechos completos de acceso de lectura y escritura para el dominio de “tenant” de destino.

Una vez comprobadas las configuraciones y permisos anteriores se deberá realizar lo siguiente:

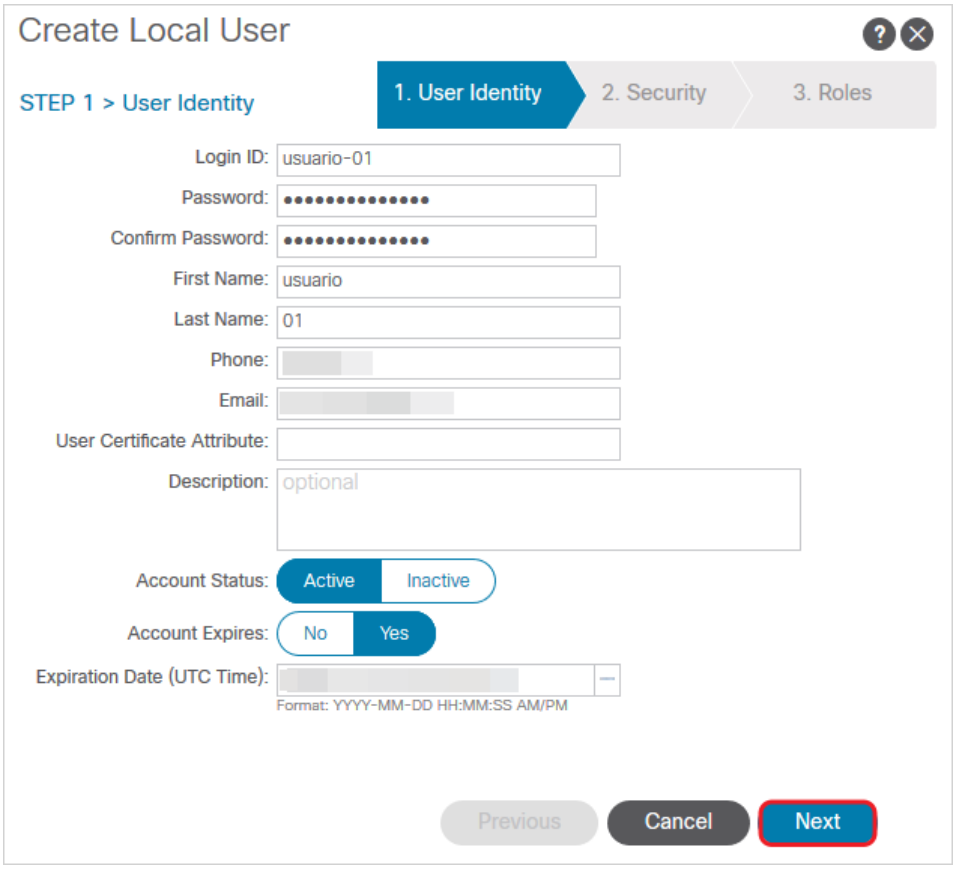
a) En la barra de menú, elija “Admin”>AAA y haga clic en “Users” y seleccione “Local Users” donde se deberá verificar que el usuario administrador por defecto (admin) está presente.



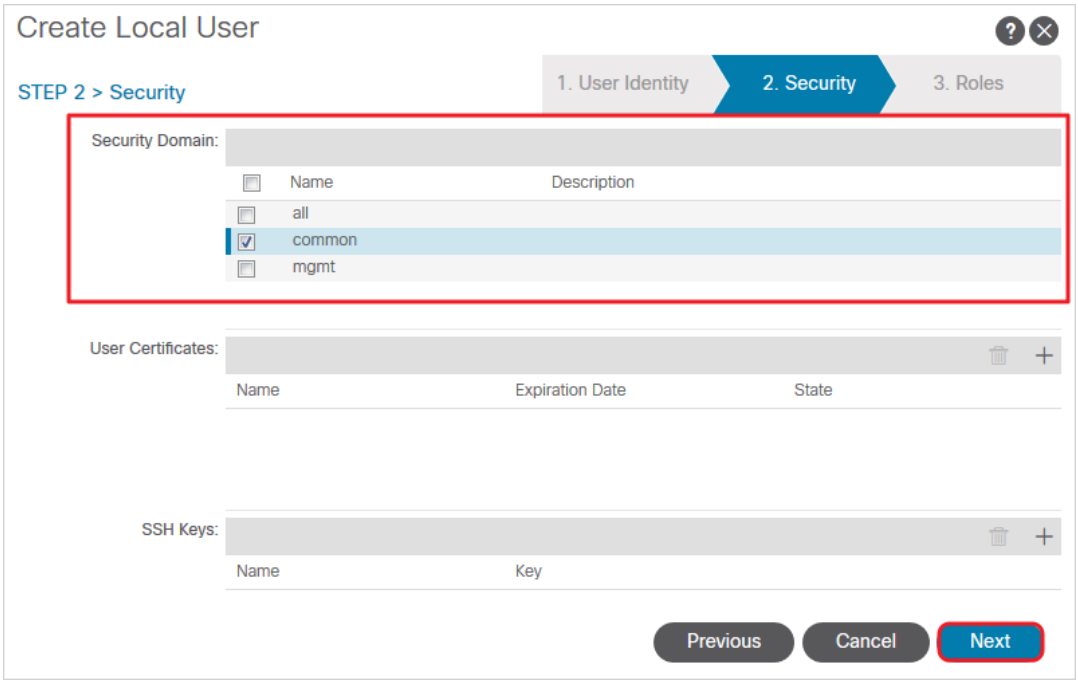
b) Haga clic en la lista desplegable del icono de tareas y seleccione “Create Local User”.



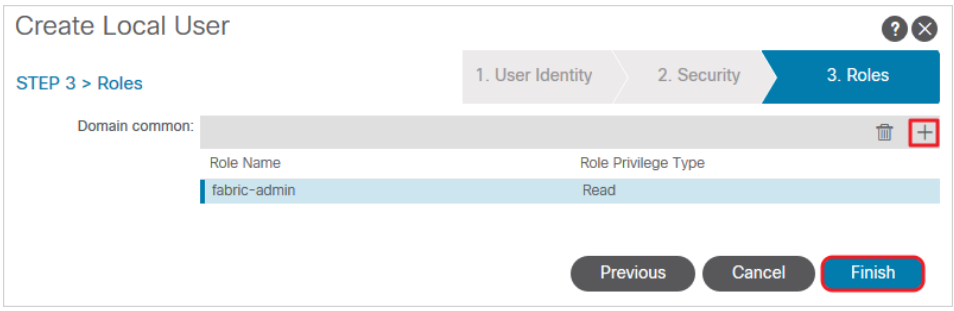
c) Se abrirá la ventana de “Create Local User” donde se deberán configurar los campos con los parámetros que más convengan a su organización y pulse “Next”.



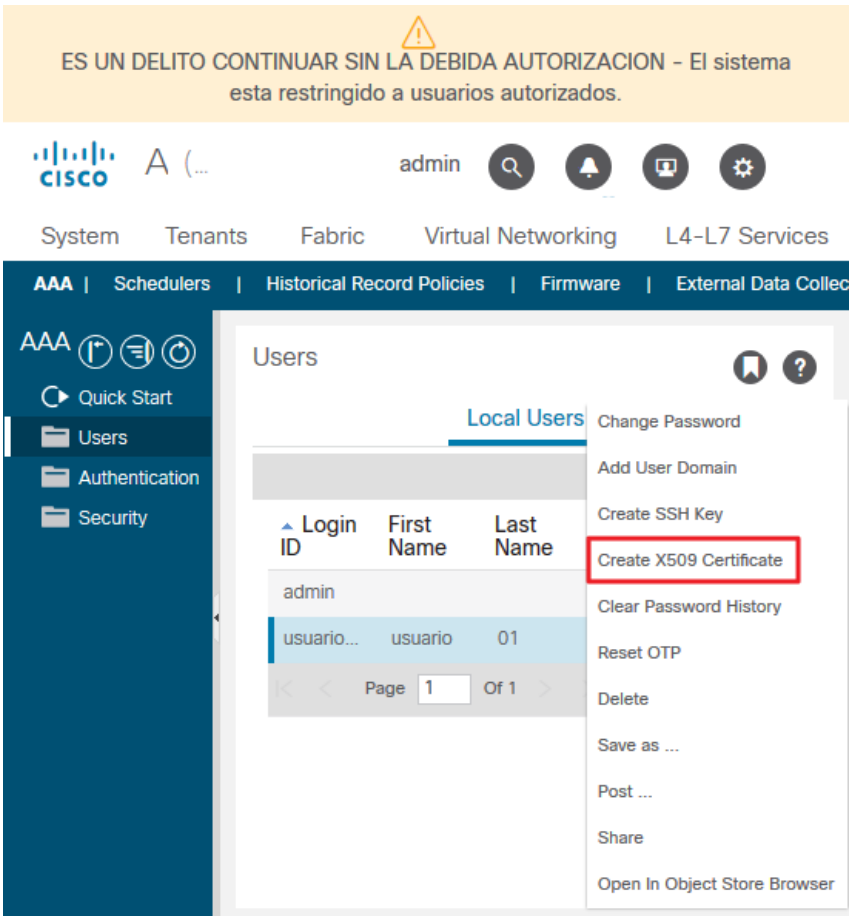
d) Posteriormente en el menú “Security” se deberán configurar los dominios de seguridad del usuario y pulsar “Next” para continuar.



e) Finalmente, en el menú “Roles” se deberán seleccionar los roles del usuario a crear añadiéndolos por medio del icono “+". Una vez completado se deberá pulsar “Finish” para finalizar.



f) Nuevamente en el apartado User, haciendo clic derecho sobre el nuevo usuario creado se desplegará un menú donde podrá elegir la opción “Create X509 Certificate”. En este apartado podrá crear un certificado X509

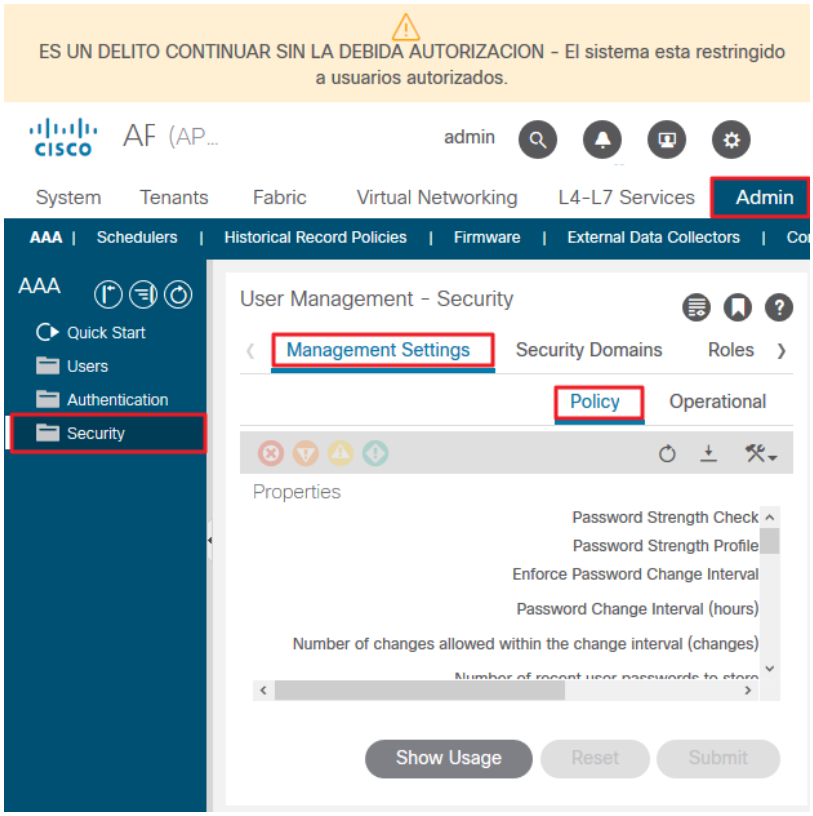


7.1.3 CONFIGURACIÓN DE POLÍTICA DE CONTRASEÑAS USANDO LA GUI APIC

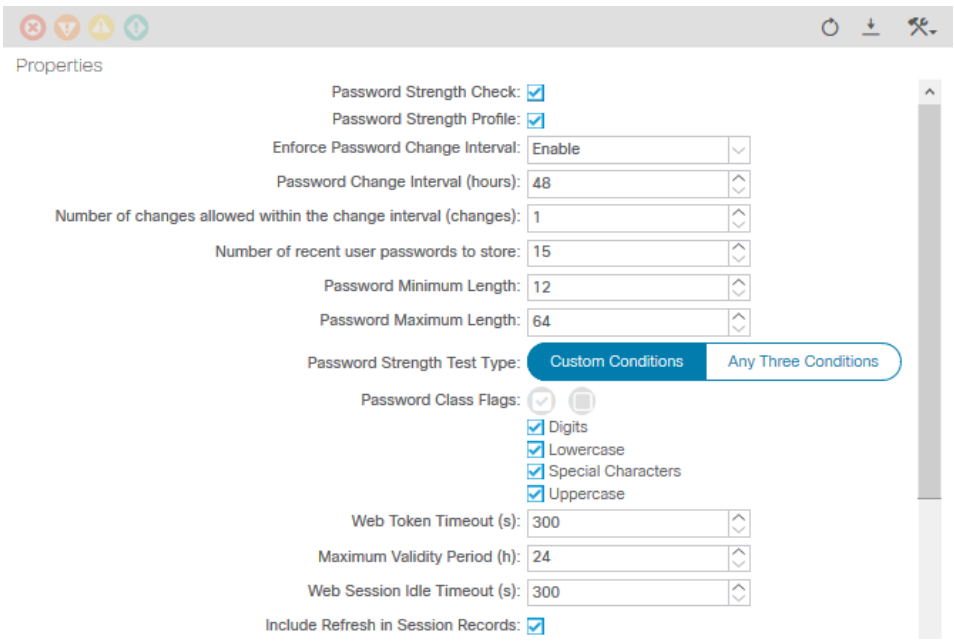
El apartado “Security” de AAA permite una configuración en la complejidad y caducidad de contraseñas, además, se puede especificar cuántos intentos fallidos de inicio de sesión puede tener el usuario dentro de un período de tiempo específico siempre y cuando actualice a la versión 4.2(4) o posterior.

Para realizar modificaciones en la política de seguridad de los usuarios locales, deberá realizar las siguientes tareas:

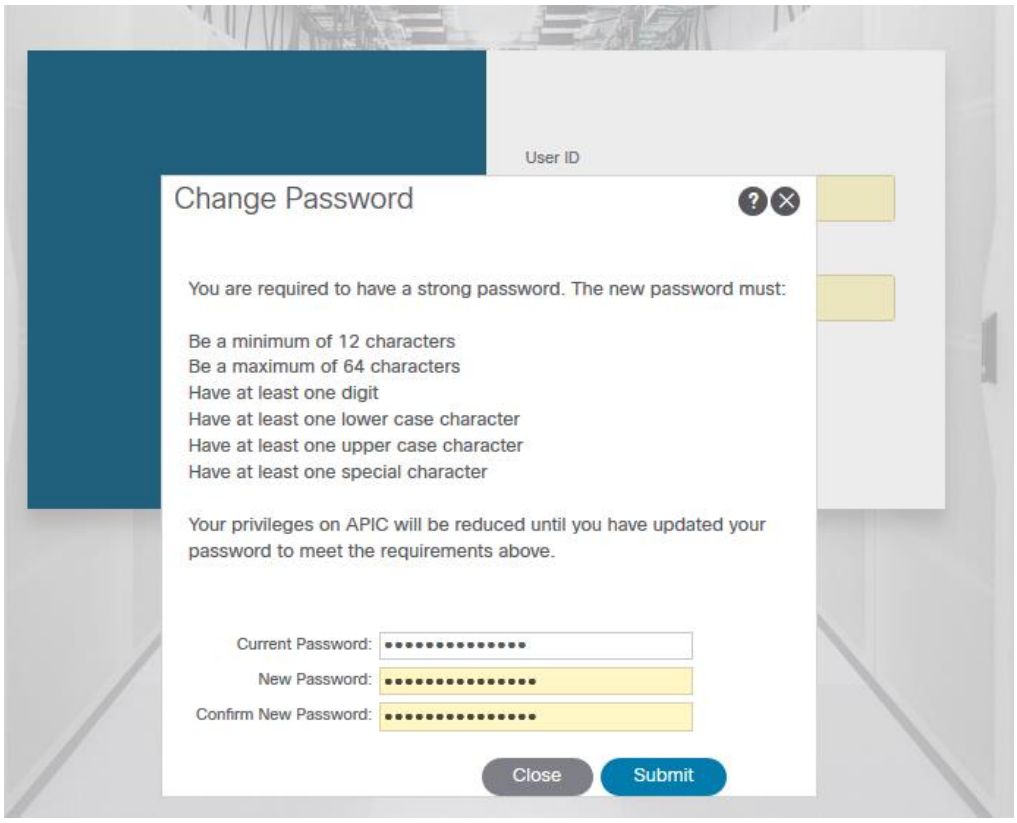
a) En la barra de menú elija “Admin”>AAA>”Security. Una vez allí, deberá seleccionar “Management Settings”>”Policy”.



b) Deberá escoger los parámetros y configuraciones que, adecuándose a su organización, sean los más restrictivos.



c) Si la contraseña de su usuario no cumple con la nueva política de contraseñas, en el momento que cierre sesión y vuelva a iniciar le pedirá el cambio de la misma para que cumpla con las nuevas configuraciones.



7.2 CONFIGURACIÓN DE PROTOCOLOS DE AUTENTICACIÓN

En este apartado se detallan configuraciones para la autenticación mediante RADIUS, TACACS+ y LDAP. Debe tener en consideración que una práctica muy recomendable en la configuración de estos protocolos es la modificación de los puertos por defecto de escucha y administración.

Nota: Los usuarios remotos para la autenticación AAA con shell: domains = all / read-all / no podrán acceder a los switches Leaf y Spine en la estructura por motivos de seguridad. Esto sucede en todas las versiones desde la versión 4.0(1h).

7.2.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuándo comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Nota: La implementación de una solución de autenticación RADIUS, supone asumir las siguientes vulnerabilidades conocidas:

- Los mensajes RADIUS no viajan cifrados, a excepción de aquellos datos especialmente sensibles como las contraseñas.
- RADIUS utiliza MD5 como algoritmo criptográfico de hashing, lo que lo hace vulnerable a ataques de colisión.
- La comunicación se realiza a través del protocolo UDP, lo que permite que las direcciones IP puedan ser fácilmente falseadas y susceptible de suplantación de identidad.
- Las especificaciones para la clave compartida no son lo suficientemente robustas y es reutilizada por el servidor con los clientes. Por tanto, es vulnerable a ataques de fuerza bruta. Una vez obtenida la clave, el campo "Autenticator" utilizado en mensajes de autenticación (Access-Request) es fácilmente generado.

Para configurar el acceso RADIUS mediante el APIC de cisco deberá comprobar las siguientes configuraciones:

a) ACI fabric está instalado, los Controladores de Infraestructura de Políticas de Aplicación (APIC) están en línea y el clúster APIC está formado y en buen estado.

b) El nombre de host del servidor RADIUS o la dirección IP, el puerto, el protocolo de autorización y la clave están disponibles.

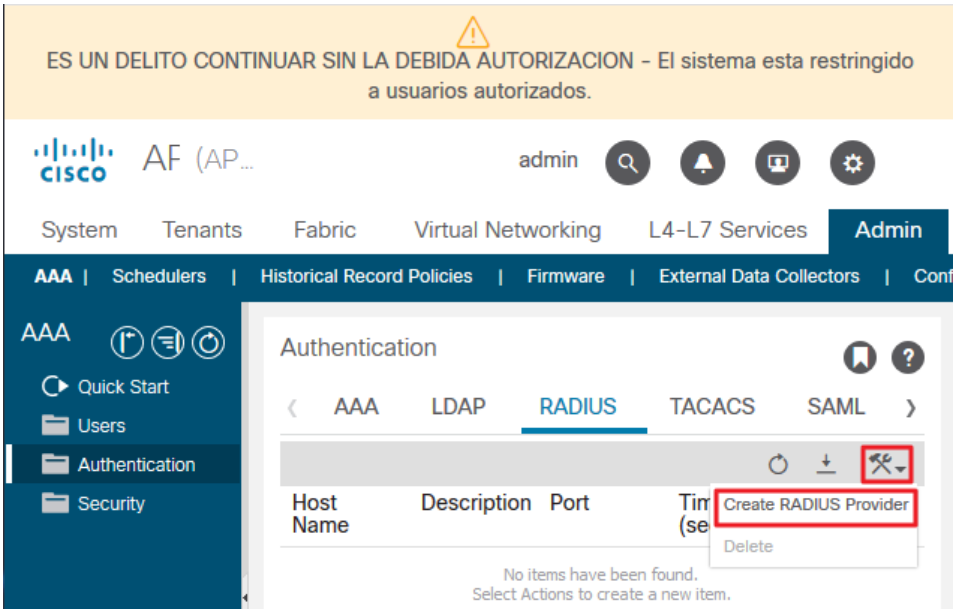
c) El grupo de administración “endpoint” APIC está disponible.

Una vez comprobadas las configuraciones citadas anteriormente, se describen los pasos necesarios para la configuración de un servidor RADIUS en el APIC de cisco.

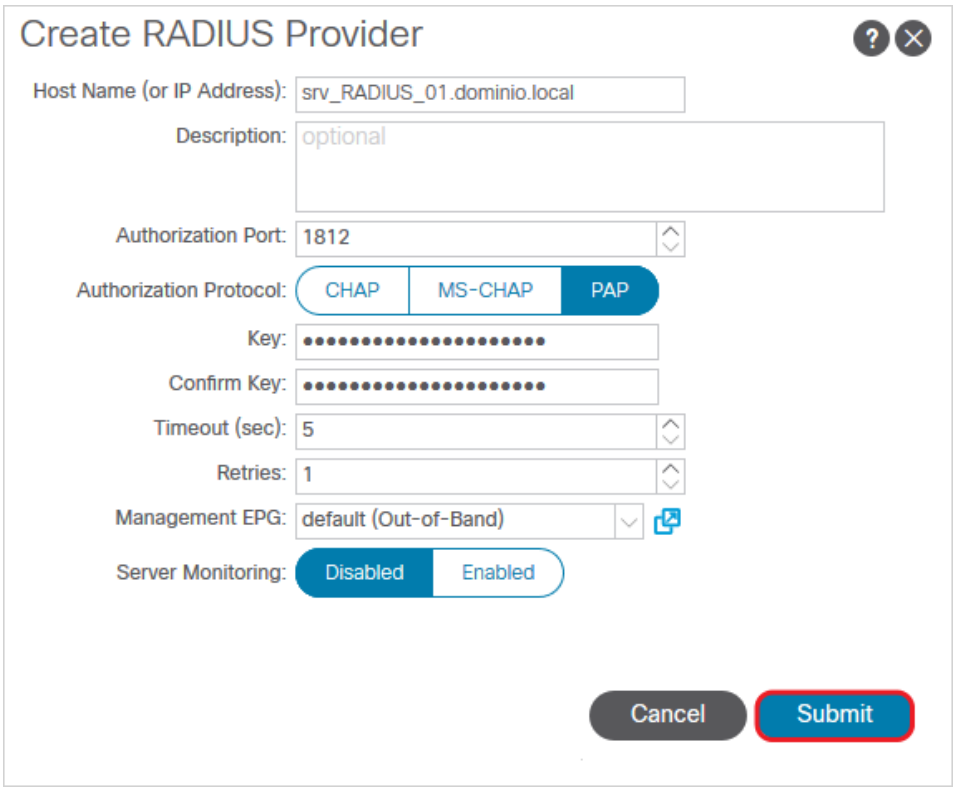
a) Creación de un proveedor RADIUS en el APIC.

i. En la barra de menú, elija “Admin”>AAA. Posteriormente en el panel de navegación , haga clic en “Authentication” y luego haga clic en la pestaña “RADIUS”.

ii. En el panel de trabajo, seleccione el icono de trabajo/acciones y pulse en “Create RADIUS Provider”.



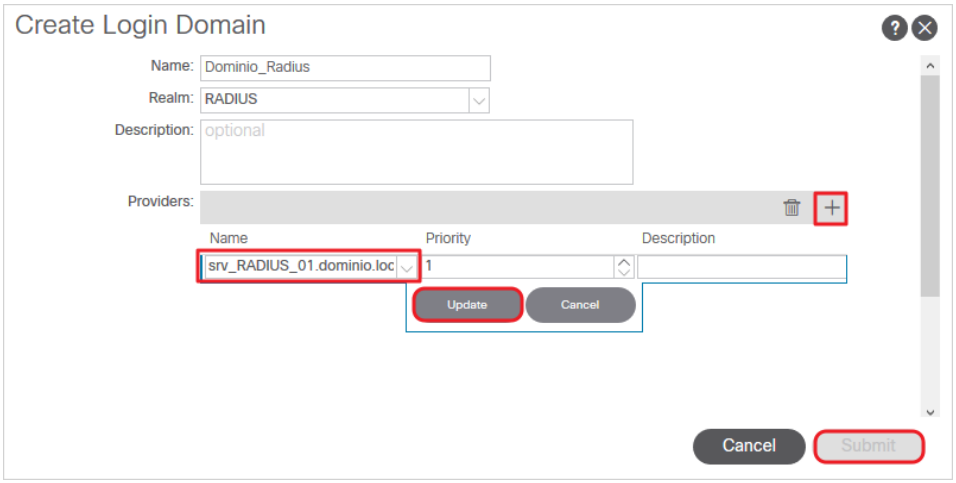
iii. Especifique el nombre de host RADIUS (o la dirección IP), el puerto, el protocolo y el grupo de punto final de administración. Pulse “Submit” para continuar.



b) Creación de un dominio de inicio de sesión para RADIUS.

i. En el panel de navegación, elija “Authentication”>AAA. Posteriormente pulse en el icono de trabajo y seleccione “Create Login Domain”.

ii. En la ventana “Create Login Domain” elija las opciones que convengan y en el apartado “Providers”, pulse en el icono de “+” y seleccione el servidor RADIUS configurado anteriormente. Pulse “Update” y posteriormente “Submit” para completar el proceso.



7.2.2 TACACS+

El sistema de control de acceso (TACACS) se refiere a una familia de protocolos que manejan la autenticación remota y los servicios relacionados para el control de acceso en red a través de un servidor centralizado. El protocolo original TACACS, derivó a dos protocolos más actuales:

a) Extended TACACS (XTACACS): Es una extensión patentada de TACACS introducida por Cisco Systems en 1990 sin compatibilidad con el protocolo original. TACACS y XTACACS permiten que un servidor de acceso remoto se comunique con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

b) Terminal Access Controller Access-Control System Plus (TACACS+): Es un protocolo desarrollado por Cisco y lanzado como un estándar abierto a partir de 1993. Aunque derivado de TACACS, TACACS+ es un protocolo separado que maneja servicios de autenticación, autorización y contabilización (AAA). TACACS+ ha reemplazado en gran medida a sus predecesores.

TACACS+ y RADIUS generalmente han reemplazado a TACACS y XTACACS en redes construidas o actualizadas más recientemente. TACACS+ es un protocolo completamente nuevo y no es compatible con sus predecesores, TACACS y XTACACS. La gran diferencia de TACACS+ es que usa TCP mientras que RADIUS utiliza UDP.

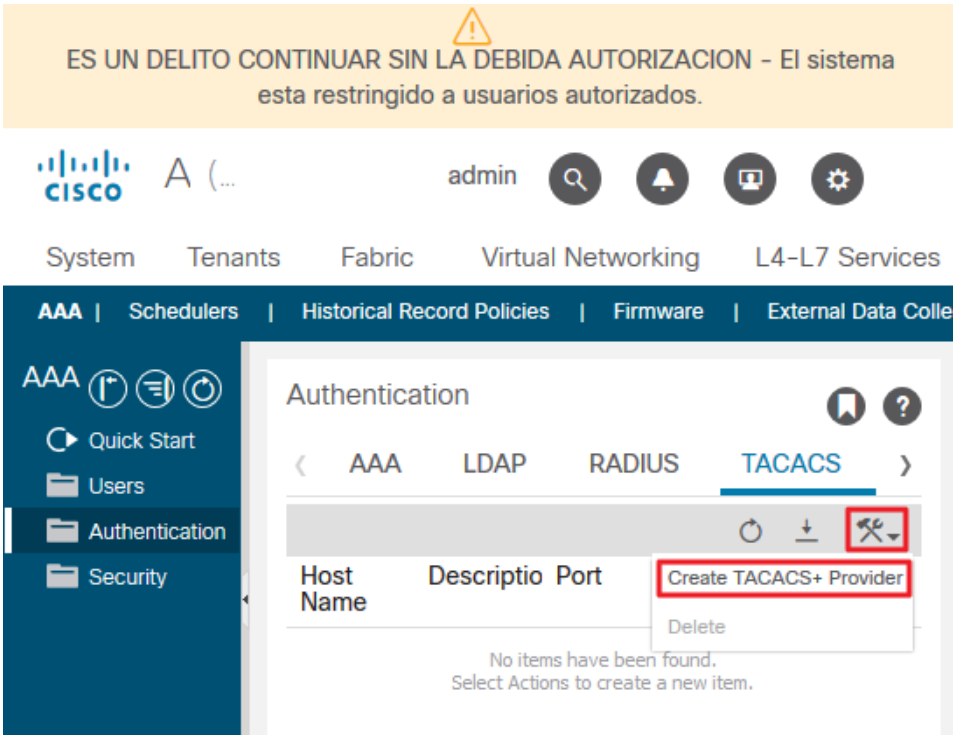
Como TCP es un protocolo orientado a la conexión, TACACS+ no tiene que implementar el control de transmisión. RADIUS, sin embargo, tiene que detectar y corregir errores de transmisión como pérdida de paquetes, tiempo de espera, etc, ya que depende de UDP. TACACS+, a diferencia de RADIUS, cifra las cuentas de usuario, la autorización, etc, y por lo tanto, no tiene las vulnerabilidades presentes en el protocolo RADIUS.

TACACS+ es una extensión diseñada por CISCO para TACACS que cifra el contenido completo de cada paquete. Además, proporciona control granular (varios métodos de asignación de privilegios por usuario o grupos).

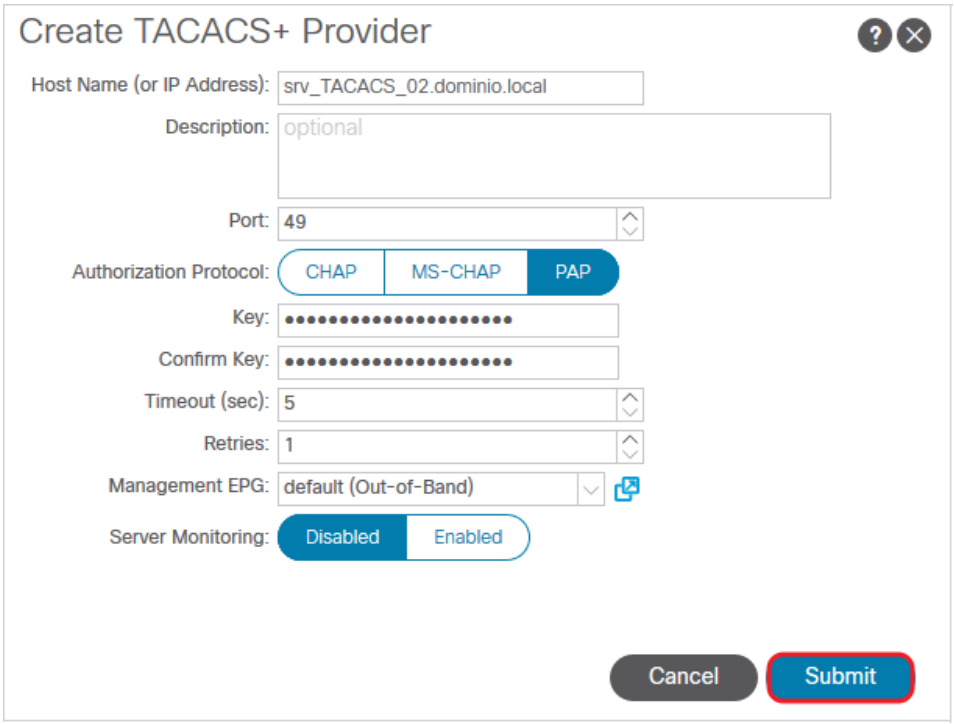
Para configurar el acceso TACACS+ mediante el APIC de cisco deberá comprobar las siguientes configuraciones:

a) En la barra de menú, elija “Admin”>AAA. Posteriormente en el panel de navegación, haga clic en “Authentication” y luego haga clic en la pestaña “TACACS”.

i. En el panel de trabajo, seleccione el icono de trabajo/acciones y pulse en “Create TACACS+ Provider”.



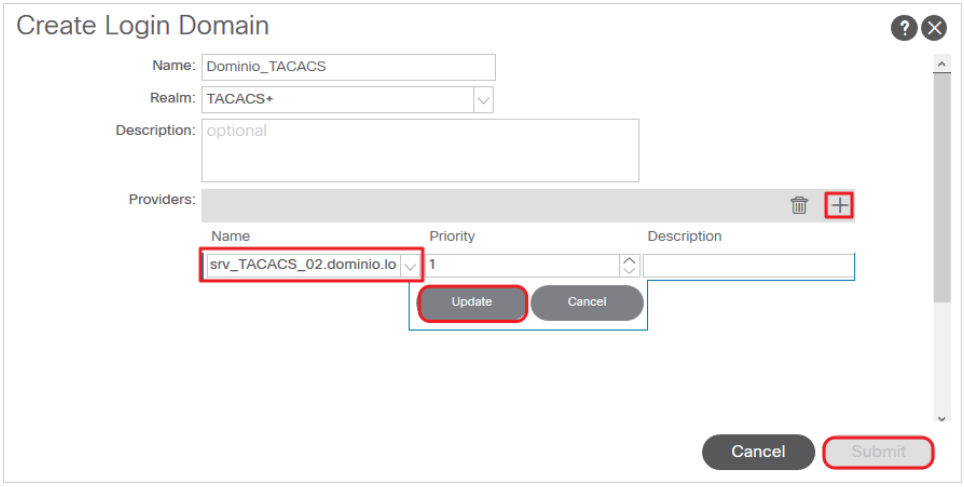
ii. Especifique el nombre de host TACACS (o la dirección IP), el puerto, el protocolo y el grupo de punto final de administración. Pulse “Submit” para continuar.



b) Creación de un dominio de inicio de sesión para TACACS.

i. En el panel de navegación, elija “Authentication”>AAA. Posteriormente pulse en el icono de trabajo y seleccione “Create Login Domain”.

ii. En la ventana “Create Login Domain” elija las opciones que convengan y en el apartado “Providers”, pulse en el icono de “+” y seleccione el servidor TACACS+ configurado anteriormente. Pulse “update” y posteriormente “Submit” para completar el proceso.



7.2.3 LDAP

LDAP (Lightweight Directory Access Protocol) se trata de un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol.

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Algunas implementaciones LDAP:

a) Active Directory: Es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración. Un Servicio de Directorio es un depósito estructurado de la información de los diversos objetos que contiene el Active Directory, en este caso podrían ser impresoras, usuarios, equipos… Utiliza distintos protocolos (principalmente, LDAP, DNS, DHCP, Kerberos…). Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

b) Novell Directory Services: También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos, que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso, por medio de herencia. La ventaja de esta implementación es que corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo. Es el precursor en materia de estructuras de Directorio, ya que fue introducido en 1990 con la versión de Novell Netware 4.0. Aunque AD de Microsoft alcanzó mayor popularidad, todavía no puede igualar la fiabilidad y calidad de eDirectory y su capacidad Multiplataforma.

c) OpenLDAP: Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la plataforma, varias distribuciones GNU/Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.

   OpenLDAP tiene cuatro componentes principales:

   i. slapd – demonio LDAP autónomo.

   ii. slurpd – demonio de replicación de actualizaciones LDAP autónomo.

   iii. Rutinas de biblioteca de soporte del protocolo LDAP

   iv. Utilidades, herramientas y clientes.

Para configurar el acceso LDAP mediante el APIC de cisco deberá comprobar las siguientes configuraciones:

a) ACI fabric está instalado, los Controladores de Infraestructura de Políticas de Aplicación (APIC) están en línea y el clúster APIC está formado y en buen estado.

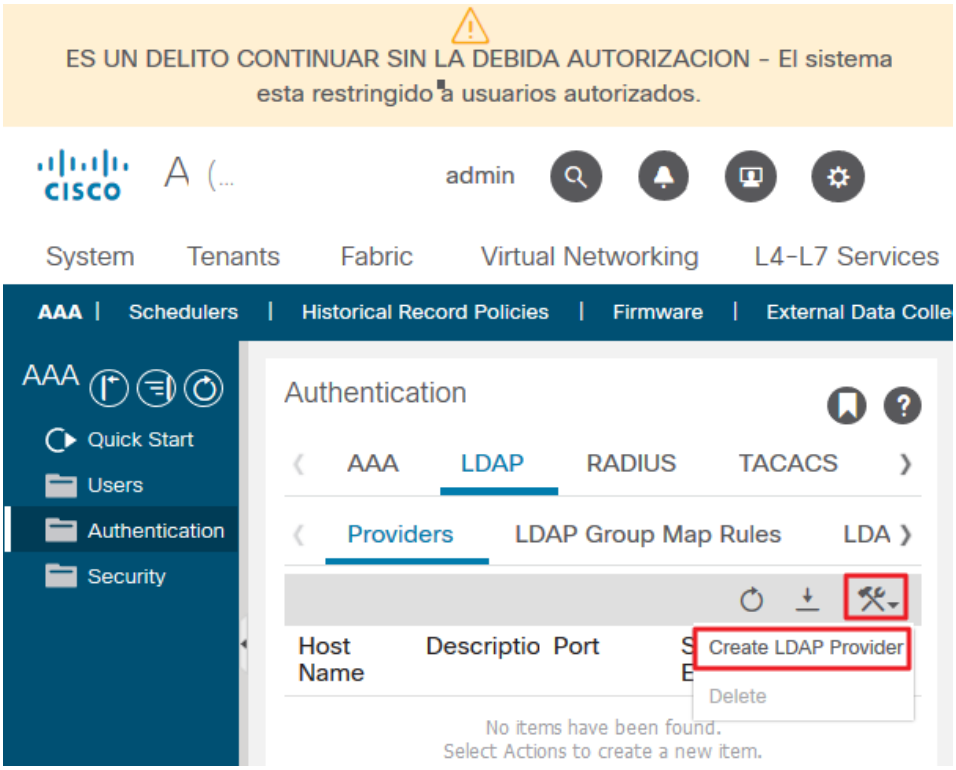
b) El nombre de host del servidor LDAP o la dirección IP, el puerto y la clave están disponibles.

c) El grupo de administración “endpoint” APIC está disponible.

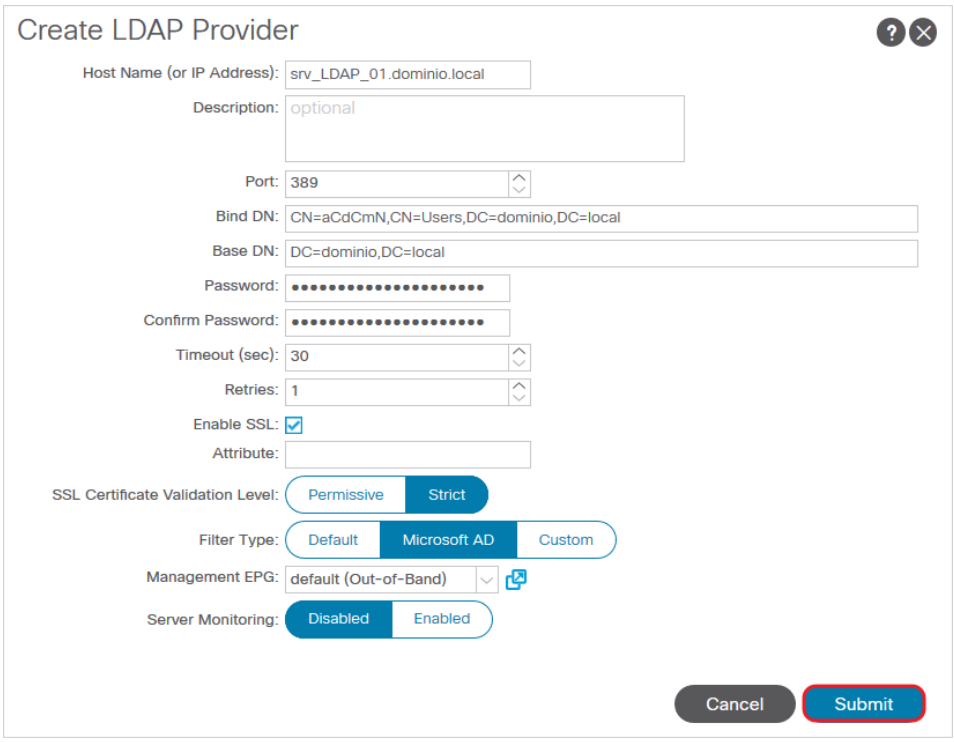
Una vez comprobadas las configuraciones citadas anteriormente, se describen los pasos necesarios para la configuración de un servidor LDAP en el APIC de cisco.

a) En la barra de menú, elija “Admin”>AAA. Posteriormente en el panel de navegación, haga clic en “Authentication” y luego haga clic en la pestaña “LDAP”.

i. En el panel de trabajo, seleccione el icono de trabajo/acciones y pulse en “Create LDAP Provider”.



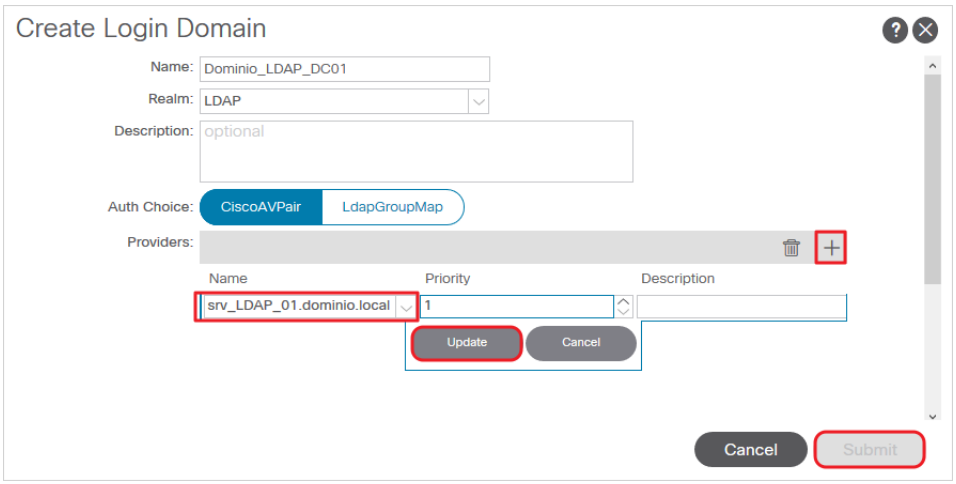
ii. Especifique el nombre de host LDAP (o la dirección IP), el puerto, el Bind DN, el Base DN, etc. Completando los parámetros necesarios para su organización y que doten al LDAP de una mayor seguridad. Pulse “Submit” para continuar.



b) Creación de un dominio de inicio de sesión para LADP.

i. En el panel de navegación, elija “Authentication”>AAA. Posteriormente pulse en el icono de trabajo y seleccione “Create Login Domain”.

ii. En la ventana “Create Login Domain” elija las opciones que convengan y en el apartado “Providers”, pulse en el icono de “+” y seleccione el servidor “LDAP” configurado anteriormente. Pulse “update” y posteriormente “Submit” para completar el proceso.



7.3 CONFIGURACIÓN 802.1X

El estándar IEEE 802.1X, define un protocolo de autenticación y control de acceso basado en cliente-servidor que restringe la conexión de clientes no autorizados a una LAN a través de puertos de acceso público. El servidor de autenticación autentica a cada cliente conectado a un puerto de dispositivo Cisco NX-OS.

Hasta que el cliente se autentique, el control de acceso 802.1X solo permite el tráfico del Protocolo de autenticación extensible a través de LAN (EAPOL) a través del puerto al que está conectado el cliente. Una vez que la autenticación es exitosa, el tráfico normal puede pasar por el puerto.

El sistema cliente / servidor distribuido RADIUS le permite proteger las redes contra el acceso no autorizado. En la implementación de Cisco ACI, los clientes RADIUS se ejecutan en los ToR y envían solicitudes de autenticación y contabilización a un servidor RADIUS central que contiene toda la información de acceso de servicio de red y autenticación de usuario.

La característica 802.1X puede restringir el tráfico en un puerto con los siguientes modos:

a) Modo de host único: permite el tráfico desde un solo dispositivo de punto final en el puerto 802.1X. Una vez que el dispositivo de punto final se autentica, el APIC coloca el puerto en el estado autorizado. Cuando el dispositivo de punto final abandona el puerto, el APIC vuelve a colocar el puerto en el estado no autorizado. Una violación de seguridad en 802.1X se define como la detección de tramas provenientes de cualquier dirección MAC que no sea la única dirección MAC autorizada como resultado de una autenticación exitosa. En este caso, la interfaz en la que se detecta esta violación de asociación de seguridad (trama EAPOL de la otra dirección MAC) se desactivará. El modo de host único se aplica solo para la topología de host a switch y cuando un host único está conectado a la capa 2 (puerto de acceso Ethernet) o al puerto de capa 3 (puerto enrutado) del APIC.

b) Modo de host múltiple: permite múltiples hosts por puerto, pero solo el primero se autentica. El puerto se mueve al estado autorizado después de la autorización exitosa del primer host. No se requiere que los hosts posteriores estén autorizados para obtener acceso a la red una vez que el puerto esté en el estado autorizado. Si el puerto queda sin autorización cuando falla la re-autenticación o se recibe un mensaje de cierre de sesión de EAPOL, a todos los hosts conectados se les niega el acceso a la red. La capacidad de la interfaz para apagarse en caso de violación de la asociación de seguridad se deshabilita en modo de host múltiple. Este modo es aplicable tanto para topologías de switch a switch como de host a switch.

c) Modo de autenticación múltiple: Permite que varios hosts y todos los hosts se autentiquen por separado.

d) Modo de dominio múltiple: Para datos separados y dominio de voz. Para usar con teléfonos IP.

ACI 802.1X admite los siguientes modos de autenticación:

a) EAP: El autenticador envía un marco EAP de solicitud/identidad al solicitante para solicitar su identidad (por lo general, el autenticador envía un marco de solicitud/identidad inicial seguido de una o más solicitudes de información de autenticación). Cuando el solicitante recibe la trama, responde con una trama EAP de solicitud/identidad.

b) MAB: La omisión de autenticación de MAC (MAB) se admite como modo de autenticación alternativa. MAB habilita el control de acceso basado en el puerto utilizando la dirección MAC del punto final. Un puerto habilitado para MAB se puede habilitar o deshabilitar dinámicamente en función de la dirección MAC del dispositivo que se conecta a él. Antes de MAB, la identidad del punto final es desconocida y todo el tráfico está bloqueado. El switch examina un solo paquete para aprender y autenticar la dirección MAC de origen. Una vez que MAB tiene éxito, se conoce la identidad del punto final y se permite todo el tráfico de ese punto final. El switch realiza el filtrado de la dirección MAC de origen para ayudar a garantizar que solo el punto final autenticado por MAB pueda enviar tráfico.

La autenticación basada en el puerto por el estándar IEEE 802.1X tiene las siguientes pautas y limitaciones de configuración:

a) Cisco ACI admite la autenticación 802.1X solo en puertos físicos.

b) Cisco ACI no admite la autenticación 802.1X en “port channels” o subinterfaces.

c) Cisco ACI admite la autenticación 802.1X a los miembros de un “port channel” pero no en el “port channel” en sí.

d) Los puertos miembros con y sin configuración 802.1X pueden coexistir en un “port channel”. Sin embargo, debe asegurarse de que la configuración 802.1X sea idéntica en todos los puertos miembros para que la canalización funcione con 802.1X

e) Cuando habilita la autenticación 802.1X, los solicitantes se autentican antes de que cualquier otra característica de Capa 2 o Capa 3 se habilite en una interfaz Ethernet.

f) 802.1X solo se admite en un chasis tipo “leaf” que es de tipo EX o FX.

g) 802.1X solo es compatible con los puertos de acceso de Fabric. 802.1X no es compatible con “port channels” o “Virtual-Port-Channels”.

h) IPv6 no es compatible con clientes dot1x en la versión 3.2 (1).

i) Si bien la actualización a versiones anteriores (downgrade), especialmente en los casos en que ciertas configuraciones de interfaz (modo de host y tipo de autenticación) no son compatibles en esa versión, el tipo de autenticación dot1x por defecto es ninguno. El modo de host debería reconfigurarse manualmente para un host único / host múltiple, según lo que se desee. Esto garantiza que el usuario configure solo los tipos de autenticación admitidos en esa versión y no se encuentre con escenarios no compatibles.

j) Multi-Auth admite 1 cliente de voz y varios clientes de datos (todos pertenecientes a los mismos datos vlan/epg).

k) Fail-epg/vlan bajo la política de autenticación de nodo 802.1X es una configuración obligatoria.

l) Multi-dominio de más de 1 cliente de voz y 1 cliente de datos pone el puerto en estado de seguridad deshabilitado.

m) Las siguientes plataformas no son compatibles con 802.1X:

i. N9K-C9396PX

ii. N9K-M12PQ

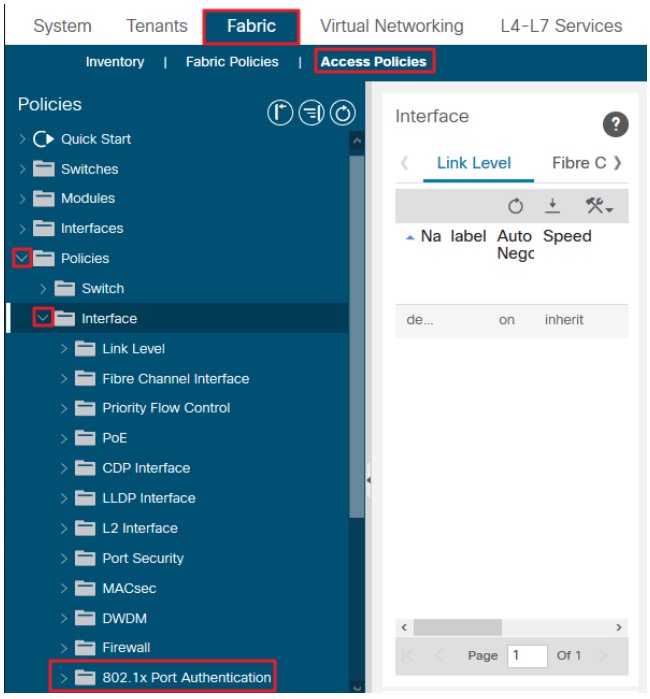
iii. N9K-C93128TX

iv. N9K-M12PQ

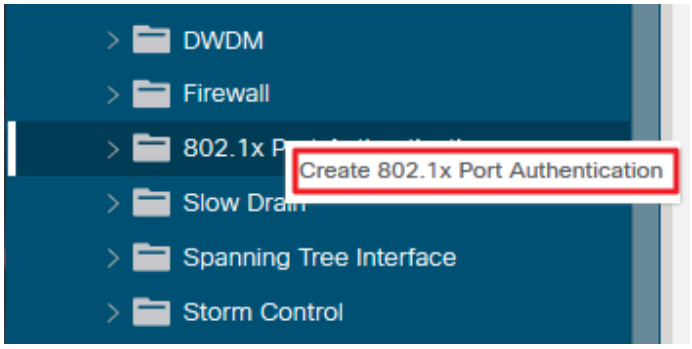
7.3.1 CONFIGURACIÓN DE AUTENTICACIÓN DE PUERTO 802.1X UTILIZANDO LA GUI APIC

Para realizar esta configuración en la GUI Cisco APIC, deberá poseer de un servidor RADIUS y configurar una política para el mismo.

a) En la barra de menú, haga clic en “Fabric”>”Access Policies” y despliegue los menús ”Policies”>”Interface”, entonces seleccione “802.1x Port Authentication” y realice las siguientes acciones:



i. Haga clic con el botón derecho en “802.1x Port Authentication“ y pulse en “Create 802.1x Port Authentication”.



ii. En el campo “Name”, ingrese un nombre para la política.

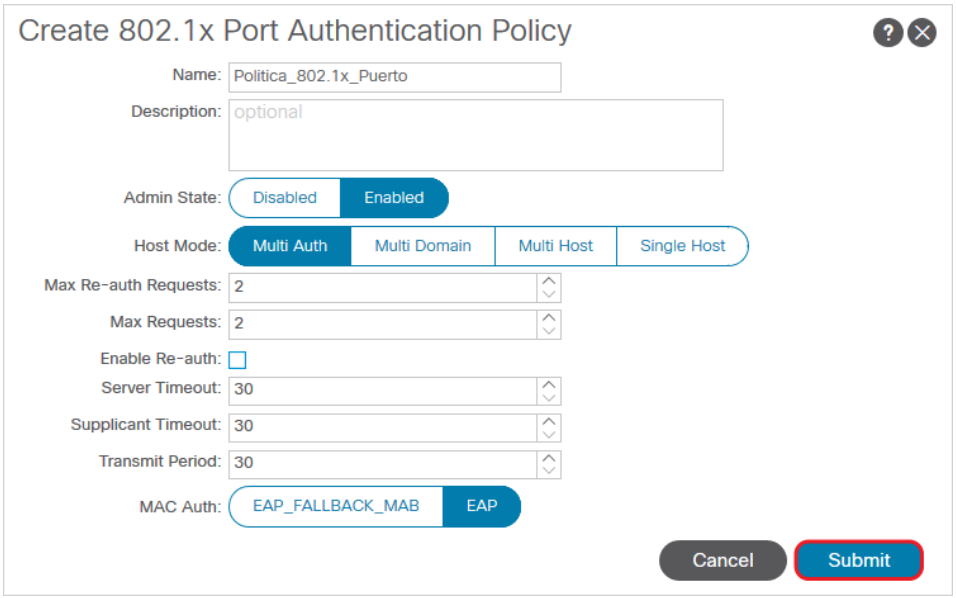
iii. En el campo “Modo de host”, seleccione el modo de política. Los modos son:

- Multi Auth: para permitir múltiples hosts y todos los hosts se autentican por separado.

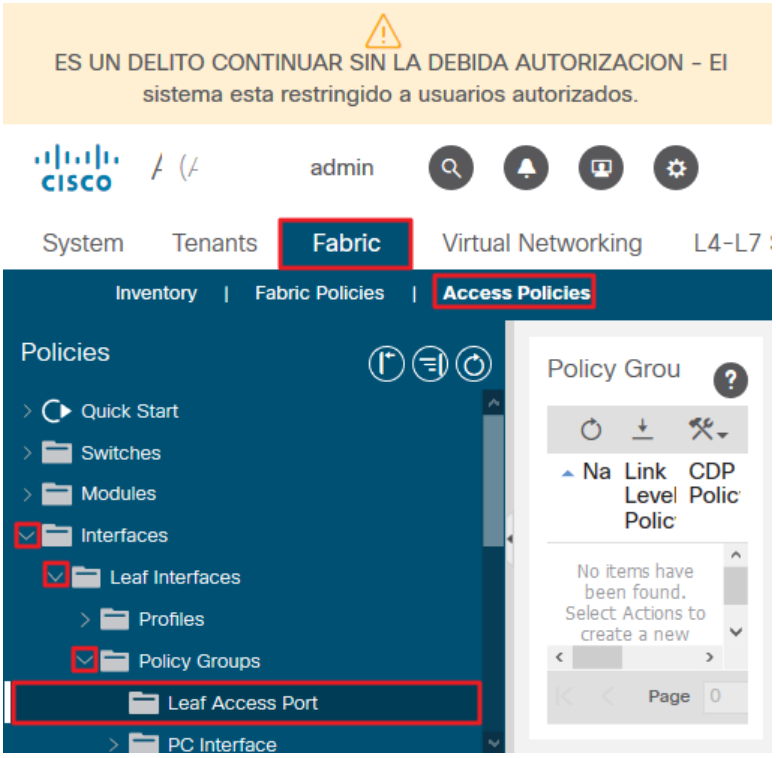
Nota: Cada host debe tener la misma información EPG / VLAN.

- Multi Domain: para datos separados y dominio de voz. Para usar con teléfonos IP.
- Multi host: para permitir múltiples hosts por puerto, pero solo el primero se autentica.
- Single Host: para permitir solo un host por puerto.

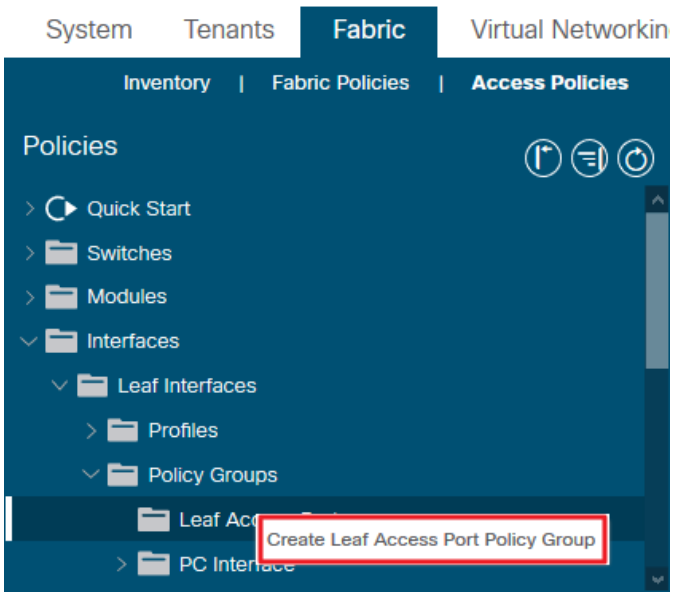
iv. Si el dispositivo no es compatible con 802.1X, en el campo “MAC Auth” , deberá seleccionar “EAP_FALLBACK_MAB”. Para finalizar pulse “Submit”.



b) Para asociar la Política de autenticación de puerto 802.1X a un Grupo de acceso de Fabric, vaya a “Fabric”>”Access Policies” y despliegue los siguientes menús ”Interfaces”>”Leaf Interfaces”>”Policy Groups”. Seleccione ”Leaf Access Port” y realice las siguientes acciones:

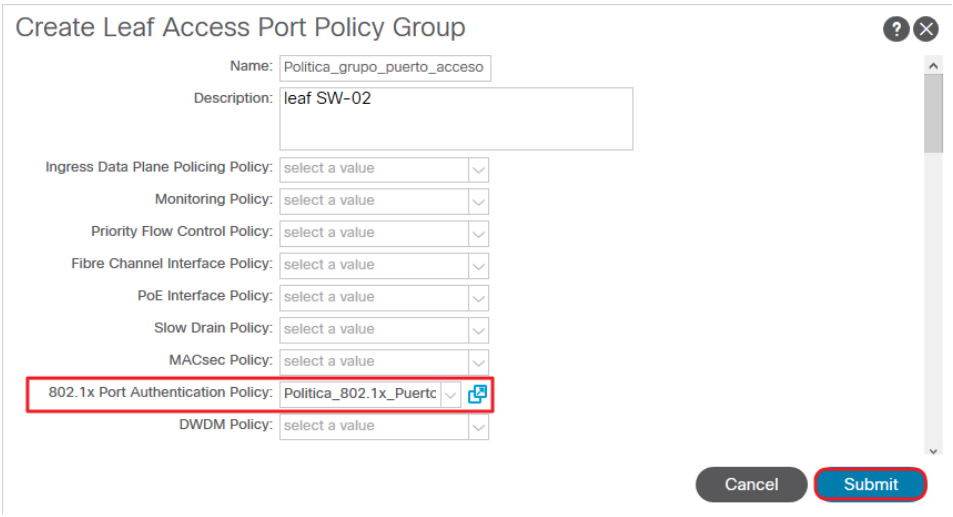


i. Haga clic derecho en “Leaf Access Port”, para abrir “Create Leaf Access Port Policy Group”.



ii. En el campo “Name”, ingrese un nombre para la política.

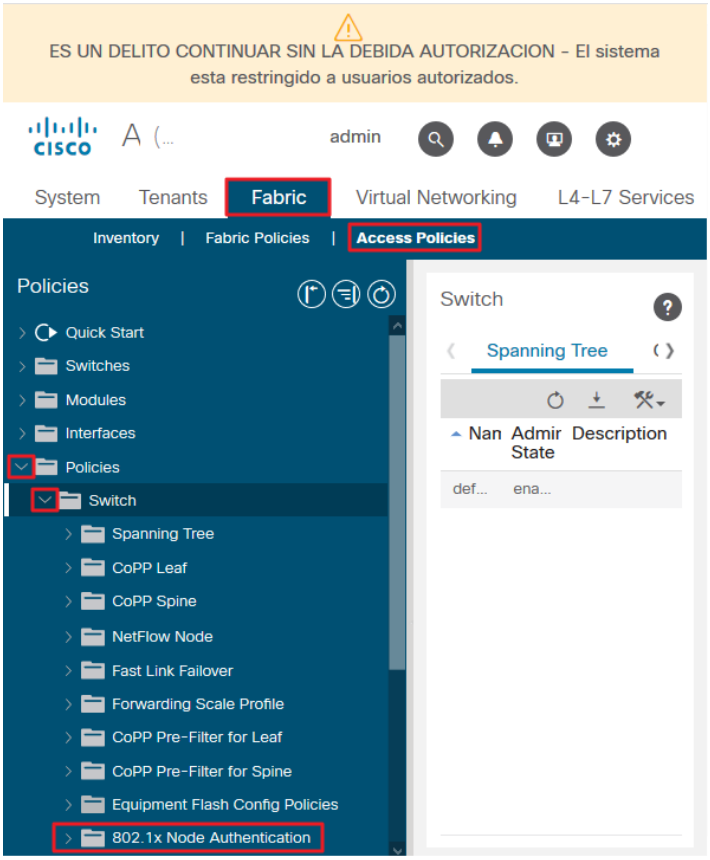
iii. En el campo “802.1x Port Authentication Policy”, seleccione la política creada anteriormente y haga clic en “Submit”.



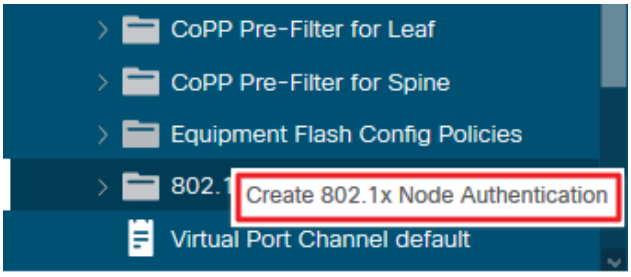
7.3.2 CONFIGURACIÓN DE AUTENTICACIÓN DE NODO 802.1X UTILIZANDO LA GUI APIC

Para realizar esta configuración con la GUI Cisco APIC, deberá poseer de un servidor RADIUS y configurar una política para el mismo.

a) En la barra de menú, haga clic en “Fabric”>”Access Policies” y despliegue los menús ”Policies”>”Switch”, entonces seleccione “802.1x Node Authentication” y realice las siguientes acciones:



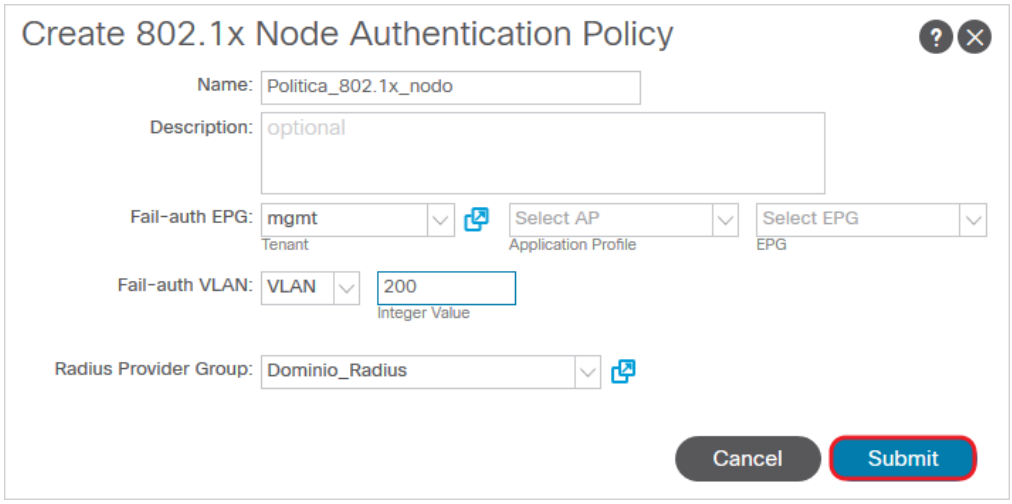
i. Haga clic con el botón derecho en “802.1x Node Authentication“ y pulse en “Create 802.1x Node Authentication”.



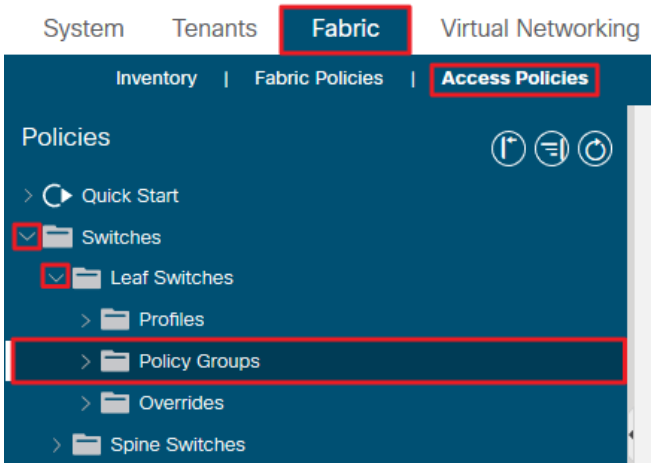
ii. En el campo “Name”, ingrese un nombre para la política.

iii. En el campo “Fail-auth EPG”, seleccione el “tenant”, el perfil de la aplicación y el EPG para implementar en caso de autenticación fallida.

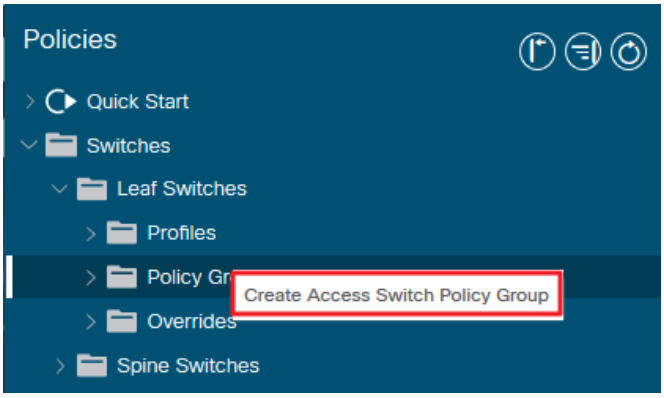
iv. En “Fail-auth VLAN”, seleccione la VLAN para implementar en caso de autenticación fallida.



b) Para asociar la Política de autenticación de nodo 802.1X a un Grupo de políticas de leaf switch, diríjase a “Fabric”>”Access Policies”>”Switches”>”leaf switches”>”Policy Groups” y realice las siguientes acciones:

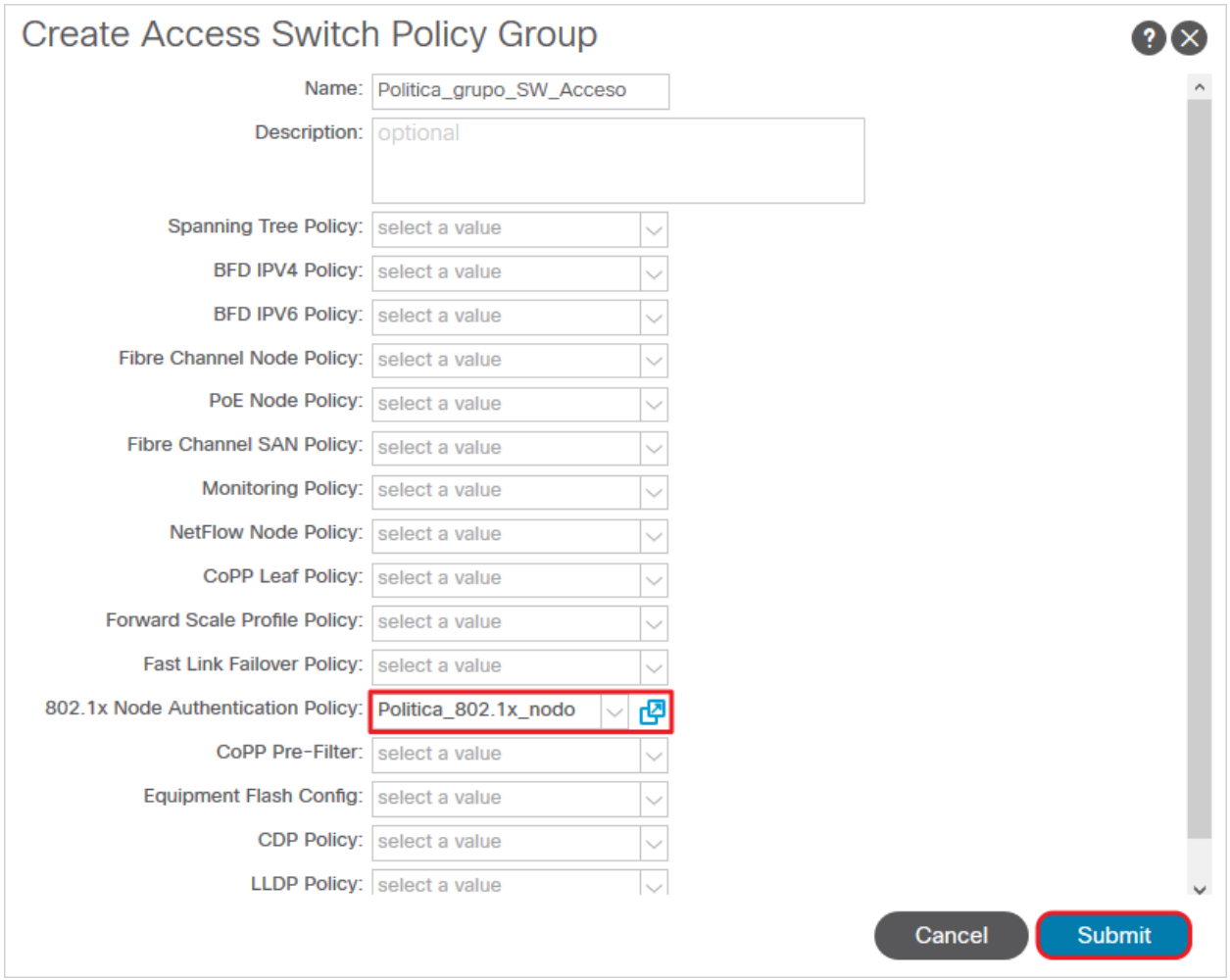


i. Haga clic derecho en “Policy Groups” y seleccione “Create Access Switch Policy Group”.

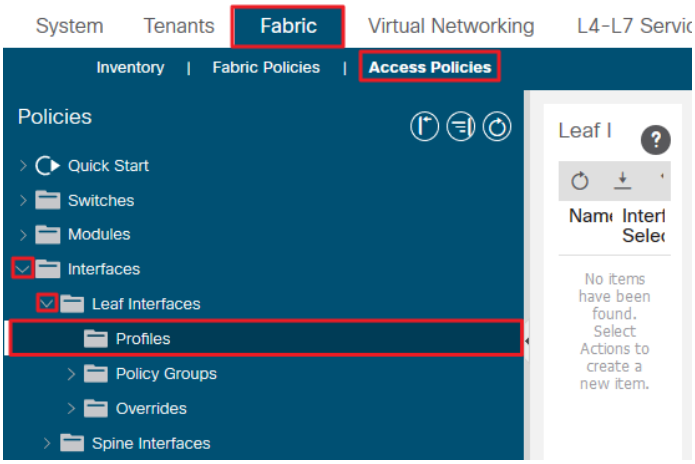


ii. En el campo “Name”, ingrese un nombre para la política.

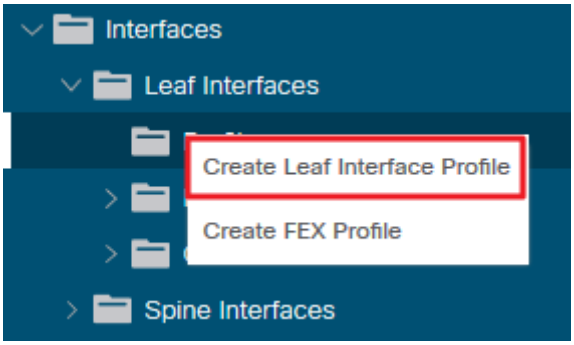
iii. En el campo “802.1X Node Authentication Policy”, seleccione la política creada anteriormente y haga clic en “Submit”.



c) Para asociar la política de autenticación de nodo 802.1X a un perfil de interfaz leaf switch, diríjase a “Fabric”>”Access Policies” y despliegue los siguientes menús: ”Interfaces”>”Leaf Interfaces”. Seleccione “Profiles” y realice las siguientes acciones:



i. Haga clic derecho en “Profiles” y seleccione “Create Leaf Interface Profile”.



ii. En el campo “Name”, ingrese un nombre para la política. Y pulse el icono “+”

iii. Se abrirá el cuadro de diálogo “Create Access Port Selector” donde deberá ingresar la información de Nombre e ID de interfaz.

iv. En el campo “Interface Policy Group”, seleccione la política creada previamente y haga clic en “OK” y posteriormente “Submit”.

7.4 SEGURIDAD DE PUERTOS

La función de seguridad del puerto protege el entramado ACI de ser inundado con direcciones MAC desconocidas al limitar el número de direcciones MAC aprendidas por puerto. El soporte de la función de seguridad de puertos está disponible para puertos físicos, canales de puertos (port channels) y canales de puertos virtuales (virtual port channels).

7.4.1 PORT SECURITY A NIVEL DE PUERTO

En el APIC, el usuario puede configurar la seguridad del puerto (Port Security) en los puertos del switch. Una vez que el límite MAC ha excedido el valor máximo configurado en un puerto, se reenvía todo el tráfico de las direcciones MAC excedidas. Se admiten los siguientes atributos:

a) Port Security Timeout: el rango actual admitido para el valor de tiempo de espera es de 60 a 3600 segundos.

b) Violation Action: la acción de infracción está disponible en modo de protección. En el modo de protección, el aprendizaje MAC está deshabilitado y las direcciones MAC no se agregan a la tabla CAM. El aprendizaje de Mac se vuelve a habilitar después del valor de tiempo de espera configurado.

c) Maximum Endpoints: El rango admitido actual para el valor configurado de puntos finales máximos es de 0 a 12000. Si el valor máximo de puntos finales es 0, la política de seguridad del puerto está deshabilitada en ese puerto.

Las pautas y restricciones para la correcta configuración son las siguientes:

a) La seguridad del puerto se configura en el puerto.

b) La seguridad de puertos es compatible con puertos físicos, canales de puertos y canales de puertos virtuales (vPC).

c) Se admiten direcciones MAC estáticas y dinámicas.

d) Los movimientos de direcciones MAC (MAC MOVE) son compatibles desde puertos seguros a puertos no seguros y desde puertos no seguros a puertos seguros.

e) El límite de la dirección MAC se aplica solo en la dirección MAC y no se aplica en una dirección MAC e IP.

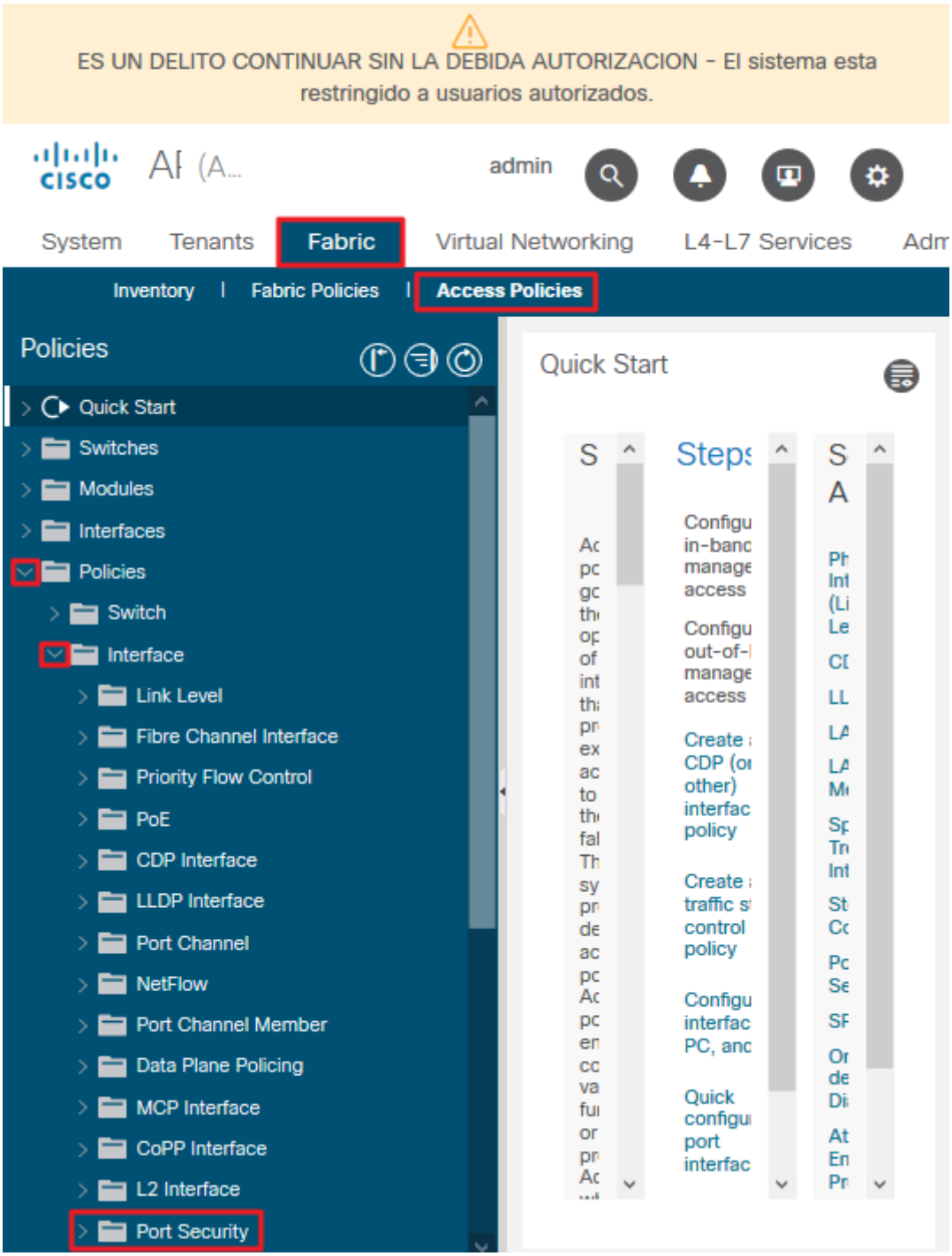
f) La seguridad del puerto no es compatible con Fabric Extender (FEX).

7.4.2 CONFIGURACIÓN DE PUERTOS DE SEGURIDAD USANDO LA GUI APIC

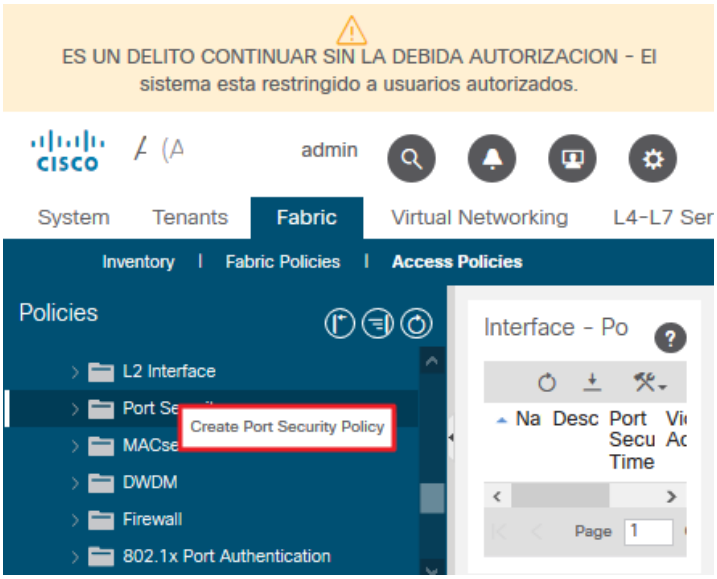
Antes de empezar, se debe tener configurado un “tenant” y un “bridge domain”.

Para ello se deberán seguir los siguientes pasos:

En la barra de menú, haga clic en “Fabric”>“Access Policies” y, en el panel de navegación, expanda “Policies”>”Interface”>”Port security”.



a) Haga clic con el botón derecho en “Port Security” y haga clic en “Create Port Security Policy”.



b) En el cuadro de diálogo “Create Port Security Policy”, realice las siguientes acciones:

i. En el campo “Name”, ingrese un nombre para la política.

ii. En el campo “Port Security Timeout”, elija el valor deseado para el tiempo de espera antes de volver a habilitar el aprendizaje MAC en una interfaz.

iii. En el campo “Maximum Endpoints”, elija el valor deseado para el número máximo de puntos finales que se pueden aprender en una interfaz.

iv. En el campo “Violation Action”, la opción disponible es proteger (protect). Posteriormente pulse “Submit”.

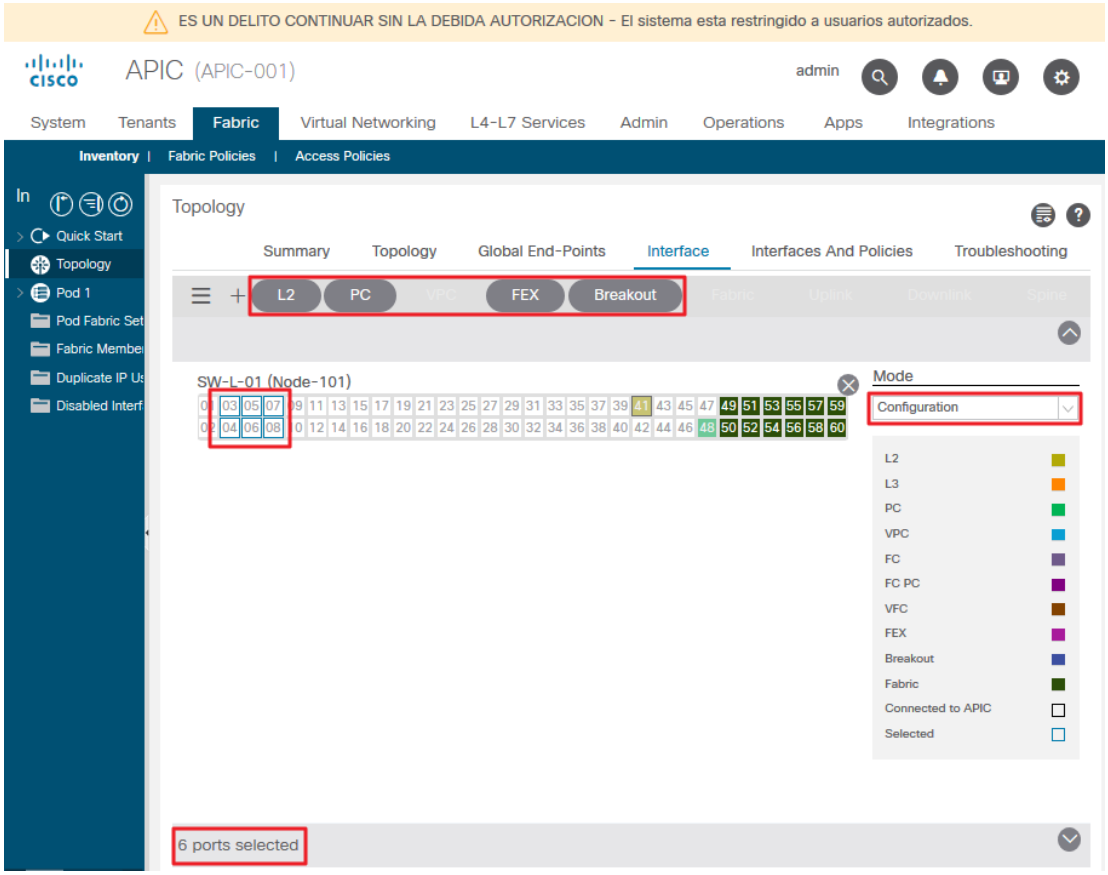
c) Antes de continuar deberá comprobar las siguientes configuraciones

i. El fabric de ACI está instalado, los controladores APIC están en línea y el clúster APIC está formado y en buen estado.

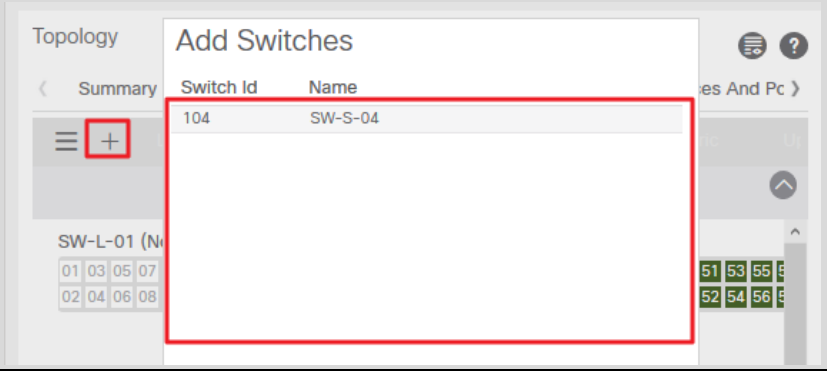
ii. Hay disponible una cuenta de administrador de fabric APIC que permitirá crear las configuraciones de infraestructura de fabric necesarias.

iii. Los leaf switch de destino están registrados en el ACI fabric y están disponibles.

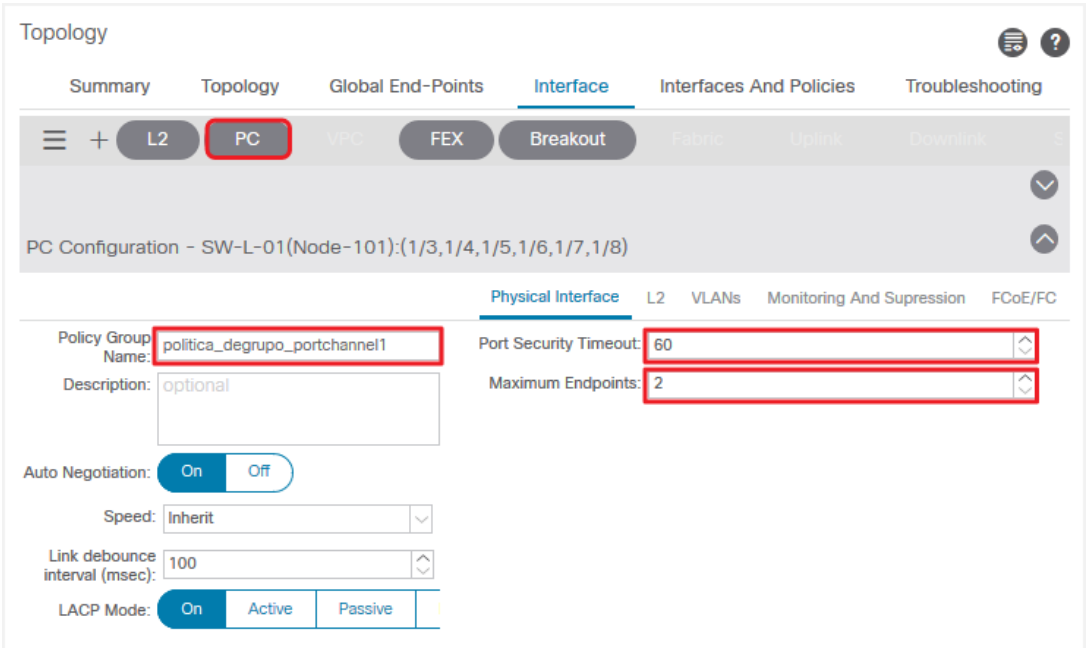
d) Una vez comprobadas esas configuraciones, en el panel de navegación, haga clic en "Fabric">"Inventory">"Topology" y seleccione "Interface" donde deberá escoger el modo configuración en el apartado "Mode" seleccionando "Configuration" y seleccionar las interfaces deseadas. Aparecerán varias opciones de configuración para esos puertos en gris oscuro en la parte superior de la representación del switch (L2, PC, FEX, etc). Seleccione el que más se adapte a su configuración.



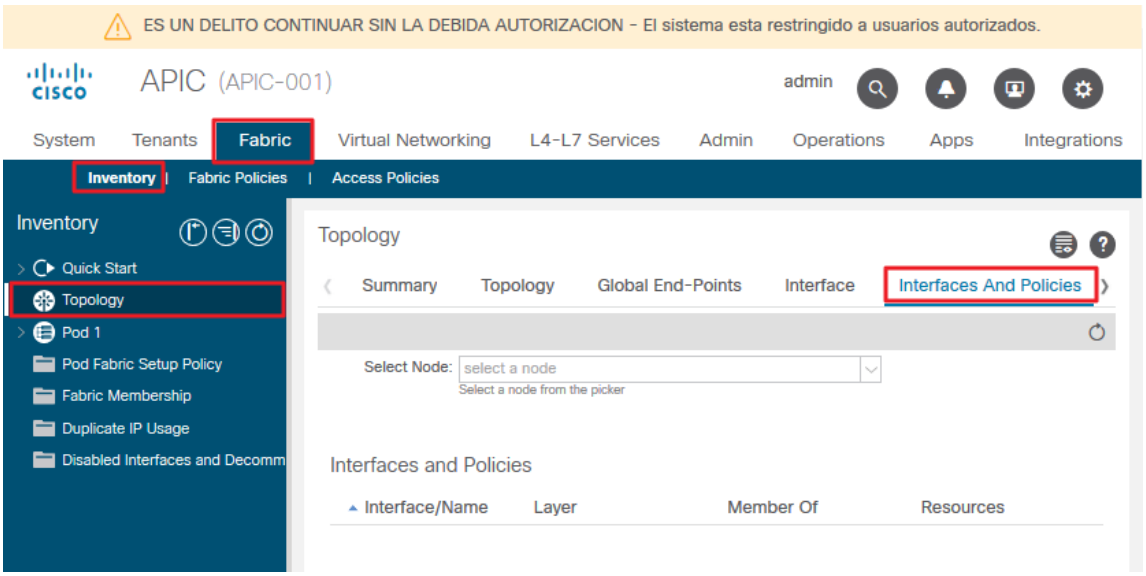
Nota: Si no se mostrara la representación gráfica del switch deseado, pulse en el icono "+" y agregue el switch.



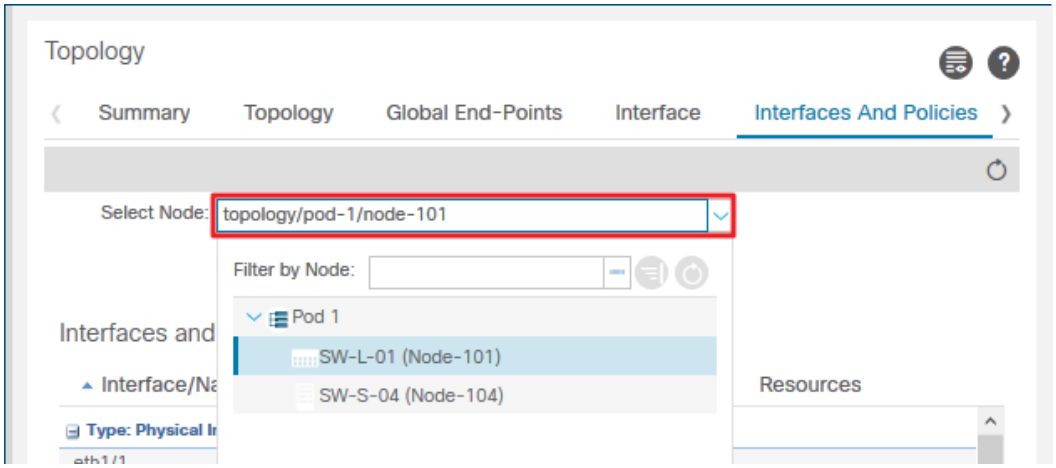
e) En el siguiente ejemplo se ha escogido la configuración de puertos “PC” (Port Channel). Inmediatamente después de pulsar la opción escogida, en este ejemplo “PC”, se mostrará un menú de configuración donde habrá que configurar previamente una política de grupo (solo en port channel) y configurar los parámetros de “Port Security Timeout” y “Maximum Endpoint” acorde a los configurados en la política de seguridad de puerto creada anteriormente. Cuando finalice pulse “Submit”.



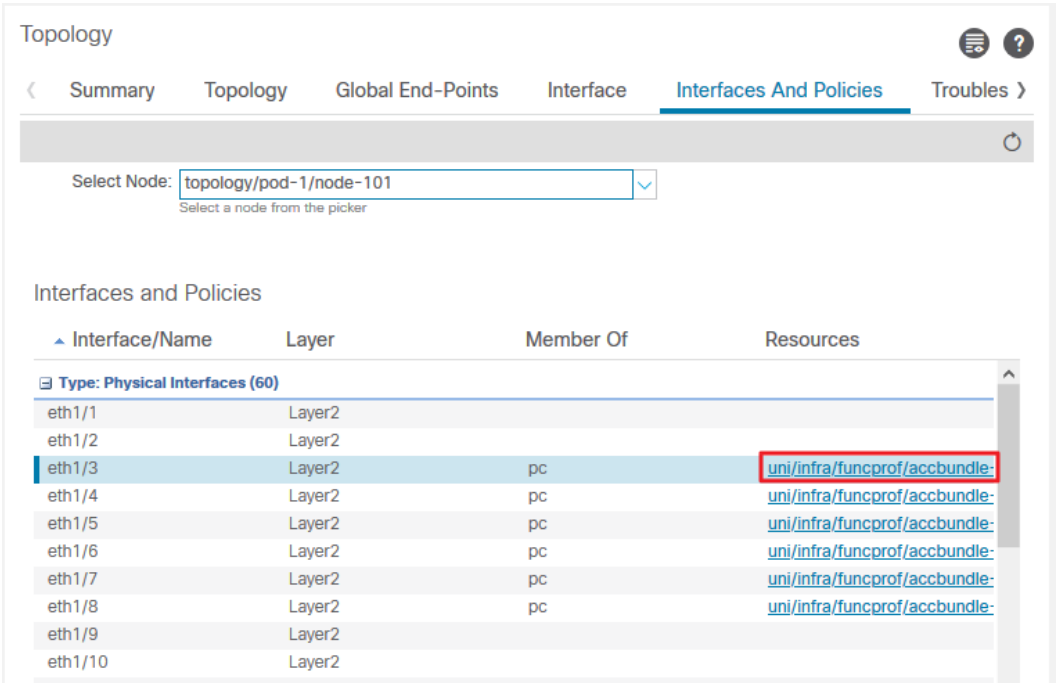
f) Una vez comprobadas esas configuraciones, en el panel de navegación, haga clic en “Fabric”>”Inventory”>”Topology” y seleccione “Interfaces And Policies”



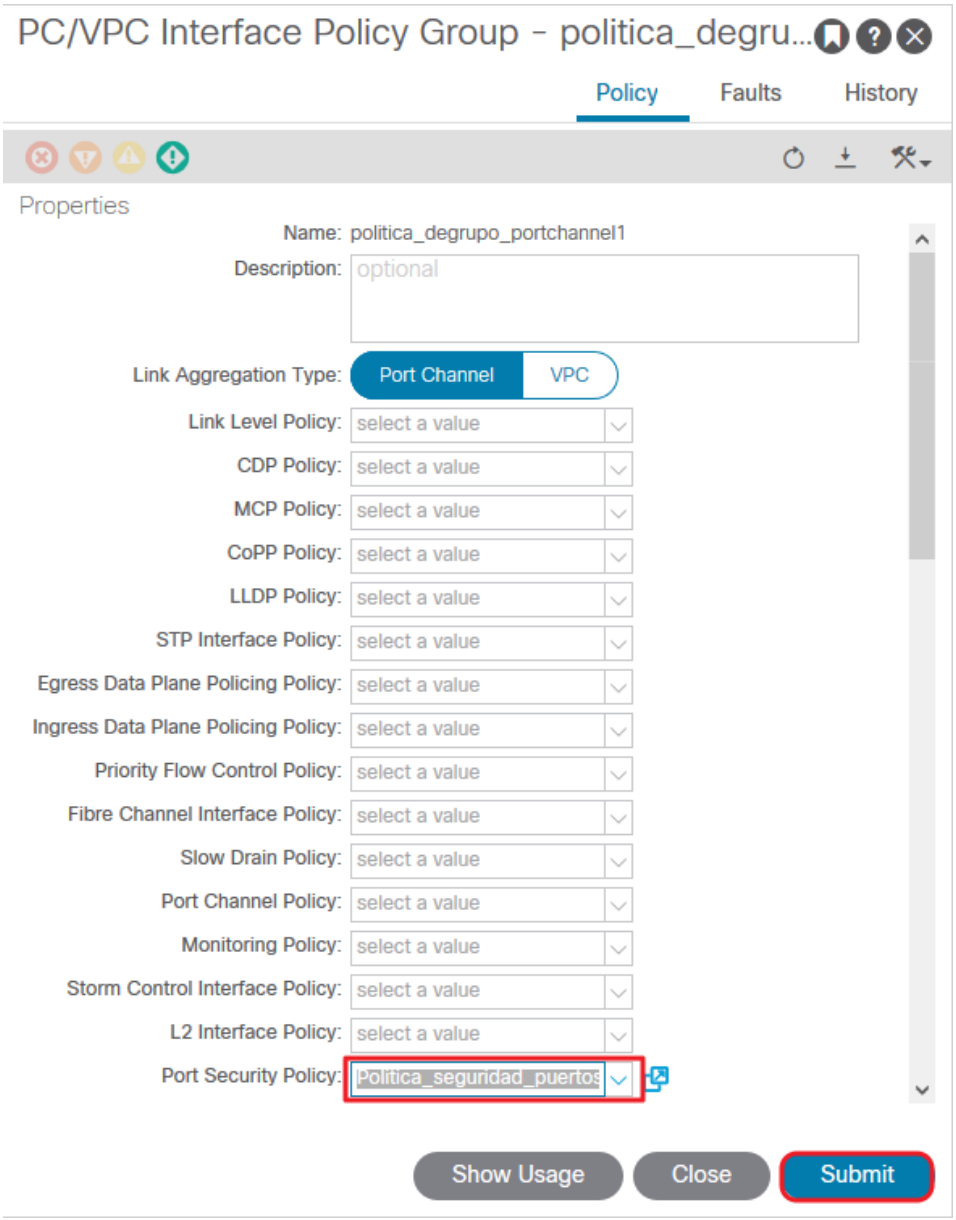
g) En el apartado “Select Node” selecciona el nodo y el switch a configurar



h) Elija el puerto apropiado para configurar la interfaz, y pulse sobre la ruta que aparece en el campo “Resources”



i) En la ventana emergente que aparecerá, deberá situarse en el apartado “Port Security Policy” y seleccionar la política creada anteriormente. Pulse “Submit” para finalizar



7.5 SEGURIDAD L2 (FHS)

Las características de first hop security (FHS) permiten una mejor seguridad y administración de enlaces IPv4 e IPv6 sobre los enlaces de capa 2. En un entorno de proveedor de servicios, estas características controlan estrechamente la asignación de direcciones y las operaciones derivadas, como la detección de direcciones duplicadas (DAD) y la resolución de direcciones (AR).

Las siguientes funciones compatibles de FHS protegen los protocolos y ayudan a construir una base de datos "endpoint" segura en la fabric de los switches leafs, que se utilizan para mitigar las amenazas de seguridad como los ataques MIM y los secuestros de IP:

a) Inspección ARP: permite que un administrador de red intercepte, registre y descarte paquetes ARP con enlaces MAC a direcciones IP no válidas.

b) Inspección ND: aprende y asegura los enlaces para las direcciones de autoconfiguración sin estado en las tablas vecinas de Capa 2.

c) Inspección DHCP: valida los mensajes DHCP recibidos de fuentes no confiables y filtra los mensajes no válidos.

d) RA Guard: permite que el administrador de la red bloquee o rechace los mensajes no deseados o no autorizados del anuncio de enrutador (RA) guard.

e) IPv4 e IPv6 Source Guard: bloquea el tráfico de datos de una fuente desconocida.

f) Control de confianza: una fuente confiable es un dispositivo que está bajo su control administrativo. Estos dispositivos incluyen los switches, enrutadores y servidores en el Fabric. Cualquier dispositivo más allá del firewall o fuera de la red es una fuente no confiable. En general, los puertos host se tratan como fuentes no confiables.

Las características de FHS proporcionan las siguientes medidas de seguridad:

a) Cumplimiento de roles: evita que los hosts no confiables envíen mensajes que están fuera del alcance de su rol.

b) Cumplimiento obligatorio: evita el robo de direcciones.

c) Mitigaciones de ataque DoS: evita puntos finales maliciosos para hacer crecer la base de datos de punto final hasta el punto en que la base de datos podría dejar de proporcionar servicios operativos.

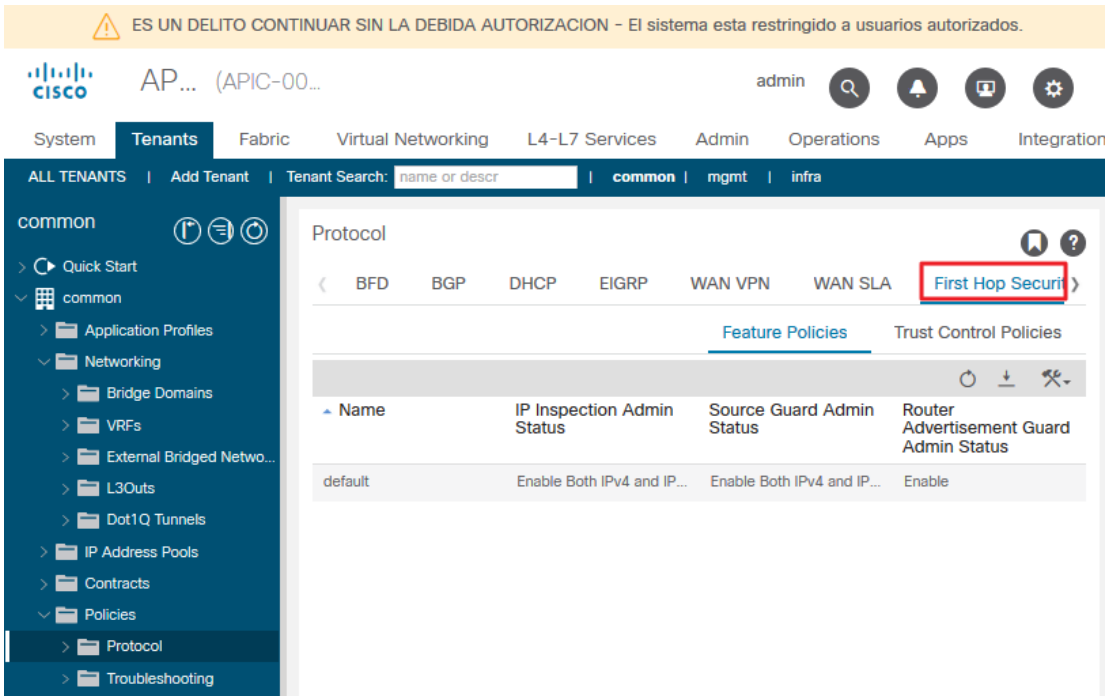
d) Servicios de proxy: proporciona algunos servicios de proxy para aumentar la eficiencia de la resolución de direcciones.

Las funciones de FHS se habilitan en función del dominio del tenant (BD). Como el bridge domain, puede implementarse en un solo leaf switch o en varios, los mecanismos de mitigación y control de amenazas del FHS se adaptan a un solo switch y a múltiples switch escenarios.

7.5.1 IMPLEMENTACION DE ACI FHS

La mayoría de las funciones de FHS se configuran en dos pasos: en primer lugar, define una política que describe el comportamiento de la función, en segundo lugar, aplica esta política a un "dominio" (que es el tenant bridge domain o el tenant “endpoint” group). Se pueden aplicar diferentes políticas que definen diferentes comportamientos a diferentes dominios que se cruzan. La decisión de usar una política específica la toma el dominio más específico al que se aplica la política.

Las opciones de política se pueden definir desde la GUI APIC de Cisco que se encuentra en la pestaña Nombre del Tenant>Policies>Protocol>First Hop Security.



7.5.2 PAUTAS Y LIMITACIONES

Se describen las pautas a seguir y las limitaciones existentes en la tecnología:

a) A partir de la versión 3.1 (1), FHS es compatible con “endpoints” virtuales (solo AVS).

b) FHS es compatible con la encapsulación VLAN y VXLAN.

c) Cualquier “endpoint” asegurado en la base de datos de la tabla de enlace de FHS en estado DOWN se borrará después de 18 horas de tiempo de espera. La entrada se mueve al estado DOWN cuando el puerto del panel frontal donde está la entrada aprendida, el enlace está en estado DOWN. Durante esta ventana de 18 horas, si el “endopint” se mueve a una ubicación diferente y se ve en un puerto diferente, la entrada se moverá del estado DOWN a REACHABLE / STALE, siempre que el “endpoint” sea accesible desde el otro puerto desde el que se mueve.

d) Cuando IP Source Guard está habilitado, el tráfico IPv6 que se origina usando la dirección IPv6 Link Local como dirección de origen IP no está sujeto a la aplicación IP Source Guard (es decir, cumplimiento de Source Mac <=> enlaces de IP de origen asegurados por la función de inspección IP). Este tráfico está permitido de manera predeterminada, independientemente de los fallos de verificación vinculantes.

e) FHS no es compatible con las interfaces L3Out.

f) FHS no es compatible con TOR basados en N9K-M12PQ.

g) FHS en ACI Multi-Site es una capacidad local del sitio, por lo tanto, solo se puede habilitar en un sitio desde el clúster APIC. Además, FHS en ACI Multi-Site solo funciona cuando BD y EPG es local y no se extiende a través de los sitios. La seguridad de FHS no se puede habilitar para BD o EPG extendidos.

h) FHS no es compatible con un “bridge domain” de capa 2 solamente.

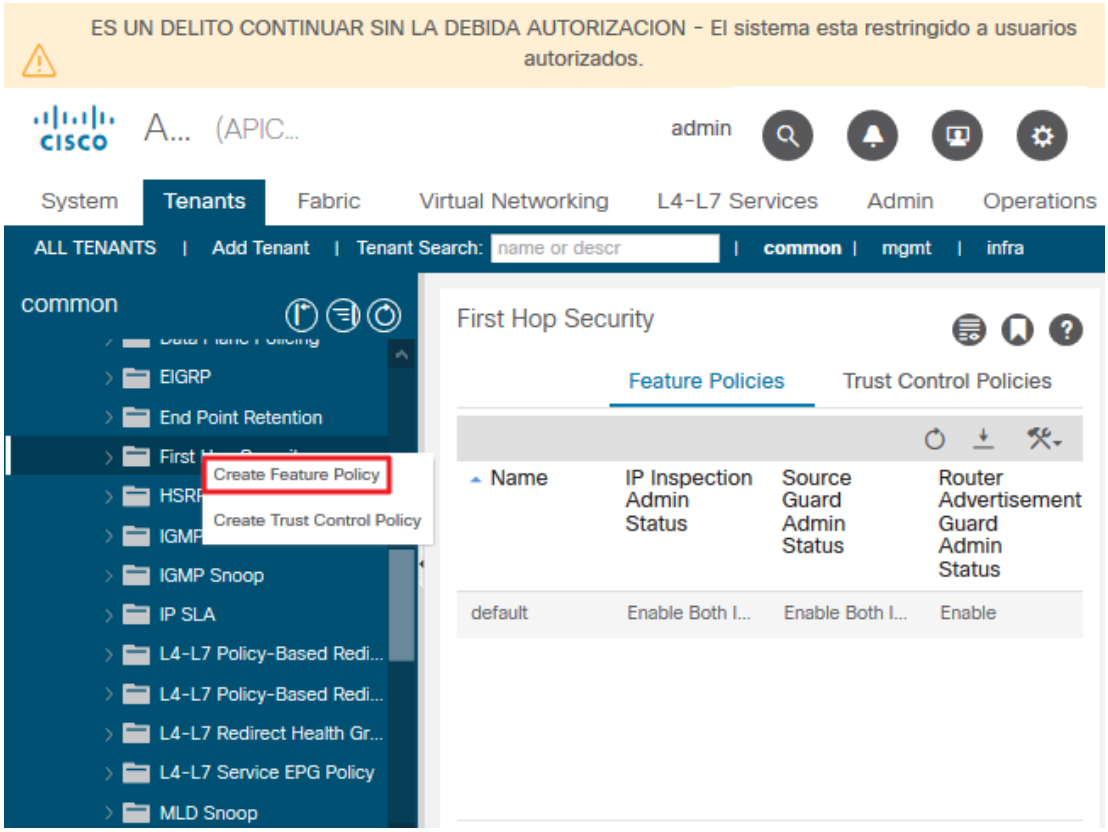
i) La activación de la función FHS puede interrumpir el tráfico durante 50 segundos porque el EP en el BD se vacía y el aprendizaje EP en el BD se desactiva durante 50 segundos.

7.5.3 CONFIGURACIÓN DE FHS USANDO LA GUI APIC

Antes de empezar, se debe tener configurado un “tenant” y un “bridge domain”.

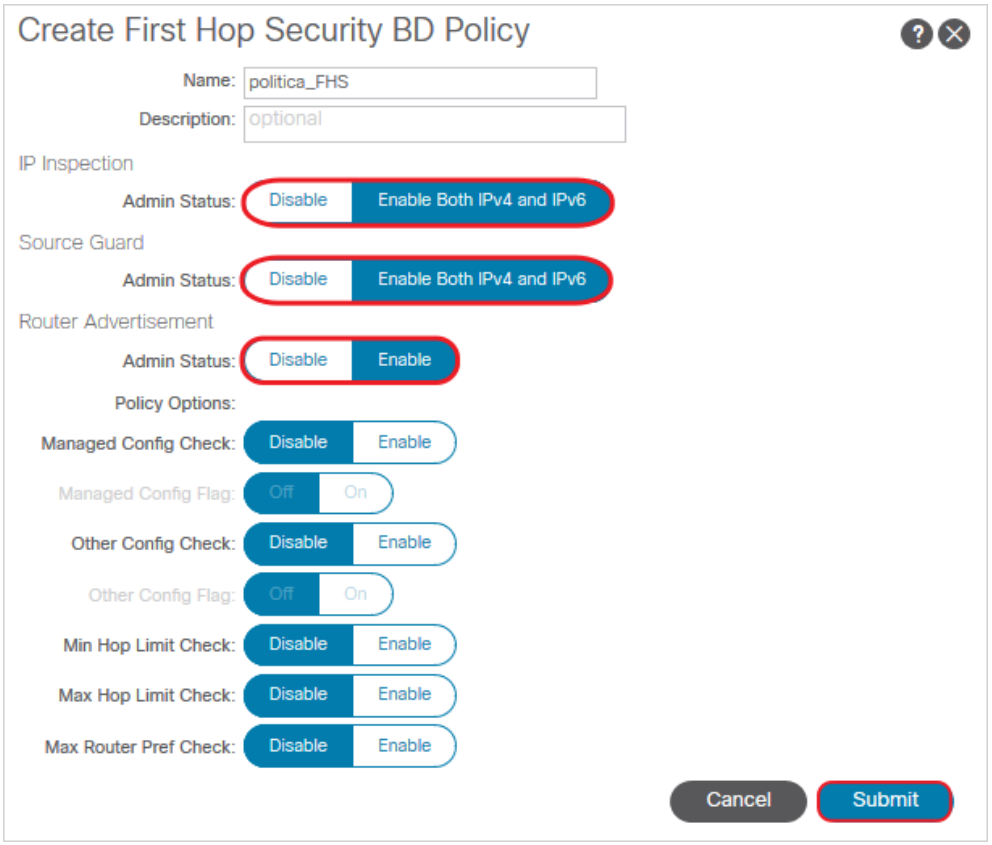
Para ello se deberán seguir los siguientes pasos:

a) En la barra de menú, haga clic en Tenants> Nombre_tenant. En el panel de navegación, haga clic en Policies> Protocol> First Hop Security. Haga clic derecho en First Hop Security para abrir Crear política de características y realizar las siguientes acciones:

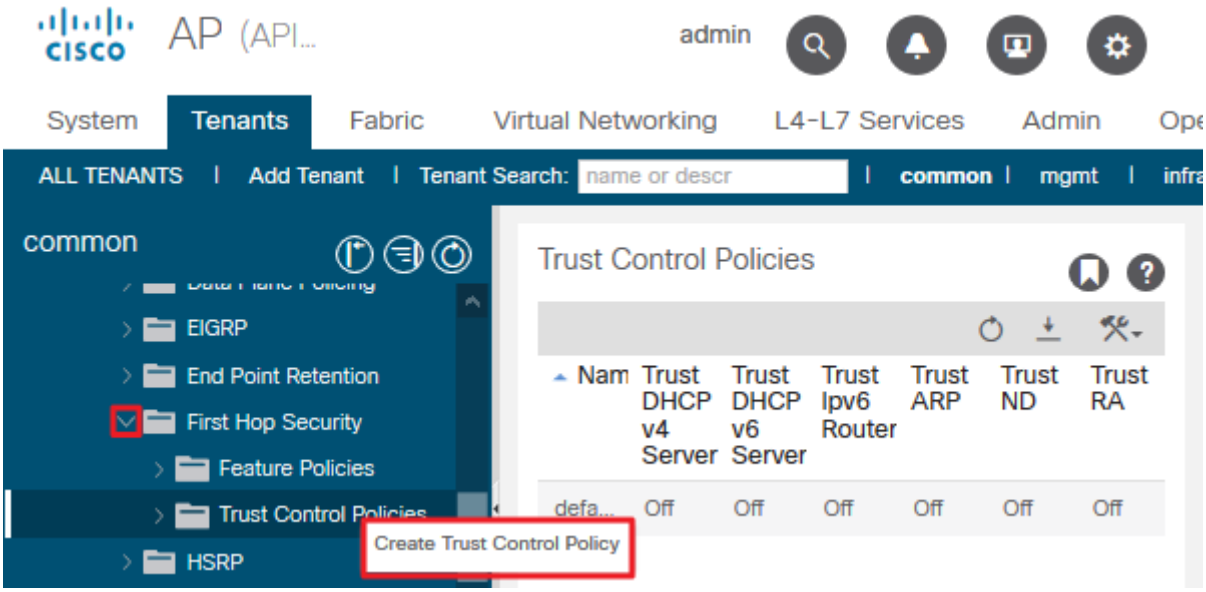


i. En el campo “Name”, ingrese un nombre para la política de seguridad del primer salto.

ii. Verifique que los campos “IP Inspection”, “Source Guard” y “Router Advertisement” estén habilitados, se deberán modificar los demás parámetros acorde a su organización, y finalmente pulse “Submit”.

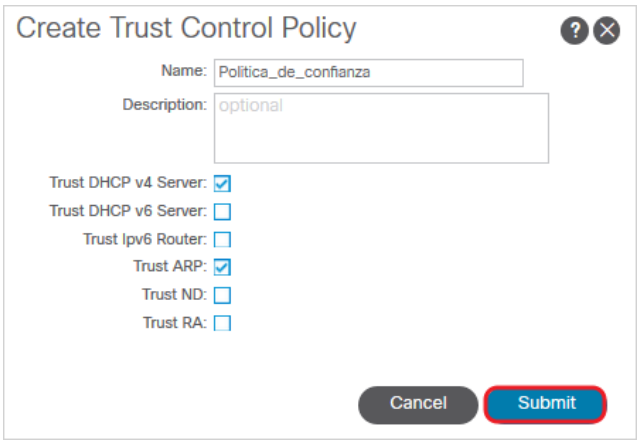


b) En el panel de navegación, expanda “First Hop Security” y haga clic con el botón derecho en “Trust Control Policies” para abrir “Create Trust Control Policy” y realizar las siguientes acciones:

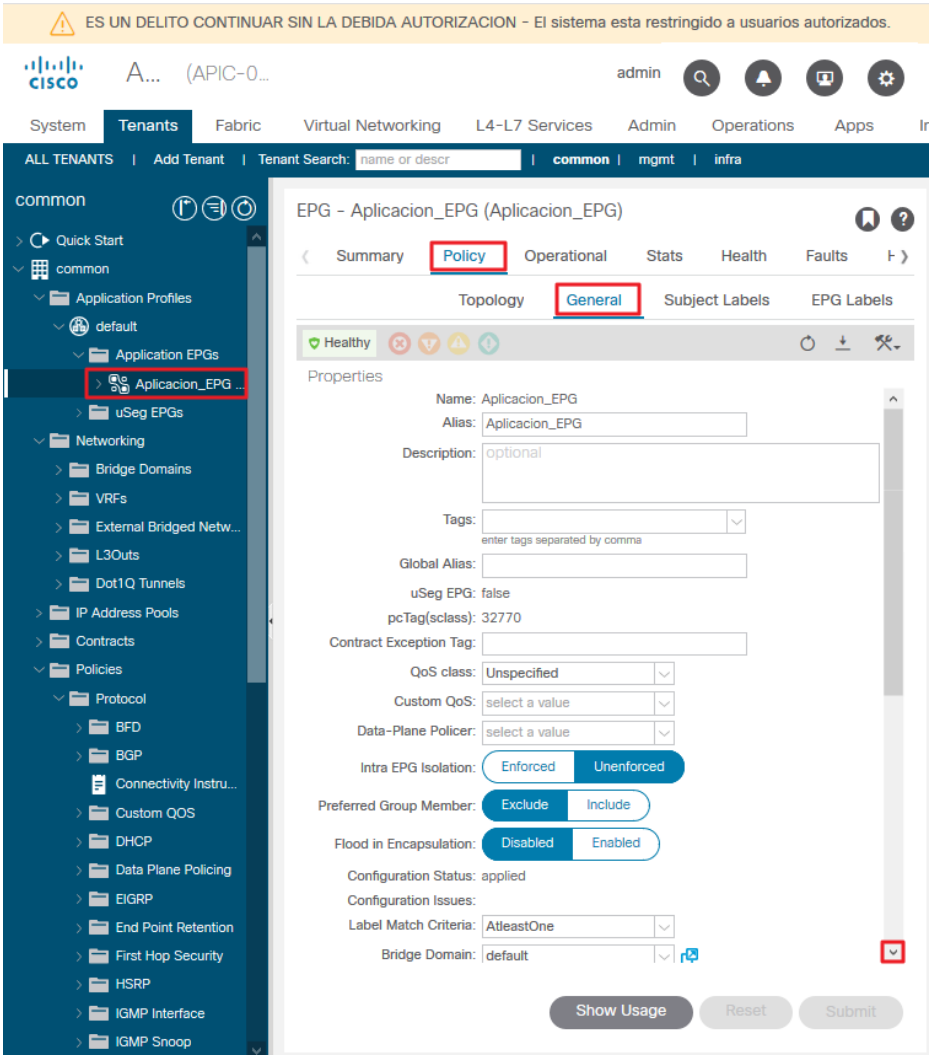


En el campo Nombre, ingrese un nombre para la política de Control de confianza.

Se deberán seleccionar las funciones deseadas que se permitirán en la política y haga clic en ”Submit”.

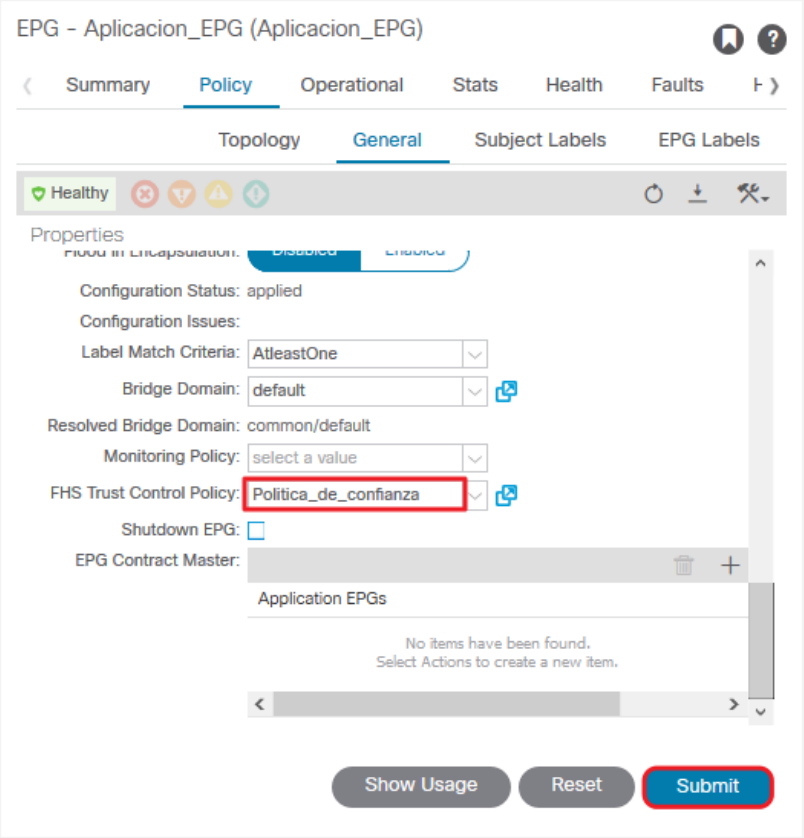


c) (Opcional) Para aplicar la política de Control de confianza a una EPG, en el panel de navegación, expanda “Aplication Profiles”> Nombre de perfil de aplicación> “ApplicationEPGs” y haga clic en Nombre de EPG de aplicación para realizar las siguientes acciones:

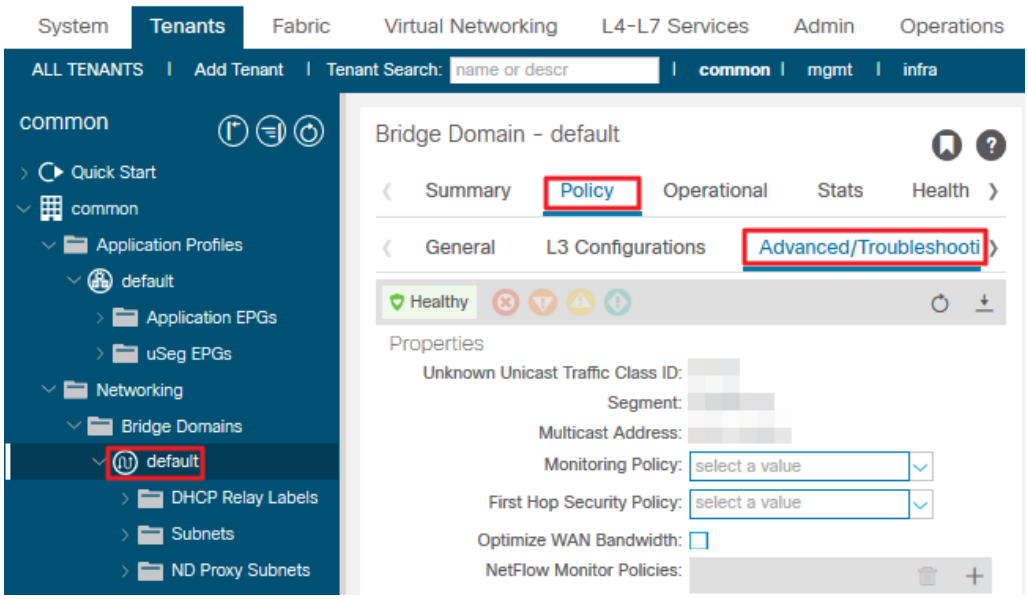


i. En el panel de trabajo, haga clic en la pestaña General

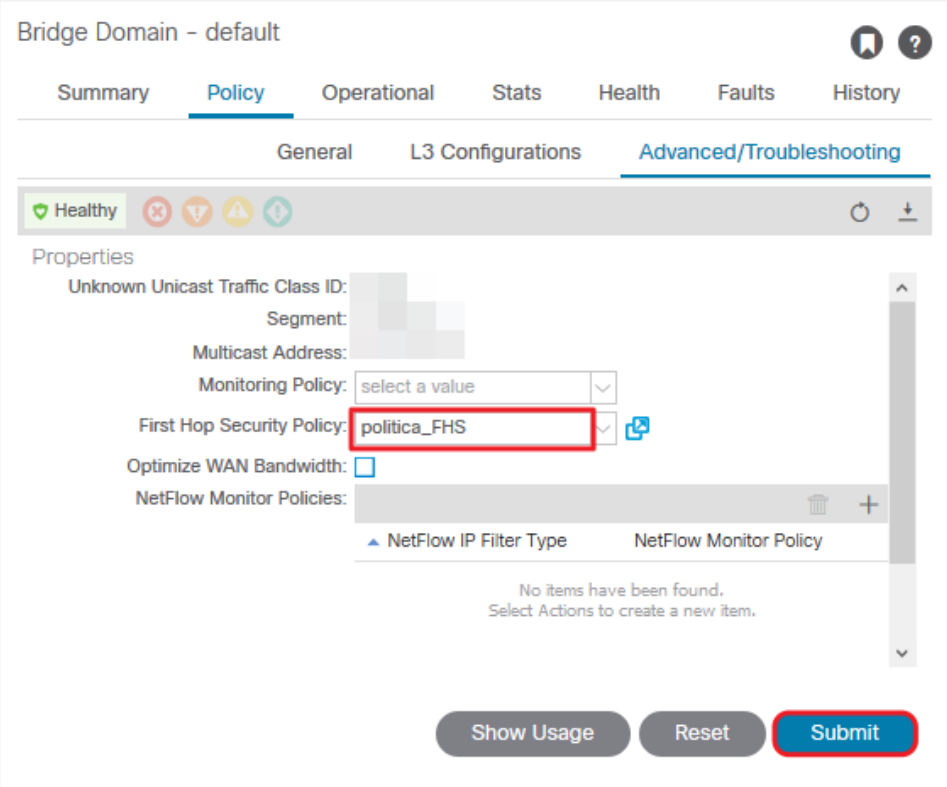
ii. Haga clic en la flecha hacia abajo para la Política de control de confianza de FHS y seleccione la política que creó anteriormente y haga clic en “Submit”.



d) En el panel de navegación, expanda “Networking”>Bridge domains”> Nombre del “Bridge Domain” y haga clic en la pestaña “Policy”>”Avanced/Troubleshooting” y realice la siguiente acción:



i. En el campo Política de “First Hop Security”, seleccione la política que acaba de crear y haga clic en “Submit”. Esto completa la configuración de FHS.



7.6 SEGURIDAD DE COOP Y EIGRP.

7.6.1 COOP

El Protocolo del Consejo de Oracle (COOP) se utiliza para comunicar la información de mapeo (ubicación e identidad) al spine proxy. Un leaf switch reenvía la información de la dirección del “endpoint” al spine switch 'Oracle' utilizando Zero Message Queue (ZMQ). COOP que se ejecuta en los nodos spine asegurará que todos los nodos spine mantengan una copia coherente de la dirección del “endpoint” y la información de ubicación y, además, mantendrá el depósito de la tabla hash distribuida (DHT) de la identidad del “endpoint” a la base de datos de mapeo de ubicación.

La comunicación de ruta de datos COOP proporciona alta prioridad al transporte mediante conexiones seguras. COOP se ha mejorado para aprovechar la opción MD5 para proteger los mensajes COOP de la inyección de tráfico malicioso. El controlador APIC y los switches admiten la autenticación del protocolo COOP.

El protocolo COOP se ha mejorado para admitir dos modos de autenticación ZMQ: estricto y compatible.

a) Modo estricto: COOP solo permite conexiones ZMQ autenticadas con MD5.

b) Modo compatible: COOP acepta conexiones ZMQ autenticadas y no autenticadas MD5 para el transporte de mensajes.

Para admitir la compatibilidad de autenticación COOP Zero Message Queue (ZMQ) en todo el entramado de Infraestructura céntrica de aplicaciones (ACI) de Cisco, el Controlador de infraestructura de políticas de aplicación (APIC) admite la contraseña MD5 y también el modo seguro COOP.

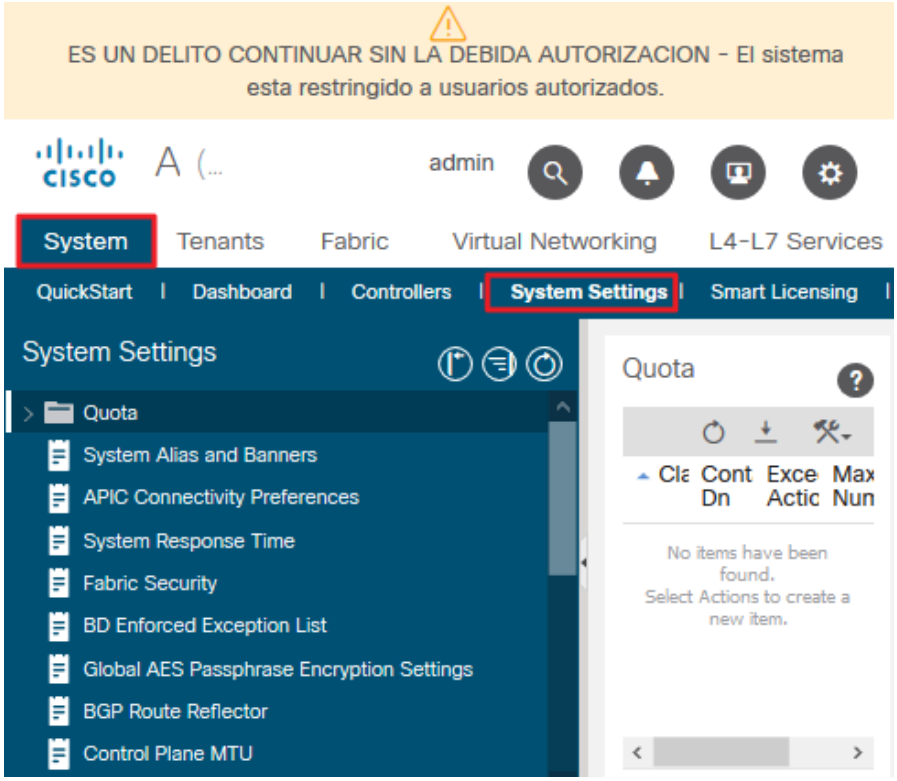
Configuración del tipo de autenticación COOP ZMQ: coop:AuthP: se agrega un nuevo objeto administrado a la base de datos del Motor de administración de datos (DME) / COOP (coop / inst / auth). El valor predeterminado para el tipo de atributo es "compatible", y los usuarios tienen la opción de configurar el tipo para que sea "estricto".

Autenticación COOP ZMQ por contraseña MD5: El APIC proporciona un objeto administrado (fabric:SecurityToken), que incluye un atributo que se utilizará para la contraseña MD5. Un atributo en este objeto administrado, llamado "token", es una cadena que cambia cada hora. COOP obtiene la notificación del DME para actualizar la contraseña para la autenticación ZMQ. El valor del token de atributo no se muestra.

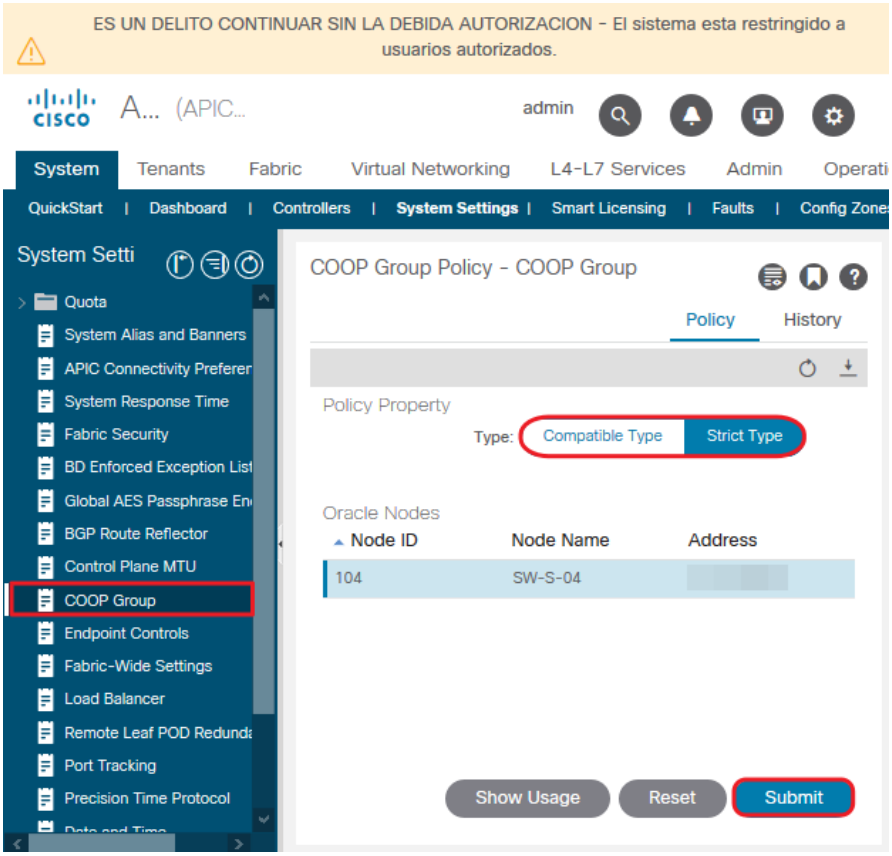
Nota: Durante una actualización de la estructura ACI, el modo estricto COOP no se permite hasta que se actualicen todos los interruptores. Esta protección evita el rechazo inesperado de una conexión COOP que podría activarse al habilitar prematuramente el modo estricto.

Para la configuración de COOP usando la GUI Cisco APIC siga y adapte los siguientes pasos según proceda:

a) En la barra de menú, elija “System”>“System Settings”.



b) En el panel de navegación, haga clic en “COOP Group”, posteriormente en el panel de trabajo, en el área “Policy Property” en el campo “Type”, elija el tipo deseado de las opciones Tipo compatible y Tipo estricto (Compatible Type / Strict Type) comprobando que se van a aplicar a los nodos deseados. Pulse “Submit” para finalizar.



7.6.2 EIGRP

EIGRP combina los beneficios de los protocolos de vector de distancia con las características de los protocolos de estado de enlace. EIGRP envía mensajes de saludo periódicos para el descubrimiento de activos de la red. Una vez que EIGRP se entera de un nuevo activo, envía una actualización única de todas las rutas y métricas de ruta locales de EIGRP. El enrutador EIGRP receptor calcula la distancia de ruta en función de las métricas recibidas y el costo asignado localmente del enlace a ese activo. Después de esta actualización inicial de la tabla de ruta completa, EIGRP envía actualizaciones incrementales solo a los activos afectados por el cambio de ruta. Este proceso acelera la convergencia y minimiza el ancho de banda utilizado por EIGRP.

Para Cisco APIC, la autenticación EIGRP utiliza la infraestructura de llavero de “Route-map” para la autenticación MD5. Se necesitan dos parámetros para configurar la autenticación entre dos pares EIGRP. Los parámetros son:

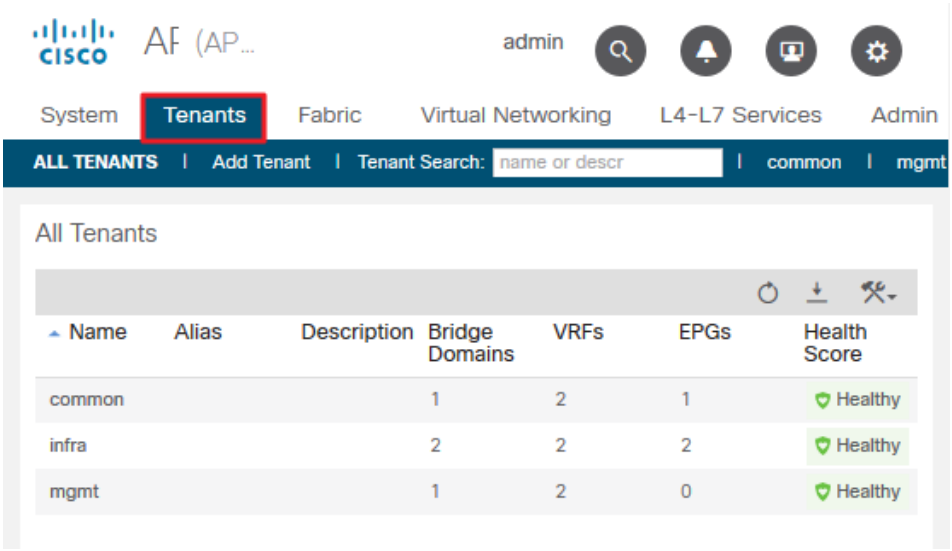
a) Mode

b) Keychain

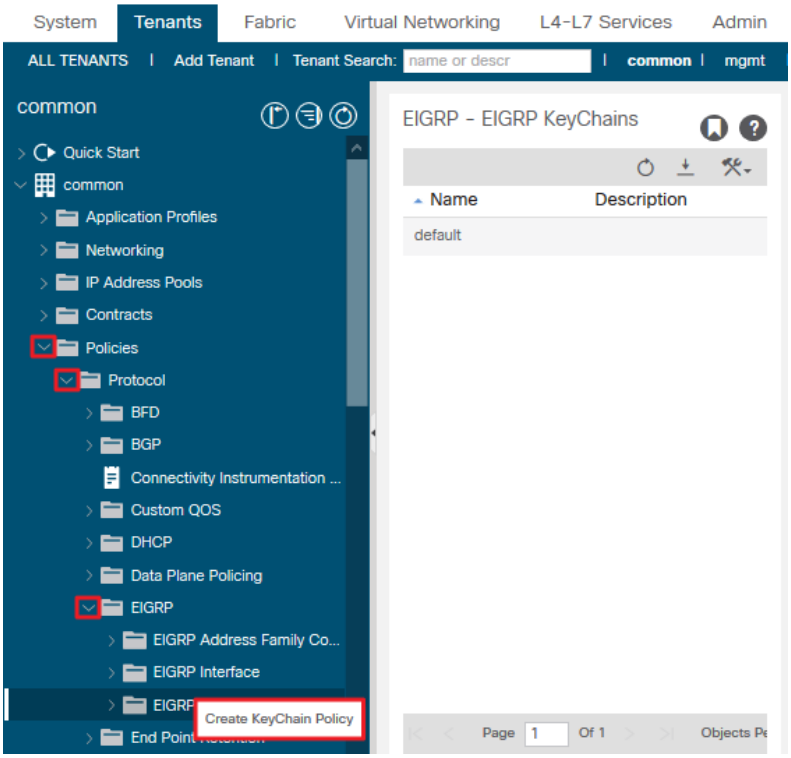
Nota: El protocolo EIGRP solo admite la autenticación MD5, por tanto, se recomienda su uso en los casos donde las necesidades de la organización requieran del mismo, limitando su utilización a la comunicación entre elementos más internos de la infraestructura.

Para la configuración de EIGRP usando la GUI Cisco APIC siga y adapte los siguientes pasos según proceda:

a) En la barra de menú, elija “Tenant” y pulse doble clic sobre el tenant a aplicar configuración.



b) En el panel de navegación, expanda “Policies”>”Protocol”>”EIGRP”. Expanda EIGRP y haga clic con el botón derecho en “EIGRP KeyChains” para abrir “Create KeyChain Policy” y realizar las siguientes acciones:



i. En la ventana “Create KeyChain Policy” configure el campo “Name”

ii. Pulse en el icono del “+” para crear una nueva política

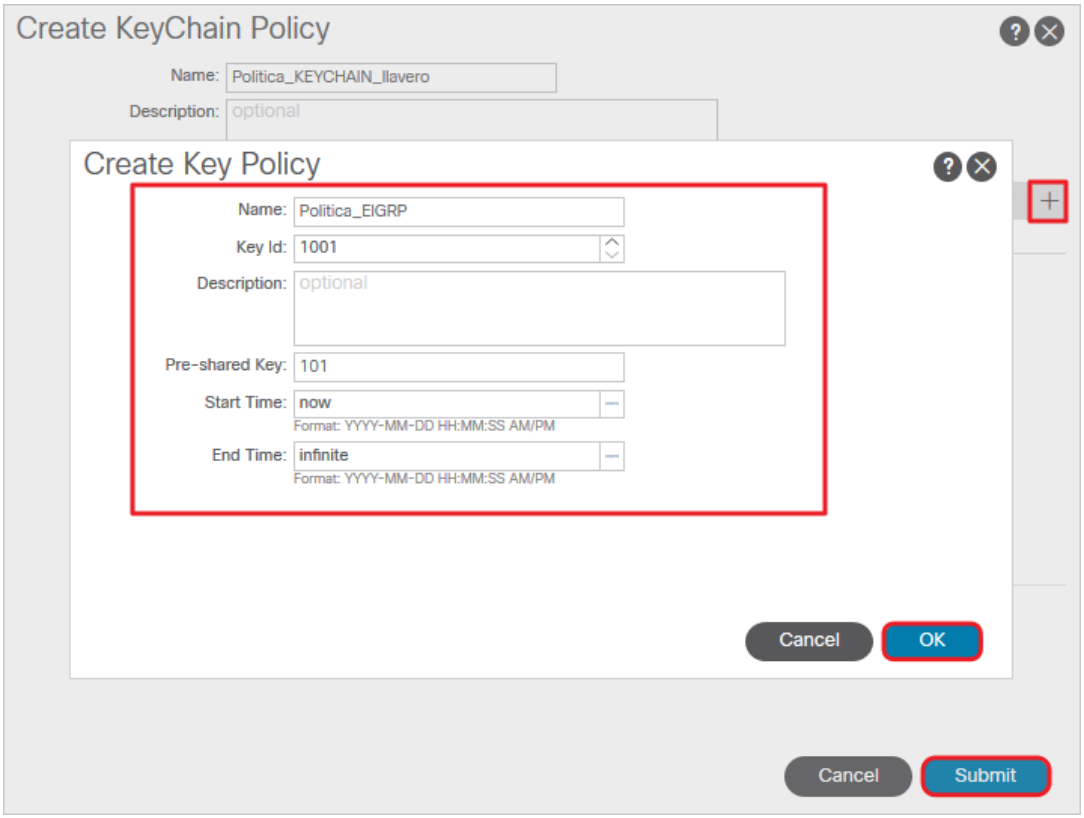
iii. En el campo “Name", ingrese un nombre para la política.

iv. En el campo “Key ID”, ingrese un número de ID de clave.

v. En el campo “Pre-shared Key”, ingrese la información de la clave previamente compartida.

vi. Opcional. En los campos “Start Time” y “End Time”, ingrese una hora.

vii. Pulse “OK” para continuar y “Submit” para guardar.



7.7 SEGURIDAD FIPS DEL FABRIC

Los Estándares federales de procesamiento de información (FIPS), detallan los requisitos de seguridad para los módulos criptográficos. FIPS 140-2 especifica que un módulo criptográfico debe ser un conjunto de hardware, software, firmware o alguna combinación que implemente funciones o procesos criptográficos, incluidos algoritmos criptográficos y, opcionalmente, generación de claves, y que esté contenido dentro de un límite criptográfico definido.

FIPS especifica ciertos algoritmos criptográficos como seguros, y también identifica qué algoritmos deben usarse para los módulos compatibles con FIPS.

Nota: FIPS habilita y deshabilita los módulos criptográficos que según su estándar se categorizan como seguros o inseguros, no obstante, la constante evolución de las tecnologías requiere la revisión exhaustiva de algoritmos criptográficos y configuraciones de seguridad. Por tanto, para el establecimiento de políticas derivadas del estándar FIPS, será necesario un estudio previo que garantice que las configuraciones implantadas por el estándar garantizan la mayor seguridad posible en la aplicación y en consecuencia, no afecta negativamente al rendimiento o a la protección de los elementos que conforman el sistema.

La habilitación de FIPS requiere el seguimiento de ciertas pautas y la consideración de ciertas limitaciones que se detallan a continuación:

a) Cuando FIPS está habilitado, se aplica a través de Cisco APIC.

b) Al realizar una actualización a una versión inferior (downgrade) del software Cisco APIC, primero debe deshabilitar FIPS.

c) Las contraseñas deberán tener un mínimo de ocho caracteres de longitud.

d) Telnet está deshabilitado. Los usuarios deben iniciar sesión utilizando solo SSH.

e) Se deberán eliminar todas las claves del servidor SSH RSA1.

f) Se deberá deshabilitar la autenticación remota a través de RADIUS/TACACS+. Solo los usuarios locales y LDAP pueden autenticarse.

g) Secure Shell (SSH) y SNMP son compatibles.

h) Se deberá deshabilitar SNMP v1 y v2. Cualquier cuenta de usuario existente en el switch que se haya configurado para SNMPv3 se debe configurar solo con SHA para autenticación y AES para privacidad.

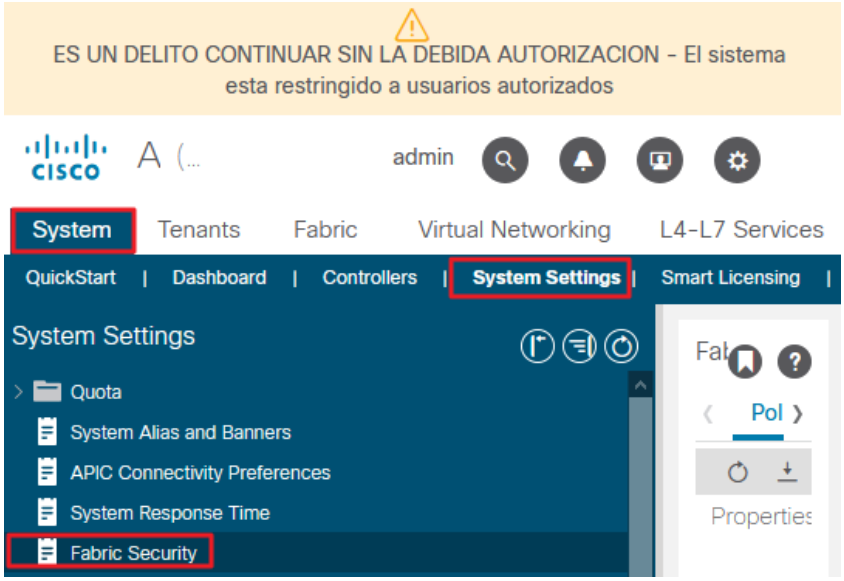
i) A partir de la versión 2.3 (1x), FIPS se puede configurar a nivel de switch.

j) A partir de la versión 3.1 (1x), cuando FIP está habilitado, NTP funcionará en modo FIPS, en modo FIPS NTP admite autenticación con HMAC-SHA1 y sin autenticación.

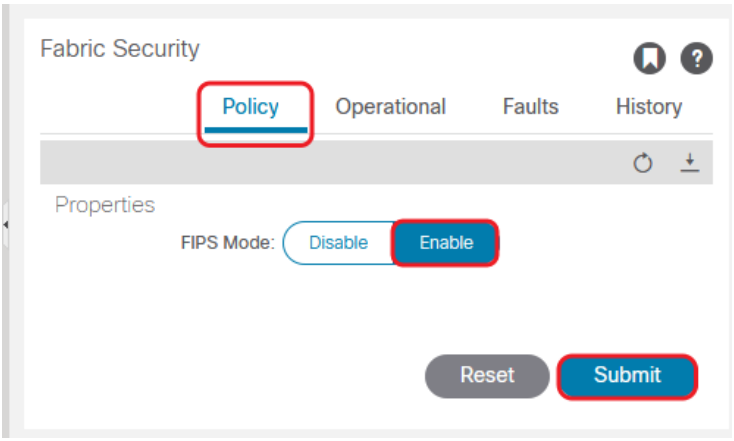
7.7.1 CONFIGURACIÓN DE FIPS USANDO LA GUI APIC

Para habilitar FIPS mediante la GUI Cisco APIC siga los siguientes pasos:

a) En la barra de menú, elija “System”>”System Settings”>”Fabric Security”.

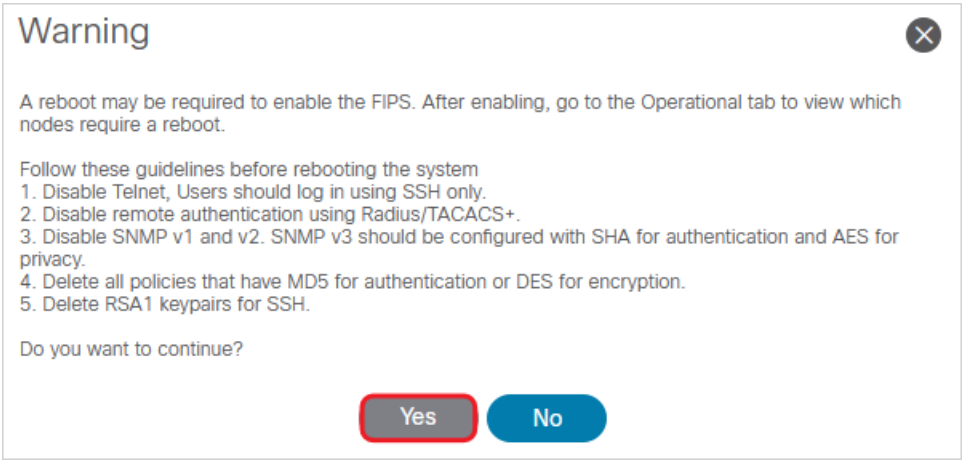


b) En el apartado “Policy” para la configuración “FIPS Mode.” Seleccione el modo FIPS deseado y pulse “Submit” para aplicar.

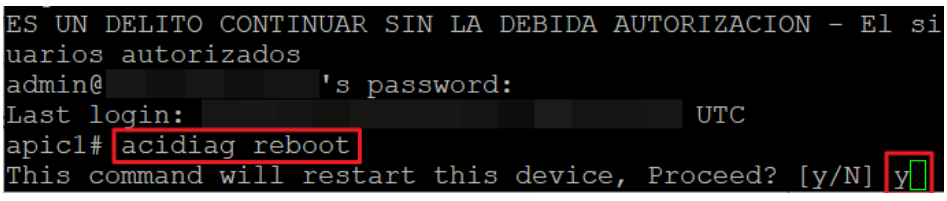


Nota: Las opciones para el modo FIPS son Deshabilitar y Habilitar. El valor por defecto es Deshabilitado.

c) Se mostrará una advertencia sobre la seguridad de protocolos y encriptaciones que se utilizará con motivo de habilitación del estándar FIPS. Si está conforme pulse “YES”.

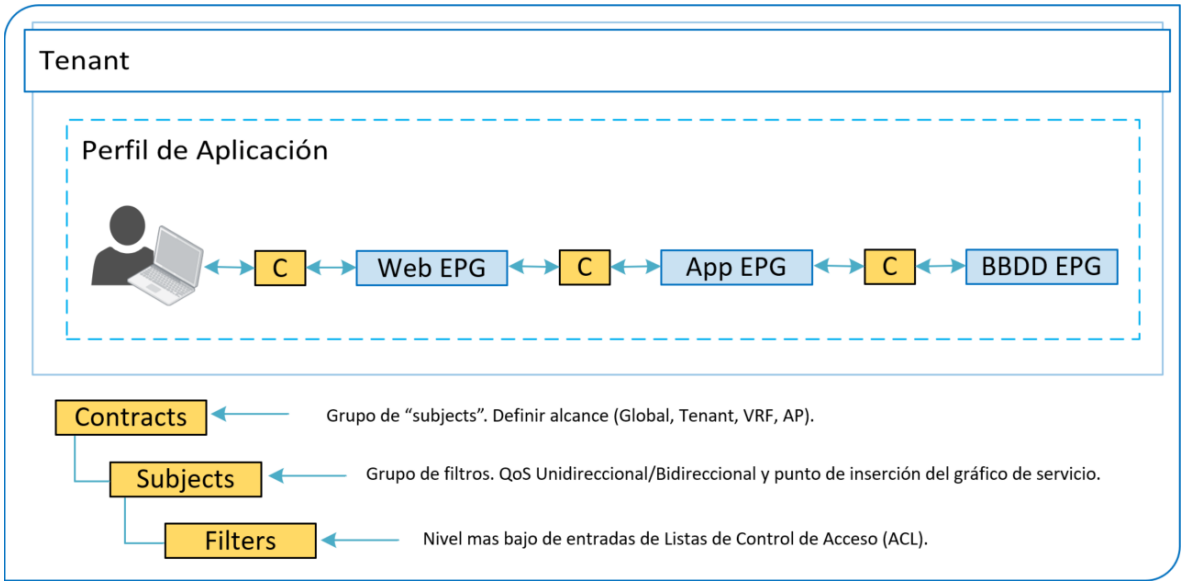


d) Cada vez que cambie el modo, debe reiniciar para completar la configuración.



7.8 DIRECTIVAS DE SEGURIDAD ACI FABRIC.

El modelo de política de seguridad de ACI Fabric se basa en contratos (contracts). Este enfoque aborda las limitaciones de las listas tradicionales de control de acceso (ACL). Los contratos contienen las especificaciones para las políticas de seguridad que se aplican en el tráfico entre grupos de "endpoints".



Las comunicaciones EPG requieren un contrato, la comunicación EPG a EPG no está permitida sin un contrato. El APIC presenta el modelo de política completo, incluidos los contratos y sus EPG asociadas, en el modelo concreto en cada cambio. Al ingresar, cada paquete que ingresa al "fabric" se marca con los detalles de la política requerida. Debido a que los contratos deben seleccionar qué tipos de tráfico pueden pasar entre las EPG, los contratos aplican políticas de seguridad. Si bien los contratos satisfacen los requisitos de seguridad manejados por las listas de control de acceso (ACL) en la configuración de red convencional, son una solución de política de seguridad más flexible, manejable e integral.

7.8.1 LISTAS DE CONTROL DE ACCESO Y CONTRATOS

Las listas de control de acceso tradicionales (ACL) tienen una serie de limitaciones que el modelo de seguridad de ACI "fabric" aborda. La ACL tradicional está muy unida a la topología de la red. Por lo general, se configuran por interfaz de entrada y salida de router o switch y se personalizan para esa interfaz y el tráfico que se espera que fluya a través de esas interfaces. Debido a esta personalización, a menudo no se pueden reutilizar en las interfaces, y mucho menos en los routers o switches.

Las ACL tradicionales pueden ser muy complicadas y crípticas porque contienen listas de direcciones IP, subredes y protocolos específicos que están permitidos, así como muchos que no están permitidos específicamente. Esta complejidad hace que sean difíciles de mantener y, a menudo, simplemente crecen, ya que los administradores son reacios a eliminar las reglas de ACL por temor a crear un problema. Su complejidad ocasiona que generalmente solo se implementen en puntos específicos en la red. En muchas ocasiones, los beneficios de seguridad de las ACL no se explotan como por ejemplo, dentro de una organización o en el tráfico en el centro de datos.

Otro problema es el posible gran aumento en el número de entradas en una sola ACL. Los usuarios a menudo desean crear una ACL que permita que un conjunto de orígenes se comunique con un conjunto de destinos mediante el uso de un conjunto de protocolos. En el peor de los casos, si X orígenes están hablando con Y destinos utilizando Z protocolos, puede haber X * Y * Z entradas en la ACL. La ACL debe enumerar cada fuente que se comunica con cada destino para cada protocolo. No se necesitan muchos dispositivos o protocolos antes de que la ACL sea muy extensa.

El modelo de seguridad de ACI "fabric" aborda estos problemas de ACL. El modelo de seguridad de ACI "fabric" expresa directamente la intención del administrador. Los administradores usan los objetos gestionados por contrato, filtro y etiqueta para especificar cómo los grupos de "endpoint" pueden comunicarse. Estos objetos administrados no están vinculados a la topología de la red porque no se aplican a una interfaz específica. Son simplemente reglas que la red debe aplicar independientemente de dónde estén conectados estos grupos de "endpoint". Esta independencia de topología facilita que estos objetos administrados se puedan implementar y reutilizar fácilmente en todo el centro de datos, no solo como puntos de demarcación específicos.

El modelo de seguridad de ACI "fabric" utiliza la construcción de agrupación de "endpoint" directamente, por lo que la idea de permitir que grupos de servidores se comuniquen entre sí es simple. Una sola regla puede permitir que un número arbitrario de orígenes se comunique con un número igualmente arbitrario de destinos. Esta simplificación mejora drásticamente su escalabilidad y facilidad de mantenimiento, lo que también significa que son más fáciles de usar en todo el centro de datos.

Los contratos contienen las políticas que rigen la comunicación entre las EPG. El contrato especifica qué se puede comunicar y las EPG especifican el origen y el destino de las comunicaciones. Los contratos vinculan las EPG.

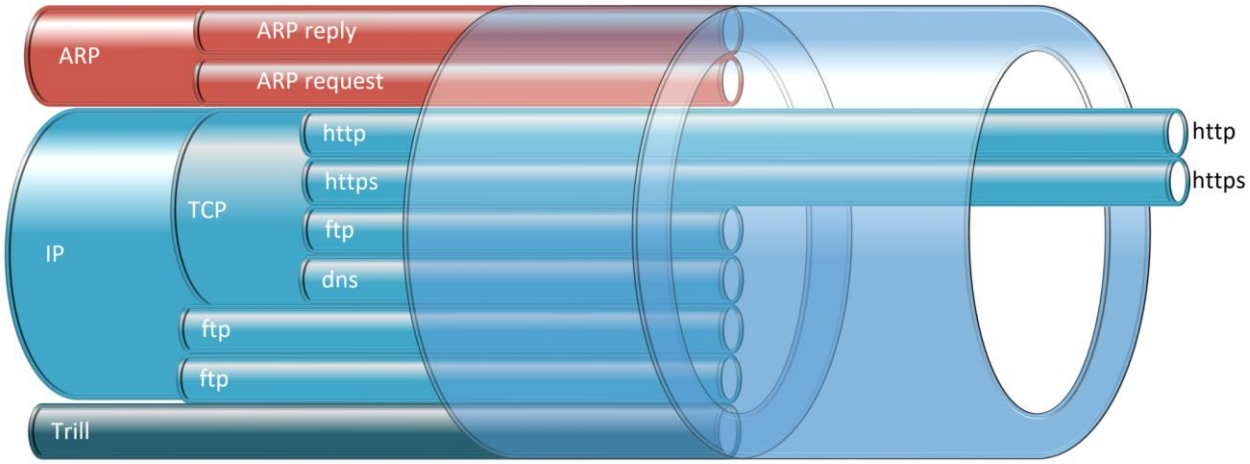
Los "endpoints" en un EPG pueden comunicarse con los "endpoints" de otro EPG y viceversa si el contrato lo permite. Esta estructura de políticas es muy flexible. Puede haber muchos contratos entre EPG's, puede haber más de dos EPG que usen un contrato, y los contratos se pueden reutilizar en múltiples conjuntos de EPG.

También hay direccionalidad en la relación entre EPG y contratos. Las EPG pueden proporcionar o poseer un contrato. Una EPG que proporciona un contrato suele ser un conjunto de "endpoints" que proporcionan un servicio a un conjunto de dispositivos cliente. Los protocolos utilizados por ese servicio están definidos en el contrato. Por otra parte, una EPG que posee un contrato suele ser un conjunto de "endpoints" clientes de ese servicio. Cuando el "endpoint" del cliente intenta conectarse a un "endpoint" del servidor (proveedor), el contrato verifica si esa conexión está permitida. A menos que se especifique lo contrario, ese contrato no permitiría que un servidor inicie una conexión con un cliente. Sin embargo, otro contrato entre las EPG podría permitir fácilmente una conexión en esa dirección.

Esta relación proveedor/cliente generalmente se muestra gráficamente con flechas entre las EPG y el contrato. Tenga en cuenta la dirección de las flechas que se muestran a continuación.

EPG 1 <------- cliente del contrato------ CONTRACT <----- servidor del contrato ------ EPG 2

El contrato se construye de manera jerárquica. Consiste en uno o más “Subjects” (sujetos), cada “Subject” contiene uno o más filtros y cada filtro puede definir uno o más protocolos.



Por ejemplo, puede definir un filtro llamado HTTP que especifique el puerto TCP 80 y el puerto TCP 8080 y otro filtro llamado HTTPS que especifique el puerto TCP 443. Luego puede crear un contrato llamado “webCtrct” que tiene dos conjuntos de temas. “openProv” y “openCons” son los temas que contienen el filtro HTTP. “secureProv” y “secureCons” son los temas que contienen el filtro HTTPS. Este contrato de “webCtrct” se puede utilizar para permitir el tráfico web seguro y no seguro entre las EPG que proporcionan el servicio web y las EPG que contienen “endpoints” clientes de ese servicio.

Estas mismas construcciones también se aplican a las políticas que rigen los hipervisores de máquinas virtuales. Cuando se coloca una EPG en un dominio de administrador de máquina virtual (VMM), el APIC descarga todas las políticas asociadas con la EPG a los “leaf switch” con interfaces que se conectan al dominio VMM. Cuando se crea esta política, el APIC la configura a un dominio VMM que especifica qué switches permiten la conectividad para los “endpoints” en las EPG. El dominio VMM define el conjunto de switches y puertos que permiten la conexión de “endpoints” en una EPG. Cuando un “endpoint” entra en línea, se asocia con las EPG apropiadas. Cuando envía un paquete, la EPG de origen y la EPG de destino se derivan del paquete y la política definida por el contrato correspondiente que verifica si el paquete está permitido. En caso afirmativo, se reenvía el paquete. Si no, el paquete se descarta.

En detalle, los contratos se componen de los siguientes elementos:

a) Nombre: Todos los contratos propiedad de un tenant deben tener nombres diferentes (incluidos los contratos creados bajo el “tenant common” o el “tenant itself”).

b) Subjects: Un grupo de filtros para una aplicación o servicio específico.

c) Filtros: Se utilizan para clasificar el tráfico según los atributos de la capa 2 a la capa 4 (como el tipo de Ethernet, el tipo de protocolo, los indicadores TCP y los puertos).

d) Acciones: Acciones a realizar en el tráfico filtrado. Se admiten las siguientes acciones:

   i. Permitir el tráfico (solo contratos regulares).

   ii. Marcar el tráfico (DSCP / CoS) (solo contratos regulares).

   iii. Redireccionar el tráfico (solo contratos regulares, a través de un gráfico de servicio).

   iv. Replicar tráfico (solo contratos regulares, a través de un gráfico de servicio o SPAN).

v. Bloquear el tráfico (contratos “taboo”).

vi. Con la versión 3.2 (x) de Cisco APIC y los switches con nombres que terminan en EX o FX, también puede utilizar una acción de Denegación de asunto o Contrato o Excepción de sujeto en un contrato estándar para bloquear el tráfico con patrones específicos.

vii. Registre el tráfico (contratos “taboo” y contratos regulares).

e) Alias: (Opcional) Un nombre modificable para un objeto. Aunque el nombre de un objeto, una vez creado, no se puede cambiar, el Alias es una propiedad que se puede cambiar.

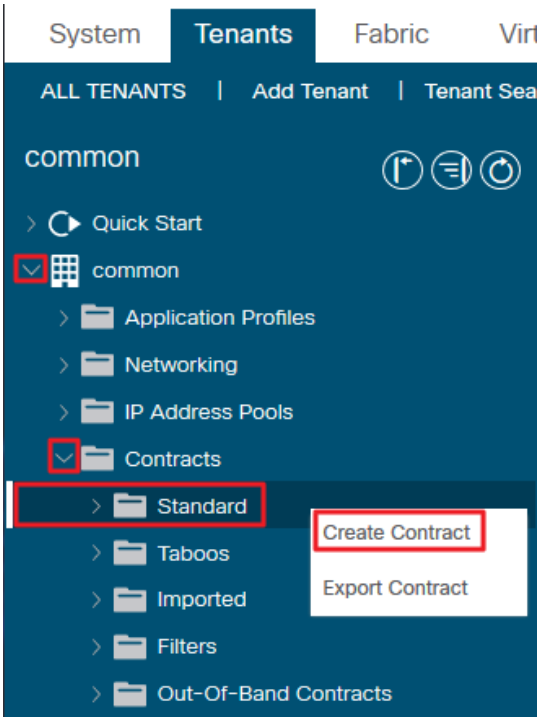
Por lo tanto, el contrato permite acciones más complejas que solo permitir o denegar. El contrato puede especificar que el tráfico que coincide con un tema determinado puede ser redirigido a un servicio, puede copiarse o puede modificarse su nivel de QoS. Los “endpoints” pueden moverse, los nuevos pueden entrar en línea y la comunicación puede ocurrir incluso si el APIC está fuera de línea o inaccesible. Por medio de esta tecnología se elimina el APIC como punto único de fallos en la red. Al ingresar paquetes al ACI “fabric”, el modelo concreto que se ejecuta en el “switch” aplica las políticas de seguridad.

7.8.2 CONTRATOS ACL PARA PERMITIR O DENEGAR USANDO LA GUI APIC

Se muestra a continuación, pautas para habilitar el permiso de contrato y denegar el registro utilizando la GUI.

a) En la barra de menú, elija “Tenants”>”ALL Tenants” y elija el “Tenant” que desea aplicar la configuración y haga doble clic sobre él.

b) En el panel de navegación, expanda [Nombre_del_Tenant]>"Contracts". Sitúese sobre "Standard" y haga clic con el botón derecho del ratón sobre el para seleccionar "Create Contract".



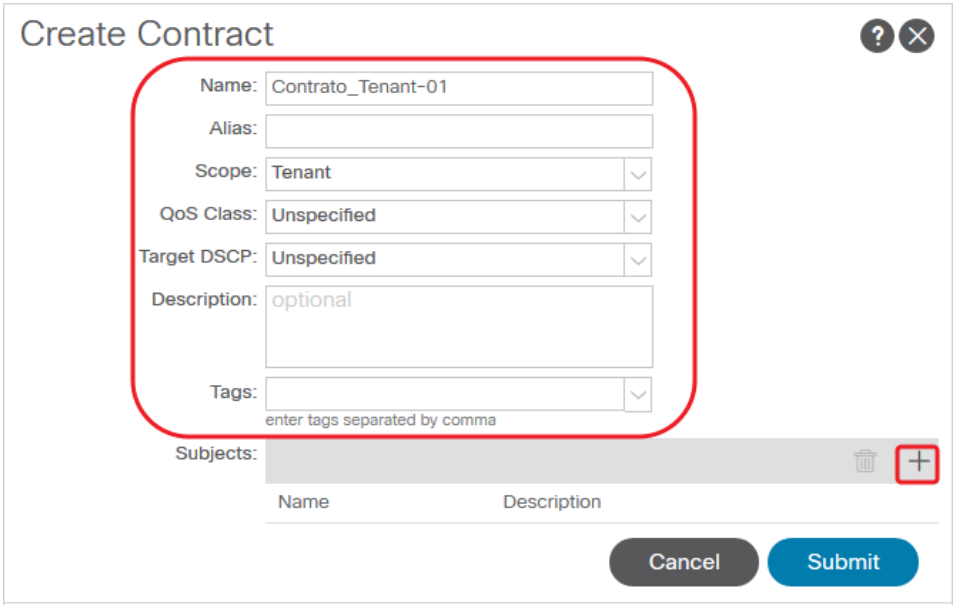
c) En el cuadro de diálogo "Create Contract", realice las siguientes acciones:

i. En el campo "Name", escriba el nombre del contrato.

ii. En el campo "Scope", elija el alcance (VRF, Tenant o Global).

iii. Opcional. Establezca la clase de DSCP o QoS de destino que se aplicará al contrato.

iv. Haga clic en el icono "+" para expandir Temas.



d) En el cuadro de diálogo “Create Contract Subject”, realice las siguientes acciones:

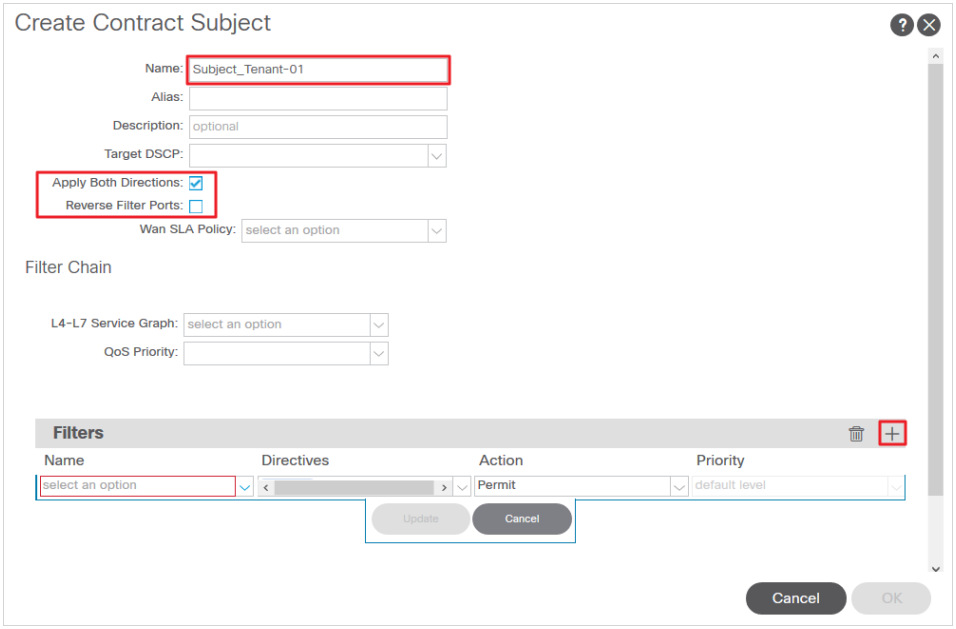
i. Ingrese el nombre del “Subject” y una descripción opcional.

ii. Opcional. En la lista desplegable para el DSCP de destino, seleccione el DSCP que se aplicará al tema.

iii. Deje la opción “Apply Both Directions” marcada, a menos que desee que el contrato solo se aplique del cliente al servidor, en lugar de en ambas direcciones.

iv. Deje la opción “Reverse Filter Ports” marcada si desmarcó “Apply Both Directions” para intercambiar los puertos de origen y destino de la capa 4. De esta forma, la regla se aplicaría del servidor al cliente.

v. Haga clic en el ícono “+” para expandir los Filtros.



vi. En la lista desplegable “Name”, elija una opción; por ejemplo, haga clic en ”arp”, “default”, “est” o “icmp”, o elija un filtro configurado previamente.

vii. En la lista desplegable Directivas, seleccione el parámetro que más convenga.

viii. (Opcional) Elija la acción de permitir o denegar según convenga en el apartado “Action”.

Nota: Con la directiva: “log” seleccionada, si la acción para este tema es Permitir, los registros de permiso ACL rastrean los flujos y paquetes que están controlados por el “Subject” y el contrato. Si la acción para este “Subject” es Denegar, los registros de denegación de ACL rastrean los flujos y los paquetes.

ix. (Opcional) Establezca la prioridad para el “Subject”. Pulse en “Update” para finalizar la configuración.

x. Finalmente pulse “OK” en la ventana “Create Contract Subject” y “Submit” en la ventana de “Create Contract”.

7.9 CONFIGURACIONES ADICIONALES DE REFUERZO

En este apartado se detallan medidas de refuerzo adicionales a las mencionadas anteriormente. Se trata de configuraciones complementarias de seguridad en la aplicación Cisco APIC.

7.9.1 ACCESO HTTPS

Los certificados “wildcard” (como *.cisco.com) y su clave privada asociada generada en otro lugar no son compatibles con el APIC, ya que no hay soporte para ingresar la clave privada o contraseña en el APIC. Además, no se admite la exportación de claves privadas para ningún certificado, incluidos los certificados “wildcard”.

Se deben descargar e instalar los certificados de CA pública intermedia o raíz (root) antes de generar una Solicitud de firma de certificado (CSR). Aunque técnicamente no se requiere un certificado de CA raíz (root) para generar una CSR, Cisco requiere el certificado de CA raíz antes de generar la CSR para evitar desajustes entre la autoridad de CA prevista y la actual utilizada para firmar la CSR. El APIC verifica que el certificado enviado esté firmado por la CA configurada.

Para usar las mismas claves públicas y privadas para la generación y renovación de certificados, debe cumplir con las siguientes pautas:

a) Debe conservar la CSR de origen, ya que contiene la clave pública que se empareja con la clave privada en el anillo de claves (key ring).

b) La misma CSR utilizada para el certificado de origen debe volver a presentarse para el certificado renovado si desea reutilizar las claves públicas y privadas en el APIC.

c) No elimine el “key ring” original cuando use las mismas claves públicas y privadas para el certificado renovado. Al eliminar el “key ring”, se eliminará automáticamente la clave privada asociada que se usa con las CSR.

Para la implementación de certificados en Cisco APIC se debe tener en consideración las siguientes premisas:

a) Multisitio, VCPlugin, VRA y SCVMM no son compatibles con la autenticación basada en certificados.

b) Solo un certificado basado en raíz (root) puede estar activo por pod.

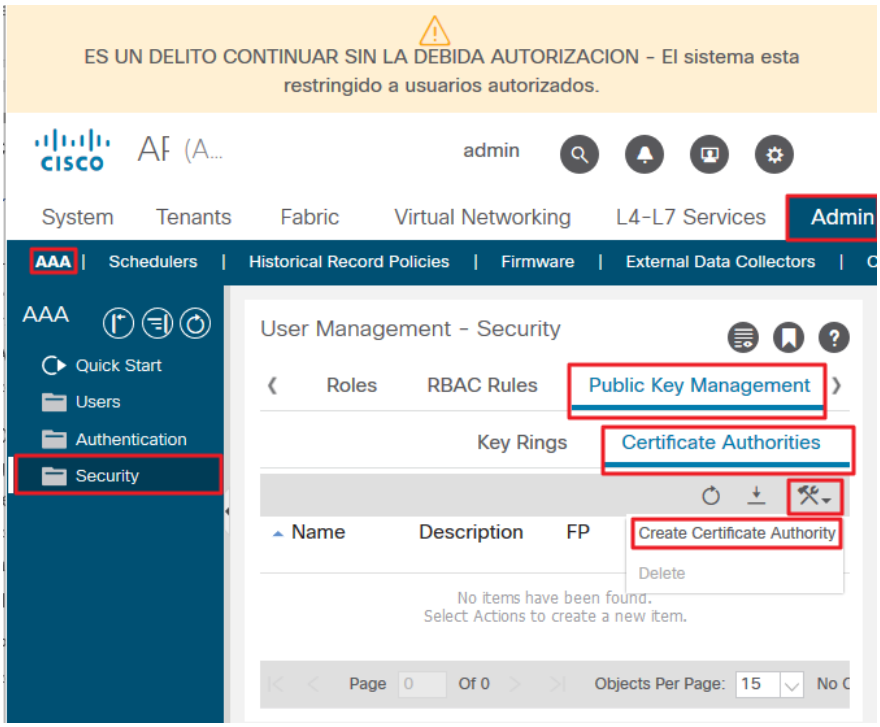
c) La autenticación basada en certificados debe deshabilitarse si desea disminuir de versión desde la versión 4.0 (1).

d) Para finalizar la sesión de autenticación basada en certificados, el usuario debe cerrar sesión y luego quitar la tarjeta CAC.

Se describen a continuación los pasos a seguir para la implementación mediante la GUI de un certificado personalizado de acceso a Cisco ACI HTTPS:

Nota: Esta tarea deberá realizarse dolo durante una ventana de mantenimiento ya que podría provocar un corte extenso en el servicio. El tiempo de inactividad afecta al acceso al clúster APIC y a los switches de usuarios o sistemas externos. El proceso NGINX en los switches también se verá afectado, pero eso será solo para la conectividad externa y no para el plano de datos del fabric. El acceso al APIC, la configuración, la administración, la resolución de problemas y demás se verán afectados. Deberá por tanto, esperar al reinicio de todos los servidores web en la “fabric” durante esta operación.

a) En la barra de menú elija “Admin”>AAA y seleccione “Security”. En el área de trabajo “User Management -Security” seleccione “Public Key Management”>“Certificate Authorities” y pulsando en el icono de Acción/Trabajo, seleccione “Create Certificate Authority”

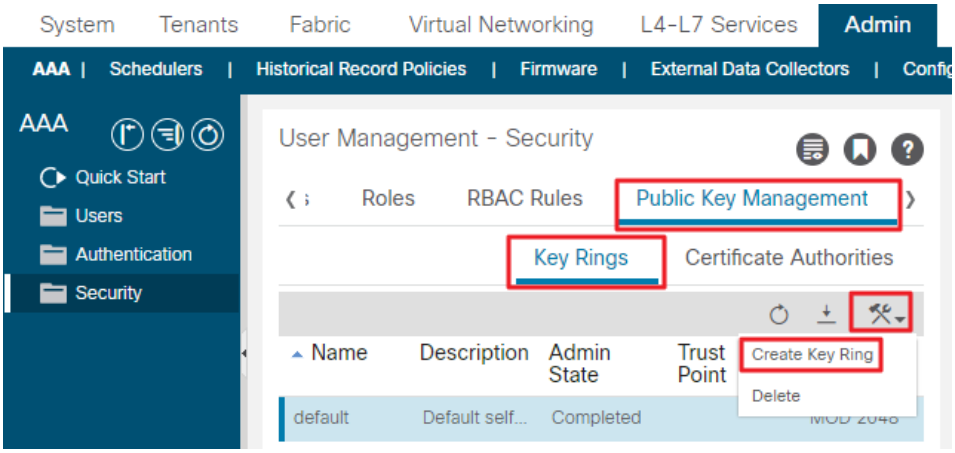


b) Complete el campo “Name” con los parámetros necesarios y en el campo “Certificate Chain”, copie los certificados intermedios y raíz para la autoridad de certificación (root CA) que firmará la Solicitud de firma de certificado (CSR) para el Controlador de infraestructura de políticas de aplicación (APIC). Cuando finalice pulse “Submit”.

Nota: El certificado debe estar en formato X649 (CER) codificado en Base64. El certificado intermedio se coloca antes del certificado de CA raíz. Debería ser similar al siguiente ejemplo:
-----BEGIN CERTIFICATE-----
<Certificado intermedio>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificado Root CA>
-----END CERTIFICATE-----

c) Una vez finalizado deberá reflejarse en el menú de trabajo algo similar a la siguiente imagen.

d) Sin salir del menú "Public Key Management", elija el menú "Key Rings". Elija el icono Acciones/trabajo y seleccione "Create Key Ring".



e) En el cuadro de diálogo "Create Key Ring" deberá completar los siguientes campos:

i. En el campo "Name", ingrese un nombre.

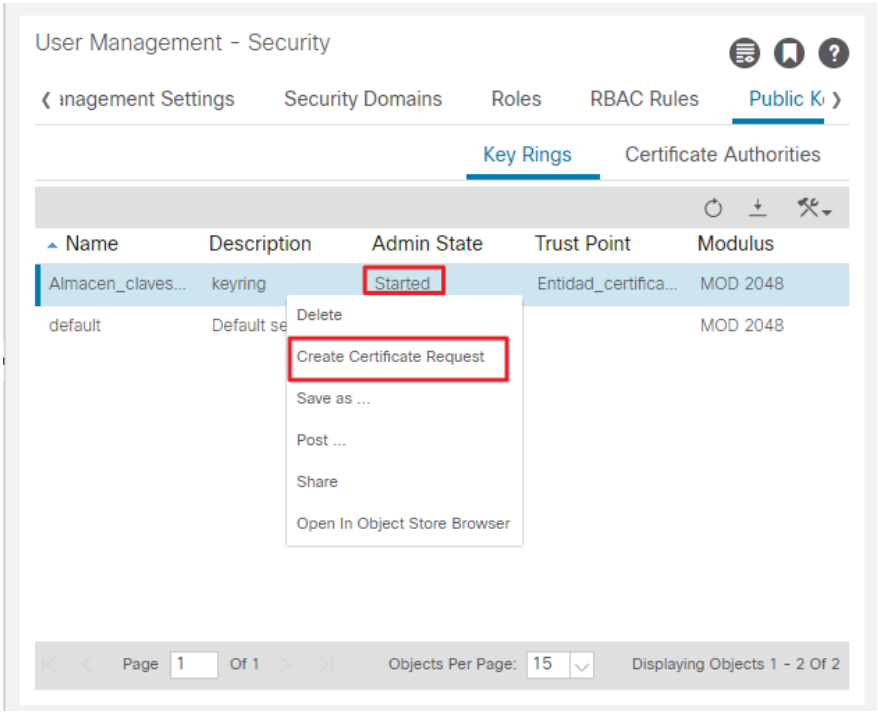
ii. El campo "Certificate" deberá quedar vacío

iii. En el campo "Modulus" elija el que más se adapte con su organización

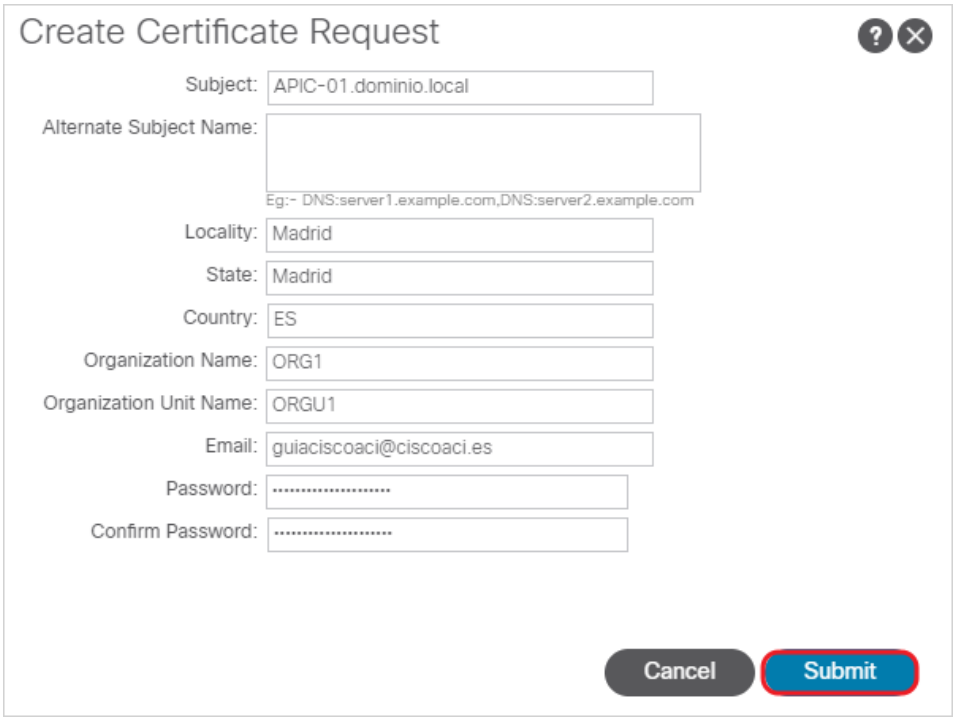
iv. En "Create Authority" deberá seleccionar la autoridad certificadora creada en el paso anterior.

Nota: No elimine el almacén de claves (key ring). Al eliminar el "key ring", se eliminará automáticamente la clave privada asociada que se usa con las CSR.

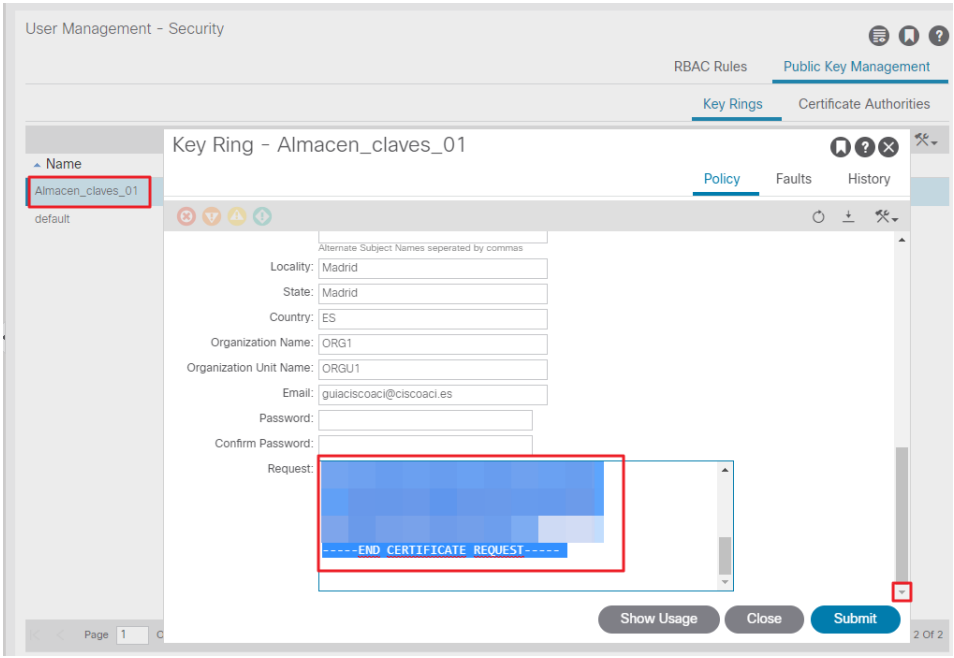
f) Compruebe en el panel de trabajo que el almacén de claves se muestra como “Started” (iniciado). Si es así, pulse el botón derecho del ratón sobre el almacén de claves creado y seleccione (Create Certificate Request).



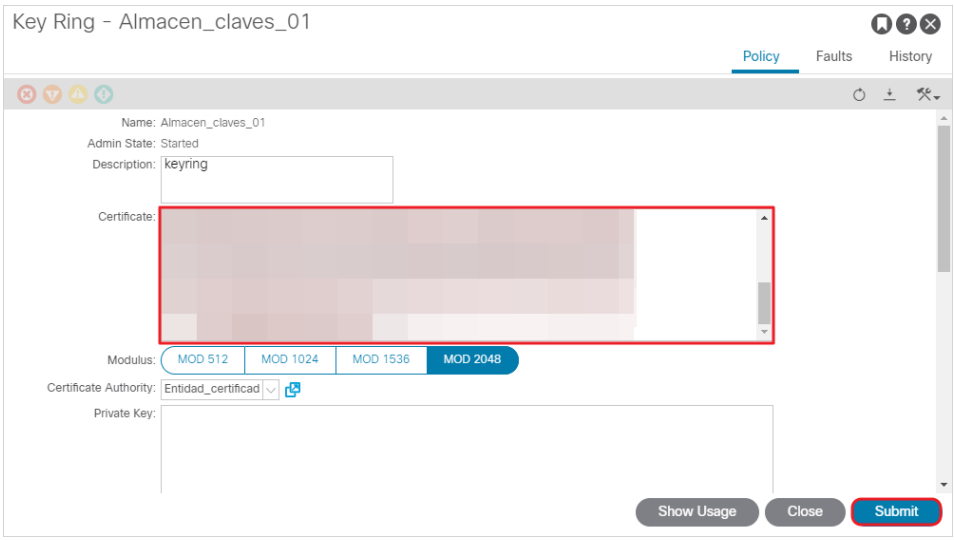
g) En la ventana emergente “Create Certificate Request” complete los campos con los datos de su organización y una contraseña segura. El campo “Subject” deberá contener el FQDN o nombre representativo del dispositivo. Pulse “Submit” para continuar.



h) Pulse doble clic sobre el almacén de claves creado anteriormente y deslizando la flecha hacia abajo, verá que se muestran los datos configurados anteriormente. Copie todo el contenido del apartado “Request” para enviarlo a la entidad certificadora para su firma. Pulse “Close” si no ha realizado ningún cambio adicional, por el contrario, pulse “Submit”.

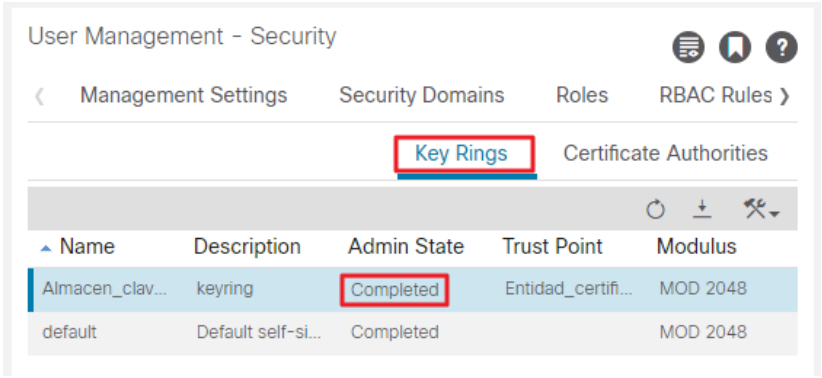


i) Copie el certificado firmado por la entidad certificadora y pulse doble clic, nuevamente, sobre el almacén de claves creado anteriormente y en el campo “Certificate” ingrese el certificado firmado por la entidad certificadora. Posteriormente, pulse “Submit” y “Submit Changes” para completar el proceso.

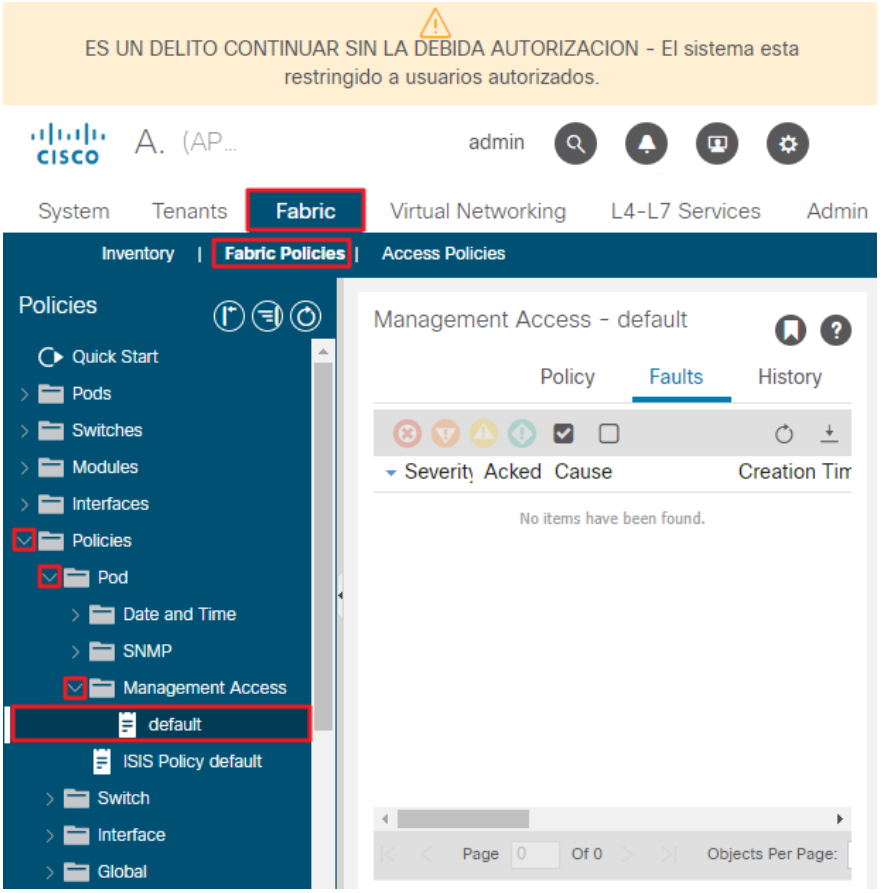


Nota: Si el CSR no fue firmado por la Autoridad de certificación indicada en el conjunto de claves, o si el certificado tiene terminaciones de línea MS-DOS, se muestra un mensaje de error y no se acepta el certificado. Elimine las terminaciones de línea de MS-DOS.

j) Compruebe en el panel de trabajo que el almacén de claves se muestra como “Completed” (completado).



k) Ahora, deberá ir a la barra de menú “Fabric”>”Fabric Policies” y desplegar “Policies”>”Pod”>Management Access” y seleccionar la política predeterminada “default”.



l) En el apartado “Policy” se recomienda modificar los siguientes parámetros:

i. HTTP-> Admin State: Disable

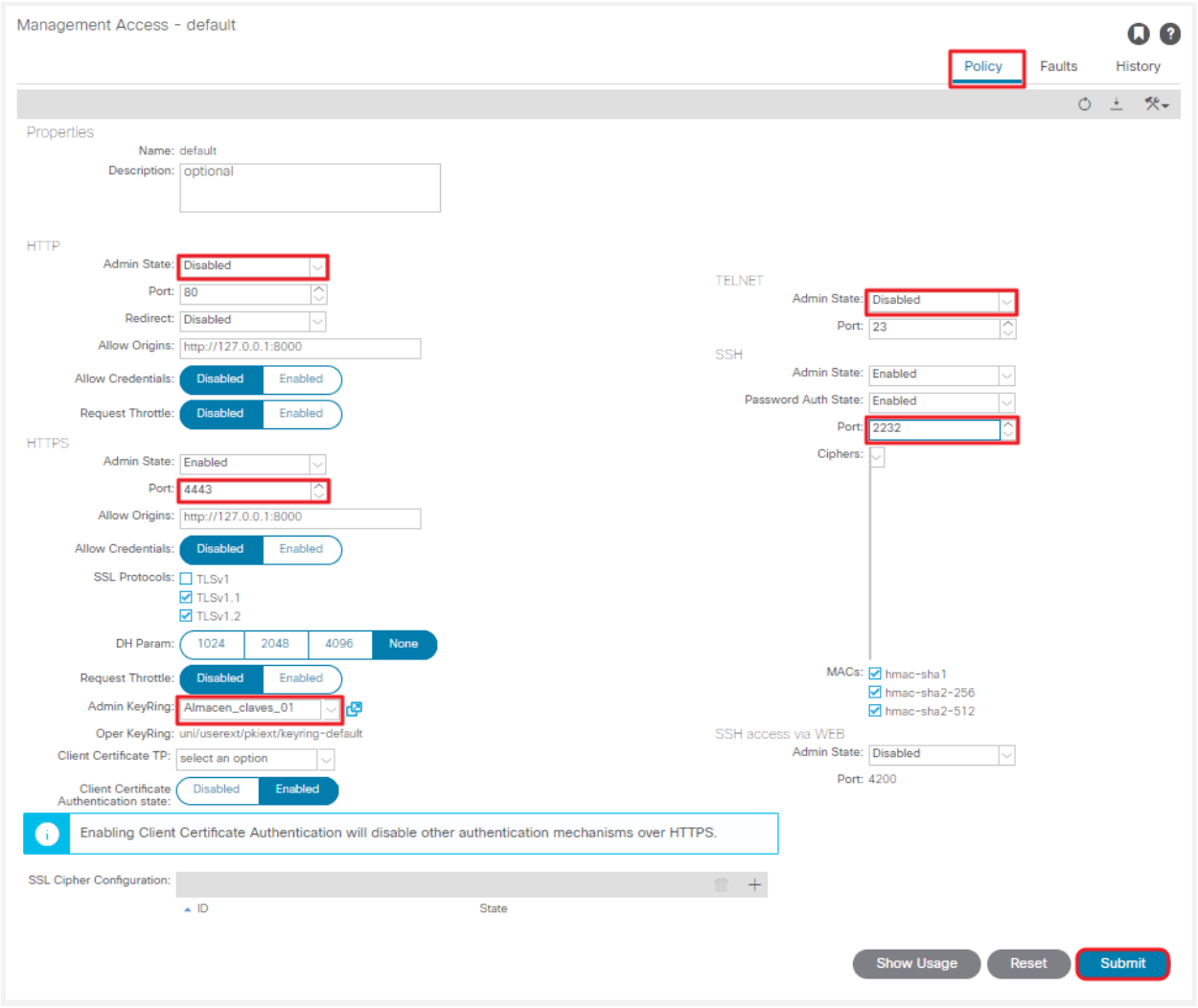
ii. HTTPS-> Port: Puerto distinto al común (443)

iii. TELNET-> Admin State: Disabled

iv. SSH-> Port: Puerto distinto al común (22)

v. Admin KeyRing: Seleccionado el almacén de claves creado en puntos anteriores.

m) El resto de parámetros deberá adaptarlos de manera que más convenga a su organización manteniendo el mayor nivel de seguridad que permita su sistema.

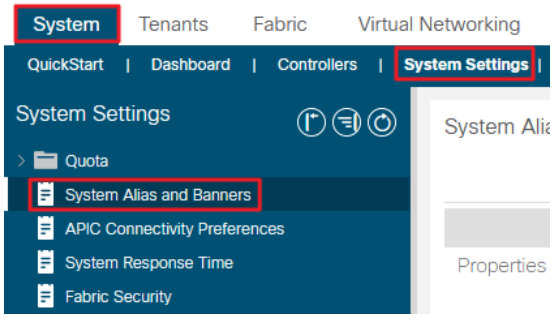


7.9.2 BANNER DE LA APLICACIÓN

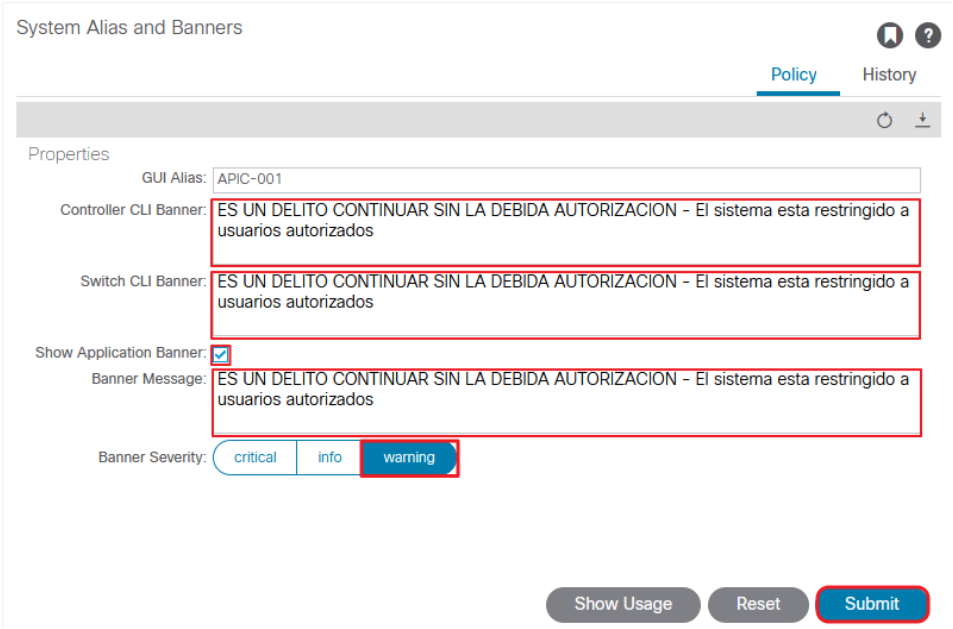
En este apartado se detallan las pautas para configurar un mensaje disuasorio (banner) para advertir a los operadores y de este modo, diferenciar los distintos APIS a los que se está accediendo.

Para realizar esta configuración mediante la GUI de Cisco APIC, deberá realizar las siguientes configuraciones:

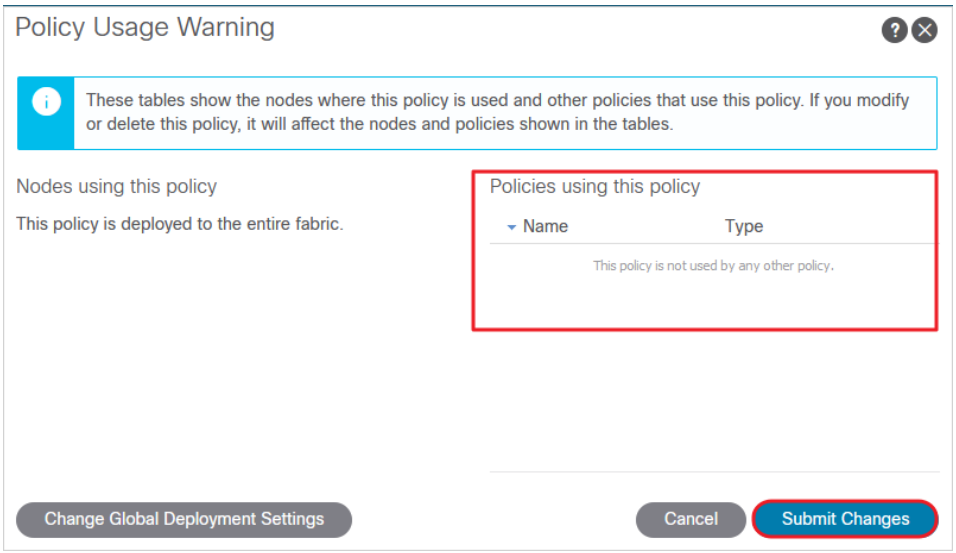
a) Diríjase a “System”>“System Settings” y seleccione “System Alias and Banners”



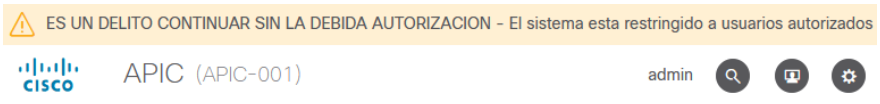
b) Deberá configurar el apartado “Controller CLI Banner”, “Switch CLI Banner” con el mensaje que más convenga a su organización y posteriormente habilitar el “check” del apartado “Show Application Banner” e introducir el mensaje nuevamente cuando el campo se habilite. Finalmente seleccione la opción “**Warning**” para el apartado “Banner Severity” para que así se muestre. Para guardar las configuraciones pulse “Submit”.



c) Se mostrará una ventana llamada “Policy Usage Warning” advirtiendo de que la modificación o eliminación de esta política, afectará a los nodos y políticas que se muestran en las tablas debajo del título “Policies using This policy”. Pulse “Submit Changes” para aplicar la configuración.



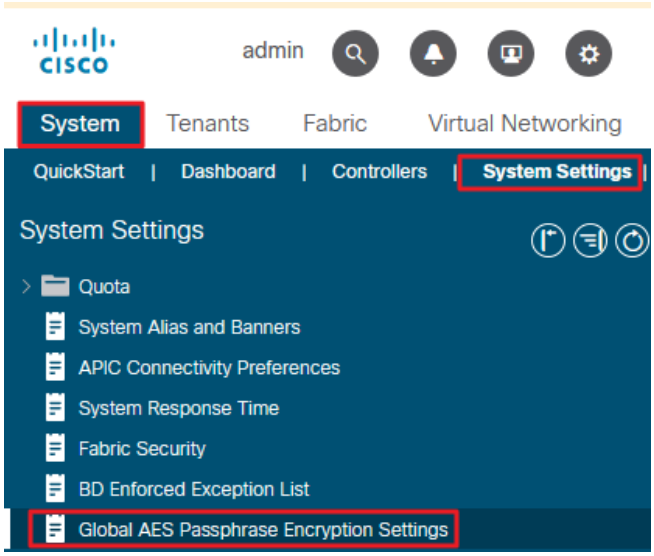
d) Si los cambios han tenido efecto se mostrará justo al inicio de la página.



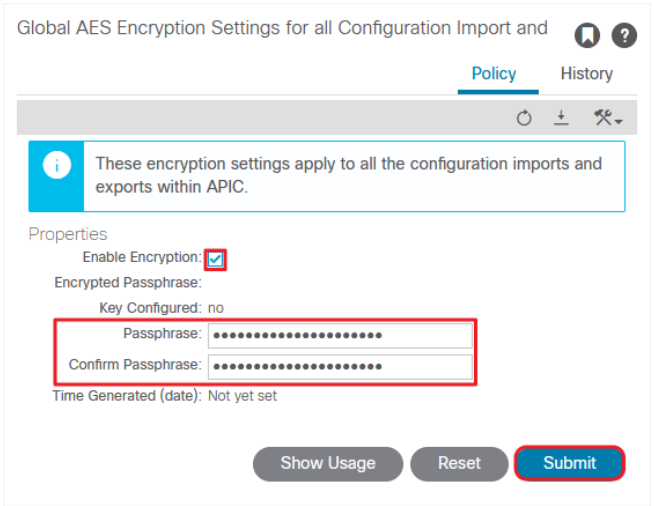
7.9.3 CIFRAR ARCHIVOS DE CONFIGURACIÓN USANDO LA GUI APIC

El cifrado AES-256 es una opción de configuración global. Cuando está habilitado, todas las propiedades seguras se ajustan a la configuración de AES. Una parte de la configuración de la estructura ACI se puede exportar utilizando la exportación de configuración con un "targetDn" específico. Sin embargo, no es posible utilizar REST API para exportar solo una parte de la estructura ACI, como una configuración de "tenant" con propiedades seguras y cifrado AES. Las propiedades seguras no se incluyen durante las solicitudes de API REST. Se muestra a continuación, pautas para habilitar el cifrado global AES utilizando la GUI.

a) Sitúese sobre el menú "System" y haciendo clic sobre él, diríjase a los siguientes submenús y apartados: "System Settings">"Global AES Passphrase Encryption Settings".

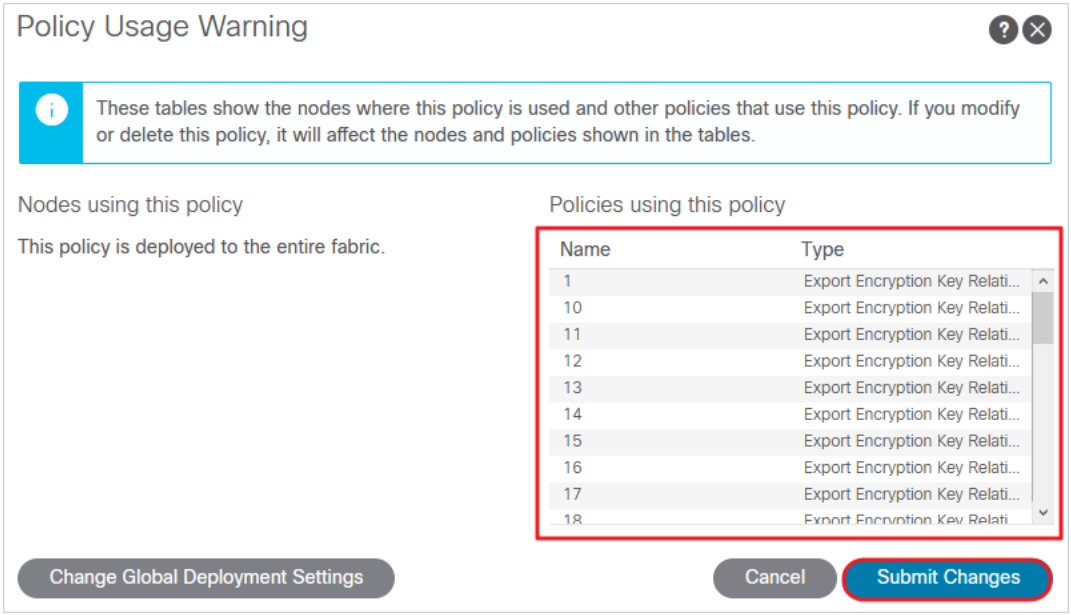


b) En el submenú "Global AES Encryption Settings for all Configuration Import and Export">"Policy", en el apartado "Properties" seleccione la casilla "Enable Encryption" y configure una contraseña segura en los apartados "Passphrase y Confirm Passphrase". Para aplicar los cambios pulse "Submit".

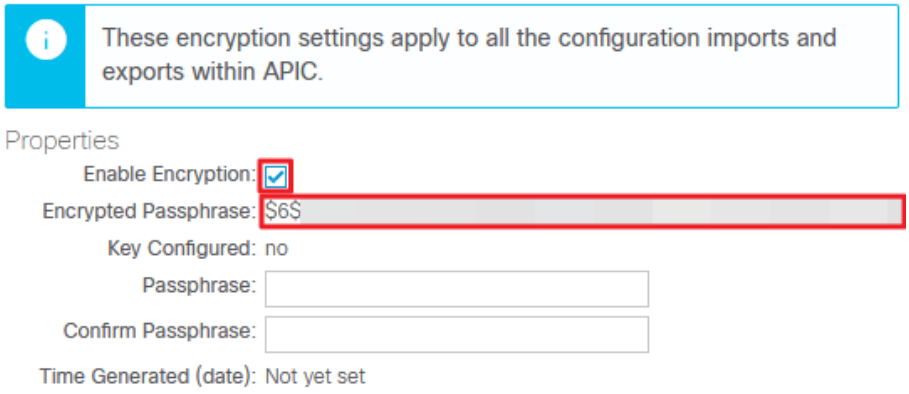


Nota: La frase de paso o contraseña deberá ser de al menos 16 caracteres.

c) Posteriormente se abrirá una ventana emergente que advertirá sobre las políticas que sufrirán cambios con la aplicación de esta configuración. Revise la columna de "Policies using This policy" y si no entra en conflicto con configuraciones de su organización, pulse el botón "Submit Changes".



d) Deberá comprobar que se han aplicado los cambios, si ha salido del menú, vaya a "System">"System Setting">"Global AES Encryption Settings for all Configuration Import and Export". Compruebe que en el apartado "Propierties" está señalado "Enable Encryption" y que se ha generado un hash correcto en el apartado "Encrypted Passphrase"

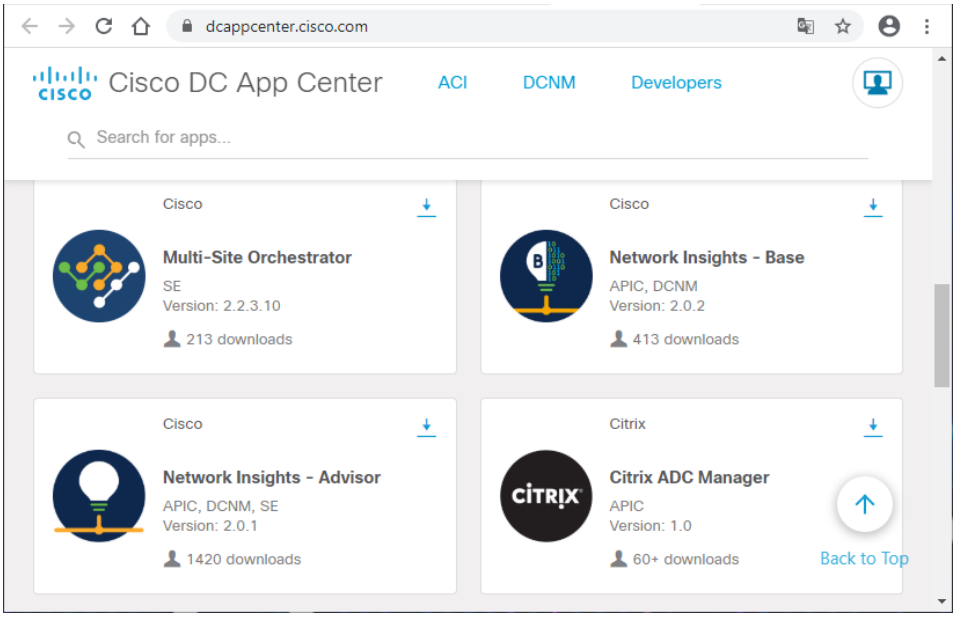


Nota: Después de habilitar el cifrado, no puede configurar una frase de paso o contraseña al crear una nueva política de importación o exportación. La frase de contraseña que configuró anteriormente ahora es global en todas las configuraciones de este cuadro y en todos los "tenant". Si exporta una configuración desde esta pestaña "you have configured a passphrase and enabled encryption", obtendrá un archivo de copia de seguridad completa. Si el cifrado no está habilitado, obtendrá un archivo de copia de seguridad con las propiedades seguras eliminadas. Estos archivos de respaldo son útiles cuando se exporta a personal que no debe conocer todos los campos seguros.

7.9.4 APLICACIONES ADICIONALES

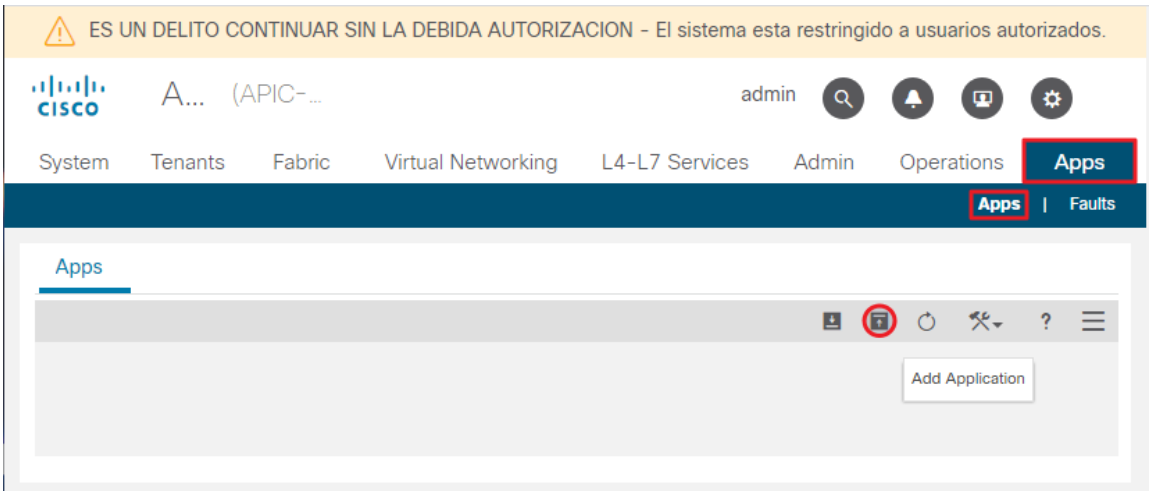
Se pueden añadir aplicaciones adicionales al Cisco APIC para mejorar la gestión de componentes de la infraestructura.

Nota: Las aplicaciones deberán descargarse desde sitios oficiales y seguros pasando previamente por programa de análisis y detección de malware.

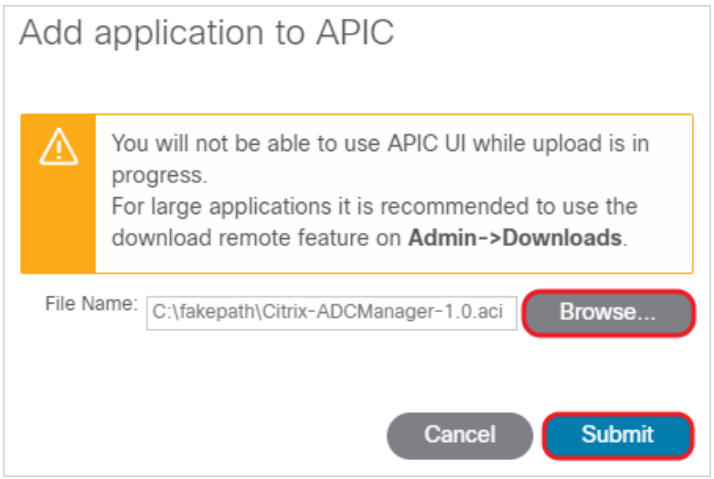


Para añadir una nueva aplicación desde la GUI de Cisco APIC, siga los siguientes pasos:

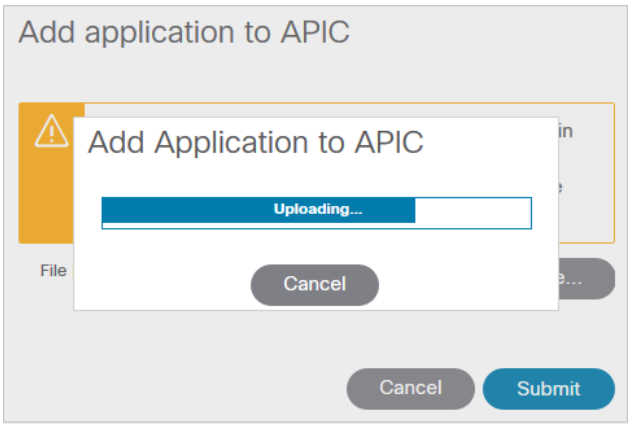
a) sitúese sobre el menú “Apps”>”Apps” y haga clic en el icono “Add Application”



b) Se abrirá una ventana llamada “Add application to APIC”. Pulse en “Browse..” y seleccione la ruta hacia la aplicación que se desea añadir, cuando ésta se encuentre seleccionada, pulse en “Submit”.



c) Se mostrará una barra de progreso indicando la subida de la aplicación al servidor.



d) Cuando finalice la carga comenzará la instalación automáticamente en el servidor APIC.