Comprensión de los servicios, la finalidad y la resolución de problemas de ISE

Contenido

Introducción

Este documento describe los servicios, el propósito y la resolución de problemas de ISE.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre Cisco Identity Services Engine.

Componentes Utilizados

El documento no se limita a ninguna versión específica de software y hardware de Cisco Identity Services Engine.

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

Antecedentes

Cisco Identity Services Engine (ISE) es una solución completa diseñada para proporcionar seguridad de red avanzada a través de la administración centralizada de políticas, la autenticación, la autorización y la contabilidad (AAA). Permite a las organizaciones gestionar el acceso a la red de los usuarios, los dispositivos y las aplicaciones al tiempo que garantiza la seguridad, el cumplimiento normativo y una experiencia de usuario fluida.

Para lograr estos objetivos, Cisco ISE utiliza una serie de servicios, cada uno de los cuales se encarga de tareas específicas que permiten que el sistema funcione de forma eficiente. Estos servicios funcionan conjuntamente para garantizar un acceso seguro a la red, una aplicación de políticas sólida, un registro detallado, una integración perfecta con sistemas externos y una definición de perfiles de dispositivos eficaz.

Cada servicio de ISE desempeña un papel fundamental a la hora de mantener la integridad y la disponibilidad de la solución. Algunos servicios gestionan funciones básicas, como la administración y la autenticación de bases de datos, mientras que otros habilitan funciones avanzadas, como la creación de perfiles de dispositivos, la administración de certificados y la supervisión.

En este artículo se ofrece una descripción general de los diversos servicios de Cisco ISE, y se explica su finalidad, importancia y los pasos posibles para la resolución de problemas en caso de que surjan problemas. Tanto si es un administrador como un profesional de la seguridad de la red, la comprensión de estos servicios le ayuda a garantizar que la implementación de ISE se realice sin problemas y de forma segura.

Descripción y resolución de problemas de servicios ISE

ISE utiliza los servicios mencionados en la captura de pantalla para respaldar su funcionalidad. Verifique el estado o los servicios disponibles en ISE mediante el comando show application status ise a través de la CLI del nodo ISE. Este es un ejemplo de resultado que muestra el estado o los servicios disponibles en ISE.

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4101512
Database Server                        running          107 PROCESSES
Application Server                     running          4118209
Profiler Database                      running          4108739
ISE Indexing Engine                    running          4119606
AD Connector                           running          4121671
M&T Session Database                   running          4114154
M&T Log Processor                      running          4118388
Certificate Authority Service          running          4121560
EST Service                            running          61939
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          4105571
ISE API Gateway Database Service       running          4107770
ISE API Gateway Service                running          4113275
ISE pxGrid Direct Service              running          36228
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          4122893
ISE Prometheus Service                 running          4124896
ISE Grafana Service                    running          4128455
ISE MNT LogAnalytics Elasticsearch     running          4130784
ISE Logstash Service                   running          4135868
ISE Kibana Service                     running          4137540
ISE Native IPSec Service               running          4142286
MFC Profiler                           running          52667
```

Servicios disponibles en ISE.

Ahora eche un vistazo más de cerca a cada servicio en detalle.

Receptor de base de datos

El servicio Database Listener es un componente crítico que ayuda a gestionar la comunicación entre ISE y el servidor de base de datos. Escucha y procesa las solicitudes relacionadas con la base de datos, lo que garantiza que el sistema ISE pueda leer y escribir en la base de datos subyacente.

Puntos clave sobre el servicio Database Listener en ISE

1. Interfaz de comunicación: Actúa como puente de comunicación entre ISE y el servidor de bases de datos, lo que permite al sistema recuperar y almacenar datos como credenciales de usuario, información de sesión, políticas de red, etc.

2. Compatibilidad con bases de datos externas: ISE se puede configurar para utilizar una base de datos externa (como Oracle o Microsoft SQL Server) para la autenticación de usuarios y el almacenamiento de políticas. El servicio Database Listener Service garantiza que ISE pueda conectarse e interactuar con esta base de datos externa de forma segura y eficaz.

3. Gestión de datos: El servicio escucha las consultas de base de datos del sistema ISE y, a continuación, las traduce a las acciones adecuadas de la base de datos externa. Puede gestionar solicitudes como insertar, actualizar o eliminar registros, así como recuperar información de la base de datos.

4. Supervisión de estado de base de datos: Además de proporcionar el canal de comunicación, también ayuda a garantizar que la conexión a la base de datos externa sea estable y operativa. Si la conexión falla, ISE vuelve al almacenamiento local o entra en un modo degradado en función de la configuración.

Servidor de base de datos

El servicio Servidor de base de datos es responsable de administrar el almacenamiento y la recuperación de los datos utilizados por el sistema. Gestiona la interacción con la base de datos subyacente que ISE utiliza para almacenar la configuración, la información de políticas, los datos de usuario, los registros de autenticación, los perfiles de dispositivos y otra información necesaria.

Puntos clave sobre el servicio de servidor de bases de datos en ISE

1. Almacenamiento de datos internos: El servicio de servidor de base de datos administra principalmente la base de datos integrada interna que ISE utiliza para almacenar localmente los datos operativos. Esto incluye datos como registros de autenticación y autorización, perfiles de usuario, políticas de acceso a la red, información de terminales y dispositivos, información de sesión.

2. Base de datos incorporada: En la mayoría de las implementaciones de Cisco ISE, el sistema utiliza una base de datos PostgreSQL integrada para el almacenamiento local. El servicio Servidor de base de datos garantiza que esta base de datos funcione sin problemas y gestiona todas las consultas, actualizaciones y tareas de gestión relacionadas con los datos almacenados

en ella.

3. Integridad de la base de datos: El servicio garantiza que todas las transacciones se procesan correctamente y que se mantiene la integridad de la base de datos. Administra tareas como el bloqueo de registros, la administración de conexiones a bases de datos y la ejecución de consultas a bases de datos.

Comprobar y solucionar problemas de inicialización o no ejecución de los servicios de receptor de base de datos y servidor de base de datos

El Receptor de Base de Datos y el Servidor de Base de Datos son servicios esenciales que deben ejecutarse juntos para que todos los demás servicios funcionen correctamente. Si estos servicios no se están ejecutando o están atascados durante la inicialización, estos pasos de solución de problemas ayudan en la recuperación.

1. Reinicie los servicios ISE mediante los comandos application stop ise y application start ise.

2. Si se trata de un nodo de VM, el reinicio del nodo desde la VM debe ayudar a la recuperación de los servicios.

3. Si el nodo es un nodo físico, reiniciar / recargar el nodo desde CIMC debe ayudar en la recuperación de servicios.

4. Si la base de datos está dañada, póngase en contacto con Cisco TAC para obtener más información sobre la solución de problemas.

El Receptor de base de datos y el Servidor de base de datos suelen desactivarse o no pueden iniciarse cuando hay una discrepancia en la base de datos o cuando la base de datos no se puede inicializar correctamente. En esos casos, la realización del restablecimiento de la aplicación mediante el comando application reset-config ise debe ayudar en la recuperación y el inicio nuevo de la base de datos. La ejecución del comando application reset-config ise elimina las configuraciones y los certificados, pero se conservan los detalles de la dirección IP y el nombre de dominio. Se recomienda ponerse en contacto con el TAC de Cisco para obtener más información y comprender el impacto potencial antes de aplicar este comando en cualquier nodo de la implementación.

Servidor de aplicaciones

El servidor de aplicaciones es un componente clave responsable de ejecutar y administrar la funcionalidad y los servicios principales de la plataforma ISE. Aloja la lógica empresarial, las interfaces de usuario y los servicios que permiten a ISE desempeñar su función de control de acceso a la red, autenticación, autorización, contabilidad y gestión de políticas.

Puntos clave sobre el servicio de servidor de aplicaciones en ISE

1. Interfaz de usuario (IU): El servicio de servidor de aplicaciones es responsable de representar la interfaz de usuario (IU) basada en Web para ISE. Esto permite a los administradores configurar y administrar políticas, ver registros e informes e interactuar con otras funciones de ISE.

2. Gestión de servicios: Se encarga de gestionar los diferentes servicios que proporciona ISE, incluida la gestión de políticas, las tareas administrativas y la comunicación con otros nodos de ISE en una implementación distribuida.

3. Procesamiento centralizado: El servicio de servidor de aplicaciones desempeña un papel central en la arquitectura de ISE, ya que proporciona la lógica que da sentido a las políticas, las solicitudes de autenticación y los datos de los dispositivos de red, los directorios y los servicios externos.

La verificación del servidor de aplicaciones se está inicializando o no se está ejecutando

El servidor de aplicaciones depende de pocas aplicaciones Web, como certificados, recursos, implementación o licencias. Cuando alguna de las aplicaciones Web no se pudo inicializar, el servidor de aplicaciones permanece bloqueado en el estado de inicialización. El servidor de aplicaciones tarda entre 15 y 35 minutos en pasar del estado **No en ejecución** → **Inicializando** → **En ejecución**, según los datos de configuración del nodo.

1. Asegúrese de que el certificado de administración de ISE es válido y está activo en la implementación para todos los nodos.
2. Asegúrese de que todos los nodos de la implementación están sincronizados con el nodo Administrador principal.
3. Si el nodo es una VM, asegúrese de que los recursos recomendados están asignados al nodo.

Verifique el estado del servidor de aplicaciones mediante el comando **show application status ise** de la CLI del nodo ISE. La mayoría de los registros relacionados con el servidor de aplicaciones están disponibles en el

Archivos Catalina.Out y Localhost.log.

Si se cumplen las condiciones mencionadas y el servidor de aplicaciones permanece bloqueado en el estado de inicialización, proteja el paquete de soporte de CLI/GUI de ISE. Recupere o reinicie los servicios mediante los comandos application stop ise y application start ise.

Base de datos Profiler

Profiler Database es una base de datos especializada que se utiliza para almacenar información sobre dispositivos de red, terminales y perfiles de dispositivo detectados por el servicio Profiler. El generador de perfiles es un componente fundamental de ISE que identifica y clasifica automáticamente los dispositivos de red (como ordenadores, smartphones, impresoras, dispositivos de IoT, etc.) en función de las características y los comportamientos de la red.

Puntos clave sobre el servicio Profiler Database en ISE

1. Definición de perfiles de dispositivos: La función principal del servicio de base de datos de perfiles es prestar apoyo al proceso de creación de perfiles. ISE utiliza este servicio para almacenar la información que recopila durante la creación de perfiles, como por ejemplo:

- Tipo de dispositivo (por ejemplo: smartphone, portátil, impresora, dispositivo IoT)
- Sistema operativo del dispositivo (por ejemplo: Windows®, macOS®, Cisco IOS® y Android®)
- Fabricante del dispositivo
- Patrones o comportamientos de red que ayudan a clasificar los dispositivos

2. Información del analizador: Almacena los atributos del generador de perfiles, como los perfiles de software y hardware del dispositivo, que se utilizan para hacer coincidir los dispositivos con las políticas predefinidas. Esta información también se utiliza para asignar dinámicamente dispositivos a las políticas de acceso a la red o VLAN correctas en función de su perfil.

3. Proceso de definición de perfiles: El proceso de creación de perfiles se basa normalmente en:

- Perfiles activos: ISE solicita información activamente a los dispositivos de la red.
- Perfiles pasivos: ISE recopila datos de forma pasiva del tráfico de red, como solicitudes DHCP, atributos RADIUS, encabezados HTTP y otros protocolos de red, para determinar el tipo de dispositivo.

Verificación y solución de problemas de ISE Profiling Services

1. Desde ISE CLI, ejecute el comando show application status ise para verificar que se está ejecutando el servicio de base de datos del generador de perfiles.

2. Desde GUI del nodo de administración principal, navegue hasta Administration > Deployment > select the node. Haga clic en Editar y verifique que los servicios de sesión y los servicios de perfiles estén habilitados.

3. Ahora, navegue hasta Administration > Deployment > Select the node. Pase a la configuración del analizador y verifique si los sondeos necesarios están habilitados para proteger los datos de los terminales.

4. Navegue hasta Administration > System > Profiling y verifique la configuración del generador de perfiles configurado para CoA.

5. Desde Visibilidad del contexto > Terminales > Seleccione los terminales y verifique los atributos recopilados por diferentes sondeos para los terminales.

Depuraciones útiles para la resolución de problemas de perfiles:

- profiler (profiler.log)
- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise.psc.log)

Motor de indexación ISE

Indexing Engine es un servicio responsable de buscar, indexar y recuperar de forma eficaz los datos almacenados en la base de datos de ISE. Mejora el rendimiento y la escalabilidad de ISE, especialmente cuando se trata de gestionar grandes volúmenes de datos y proporcionar un acceso rápido a la información necesaria para las tareas de autenticación, autorización, supervisión y generación de informes.

Puntos clave sobre el motor de indexación de ISE en ISE

1. Indización de datos: El motor de indexación de ISE crea índices para varios tipos de datos

almacenados en ISE, como registros de autenticación, registros de sesión, aciertos de políticas, datos de definición de perfiles y registros de acceso a la red. La indización ayuda a organizar estos datos de forma que las búsquedas y consultas sean más eficaces.

2. Gestión de registros e informes: Este servicio desempeña un papel fundamental en la gestión de registros al mejorar el rendimiento de los informes y las consultas de registros. Por ejemplo, cuando se buscan eventos de autenticación específicos, el motor de indexación permite una recuperación más rápida de los registros deseados, lo que es fundamental para la supervisión de la seguridad y la generación de informes de conformidad.

3.Recuperación de datos: El motor de indexación también es responsable de garantizar que ISE pueda recuperar eficazmente los datos indexados de su base de datos subyacente cuando sea necesario. Esto permite a ISE proporcionar respuestas rápidas a las consultas de la interfaz de usuario, las herramientas externas o las API.

Compruebe que el motor de indexación de ISE no se está ejecutando o inicializando

1. Verifique que las búsquedas de DNS directo e inverso estén funcionando para todos los nodos del clúster a través de CLI mediante el comando **nslookup <FQDN / IP address of the ISE node >** .
2. Verifique que los certificados de administración de ISE sean válidos y estén activos para todos los nodos del clúster.
3. Verifique que NTP esté funcionando y sincronizado con los nodos ISE a través de CLI mediante el comando **show ntp**.

El motor de indexación lo utiliza la visibilidad del contexto y el motor de indexación debe estar activo y en ejecución para que funcione la visibilidad del contexto. Los registros útiles que podrían ayudar con la resolución de problemas de Indexing Engine son los archivos **ADE.log** que podrían protegerse del paquete de soporte o seguirse a través de CLI mediante el comando **show logging system ade/ADE.log tail** durante el problema.

Conector AD

El conector de AD (conector de Active Directory) es un servicio que permite a ISE integrarse con Microsoft Active Directory (AD), lo que permite a ISE autenticar, autorizar y administrar usuarios en función de sus credenciales de AD y pertenencias a grupos. El conector de AD sirve de puente entre ISE y Active Directory, lo que permite a ISE aprovechar AD para el control de acceso a la red (NAC) y la aplicación de políticas.

Funciones clave del servicio del conector de AD en ISE

1. Integración con Active Directory: El servicio del conector de AD actúa como puente entre ISE y Active Directory. Permite a ISE conectarse de forma segura a AD, lo que posibilita que ISE utilice AD como almacén de identidades centralizado para la autenticación de usuarios y la aplicación de políticas.

2. Sincronización: El servicio del conector de AD admite la sincronización de los datos de usuario y grupo de Active Directory a ISE. Esto garantiza que ISE disponga de información actualizada sobre usuarios y grupos, lo que resulta crucial para la aplicación precisa de políticas.

3. Comunicación segura: El servicio del conector de AD establece canales de comunicación

seguros entre ISE y Active Directory, normalmente mediante protocolos como LDAP sobre SSL (LDAPS) para garantizar la integridad y la privacidad de los datos durante los procesos de autenticación y consulta.

4. Compatibilidad con múltiples dominios de Active Directory: El servicio puede admitir conexiones a varios dominios de Active Directory. Esto resulta especialmente útil en entornos grandes o de varios dominios, en los que ISE necesita autenticar a usuarios de diferentes dominios o bosques de AD.

5. Búsqueda de usuarios y grupos: Permite a ISE consultar a AD la información de usuarios y grupos. Esto puede incluir detalles como nombres de usuario, pertenencia a grupos y otros atributos de usuario que se pueden utilizar para aplicar políticas de acceso a la red. Por ejemplo, las políticas de acceso a la red se pueden aplicar en función de la pertenencia a un grupo AD de usuarios (por ejemplo: otorgar diferentes niveles de acceso a usuarios de diferentes grupos).

1. Verifique si NTP está sincronizado con los nodos y que la diferencia de tiempo entre AD e ISE sea inferior a 5 minutos.

2. Compruebe si el servidor DNS puede resolver los FQDN y dominios relacionados con AD.

3. Vaya a **Operaciones** > **Informes** > **Informes** > **Diagnósticos** > **Operaciones del conector AD**, verifique los eventos o informes relacionados con AD.

Los registros útiles para la solución de problemas son **ad_agent.log** con registros de depuración para el componente de **tiempo de ejecución**.

Base de datos de sesiones de M&T

M&T Session Database (Monitoring and Troubleshooting Session Database) juega un papel crítico en el almacenamiento y la administración de los datos relacionados con la sesión para los eventos de acceso a la red. La base de datos de sesiones de M&T contiene información sobre las sesiones activas, incluidas las autenticaciones de usuario, las conexiones de dispositivos y los eventos de acceso a la red, lo cual es esencial para monitorear, solucionar problemas y analizar la actividad de la red.

Funciones clave del servicio de base de datos de sesiones de M&T en ISE

1. Almacenamiento de datos de sesión: El servicio M&T Session Database es responsable de almacenar e indexar los datos sobre las sesiones de usuarios y dispositivos en la red. Esto incluye las horas de inicio y finalización de la sesión, los resultados de la autenticación, la identidad del usuario o del dispositivo y las políticas asociadas (como asignaciones de roles o asignaciones de VLAN). Los datos también incluyen información de cuentas RADIUS que detalla el ciclo de vida de la sesión, incluida la autenticación inicial y cualquier mensaje de cuentas que realice un seguimiento de los eventos de sesión.

2. Datos históricos y en tiempo real: El servicio proporciona acceso a datos de sesión en tiempo real (sesiones activas) y datos de sesión históricos (sesiones anteriores). Esto permite a los administradores no solo supervisar el acceso continuo de los usuarios, sino también consultar los registros de sesiones anteriores para investigar problemas o validar eventos de acceso. La

supervisión de sesiones en tiempo real puede ayudar a garantizar que no haya dispositivos no autorizados actualmente en la red.

3. Supervisión mejorada: Proporciona información sobre la actividad de los usuarios y los dispositivos, incluidas las políticas aplicadas a sus sesiones, lo que ayuda a detectar posibles problemas de seguridad o accesos no autorizados.

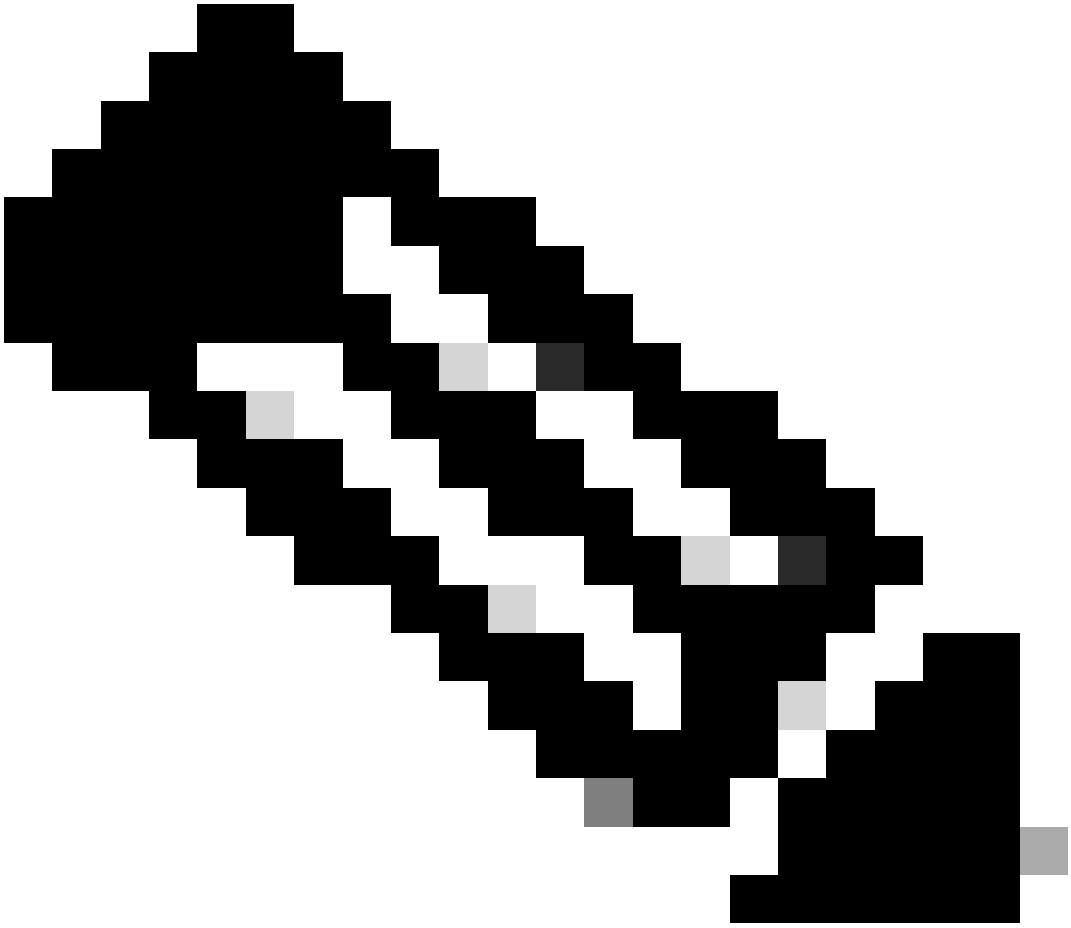
4. Auditoría e informes: Facilita la auditoría de cumplimiento y la generación de informes mediante el almacenamiento de un historial de eventos de acceso a la red y el suministro de datos para la generación de informes normativos.

Verificación y solución de problemas para la base de datos de sesiones de M&T en ISE

1. Compruebe si el nodo está asignado con los recursos recomendados.

2. Asegure **show tech-support** de ISE CLI para una verificación adicional del problema.

3. Restablezca la base de datos de la sesión de M&T ejecutando el comando **application configure ise** en a través de ISE CLI y seleccione la opción **1**.



Nota: El restablecimiento de la base de datos de M&T se debe realizar solamente después de verificar el impacto potencial en la implementación. Póngase en contacto con Cisco TAC para obtener más información.

Defectos conocidos

ID de bug de Cisco ·32364

Procesador de registro de M&T

M&T Log Processor (Monitoring and Troubleshooting Log Processor) es un componente responsable de recopilar, procesar y administrar los datos de registro generados por varios servicios dentro de ISE. Es una parte clave del marco de supervisión y solución de problemas (M&T), que ayuda a los administradores a supervisar y solucionar problemas de eventos de acceso a la red, intentos de autenticación, aplicación de políticas y otras actividades dentro del sistema ISE. El procesador de registro de M&T se encarga específicamente del procesamiento de las entradas del registro, lo que garantiza que ISE pueda almacenar, analizar y presentar la

información necesaria para la generación de informes, la auditoría y la resolución de problemas.

Funciones clave del servicio M&T Log Processor en ISE

1. Recopilación y procesamiento de registros: El servicio M&T Log Processor recopila y procesa registros generados por varios componentes de ISE, como solicitudes de autenticación, decisiones de autorización, mensajes de contabilidad y actividades de aplicación de políticas. Estos registros incluyen información detallada sobre usuarios, dispositivos e intentos de acceso a la red, como marcas de tiempo, ID de usuario, tipos de dispositivos, políticas aplicadas, éxito o fracaso de las solicitudes de acceso y motivos de los fallos.

2. Presentación de informes y cumplimiento: Los registros procesados por este servicio son cruciales para los informes de cumplimiento. Muchas regulaciones requieren que las organizaciones conserven registros de eventos de seguridad y acceso de usuarios. El servicio M&T Log Processor Service garantiza que todos los registros relevantes se procesen y estén disponibles para las auditorías de cumplimiento de las normas. Ayuda a generar informes detallados basados en datos de registro, como registros de acceso de usuarios, índices de aciertos/errores de autenticación o registros de aplicación de políticas.

Verificación y solución de problemas del servicio M&T Log Processor en ISE

1. Asegúrese de que el nodo de ISE esté implementado con los recursos recomendados según la Guía de instalación de Cisco.

2. Para verificar el problema, ejecute el comando **show logging system ade/ADE.log tail** a través de ISE CLI para obtener las excepciones/errores relevantes.

Defectos conocidos

ID de bug de Cisco ·15130

Servicio de autoridad certificadora

El servicio de autoridad certificadora (CA) es un componente fundamental que ayuda a administrar certificados digitales para proteger las comunicaciones y autenticar dispositivos, usuarios y servicios de red. Los certificados digitales son esenciales para establecer conexiones de confianza y garantizar una comunicación segura entre los clientes (ordenadores, smartphones, dispositivos de red) y los componentes de la infraestructura de red (switches, puntos de acceso inalámbricos, gateways VPN). El servicio de CA de Cisco ISE funciona junto con los certificados X.509, que se utilizan para diversos fines de seguridad de la red, incluidos la autenticación 802.1X, el acceso VPN, la comunicación segura y el cifrado SSL/TLS.

Funciones clave del servicio de autoridad certificadora en ISE

1. Gestión de certificados: El Servicio de autoridad certificadora es responsable de gestionar la creación, emisión, gestión y renovación de certificados digitales en ISE. Estos certificados se utilizan para diversos protocolos de autenticación y cifrado en toda la red. Puede actuar como

autoridad de certificación interna o integrarse con una CA externa (por ejemplo: Microsoft AD CS, CA públicas como VeriSign o DigiCert) para emitir certificados.

2. Expedición de certificados: Para entornos que requieren EAP-TLS o métodos de autenticación basados en certificados similares, ISE puede emitir certificados para dispositivos de acceso a la red (NAD), usuarios o terminales. ISE puede generar e implementar certificados automáticamente para autenticar dispositivos y usuarios, o puede solicitar certificados de una CA externa.

3. Inscripción de certificados: El servicio de CA admite la inscripción de certificados para terminales, como ordenadores portátiles, teléfonos y otros dispositivos de red, que necesitan autenticarse en la red mediante certificados. ISE utiliza protocolos como SCEP (protocolo simple de inscripción de certificados) o ACME (entorno automatizado de gestión de certificados) para facilitar la inscripción de certificados para los dispositivos.

4. Renovación de certificados: El servicio automatiza la renovación de los certificados a punto de vencer tanto para dispositivos como para usuarios. Garantiza que los certificados sean siempre válidos y estén actualizados, evitando así las interrupciones del servicio causadas por certificados caducados.

5. Integración con autoridades de certificación externas: aunque ISE puede actuar como su propia CA, es más habitual integrarla con una CA externa (por ejemplo: Servicios de certificados de Microsoft Active Directory). El servicio de CA puede administrar la interacción entre ISE y la CA externa, solicitando certificados para usuarios, dispositivos y recursos de red según sea necesario.

Servicio EST

El servicio de inscripción a través de transporte seguro (EST) es un protocolo que se utiliza para emitir certificados digitales de forma segura a los dispositivos de red y a los usuarios en un entorno de autenticación basado en certificados. EST es un protocolo de inscripción de certificados que permite a los dispositivos solicitar certificados de una entidad emisora de certificados (CA) de forma segura y automatizada. El servicio EST es especialmente útil para la autenticación de dispositivos, como en entornos 802.1X, conexiones VPN o escenarios BYOD (Bring Your Own Device, Traiga su propio dispositivo), en los que los dispositivos deben autenticarse en la red mediante certificados.

Funciones clave del servicio EST en ISE

1. Inscripción de certificados: El servicio EST es responsable de habilitar la inscripción de certificados seguros para los dispositivos (como switches, puntos de acceso o terminales) que requieren certificados con fines de autenticación. La inscripción se realiza a través de un transporte seguro (normalmente HTTPS), lo que garantiza que el proceso esté cifrado y protegido frente al acceso no autorizado.

2. Revocación y renovación de certificados: Una vez inscritos los certificados, el servicio EST también desempeña una función en la administración de la revocación o renovación de certificados. Por ejemplo, los dispositivos necesitan solicitar un nuevo certificado cuando vence el

actual y la prueba de compatibilidad puede ayudar a automatizar este proceso.

3. Control de acceso a la red mejorado: Al permitir que los dispositivos se autentiquen mediante certificados, el servicio EST refuerza la condición de seguridad de la red, especialmente en entornos que utilizan autenticación 802.1X.

Verifique que la autoridad certificadora y el servicio EST no estén en ejecución/inicializando

1. Vaya a **Administration > System > Certificates > Certificate Authority > Internal CA settings.** Asegúrese de que el estado del respondedor de CA, EST y OCSP esté ordenado y habilitado.
2. Las depuraciones útiles que podrían ayudar en la resolución de problemas son set , provisioning , ca-service y ca-service-cert. Consulte **toise-psc.log , catalina.out , caservice.log** y los archivos error.log.
3. Verifique que la CA raíz de ISE y los certificados de mensajería de ISE sean válidos en la implementación. Si se requiere la renovación de la CA raíz de ISE, navegue hasta **Administración > Certificados > Solicitudes de firma de certificado > Generar solicitud de firma de certificado,** seleccione uso como CA raíz de **ISE.** Haga clic en renovar **CA raíz de ISE**.

Servicio de motor SXP

El servicio SXP Engine es responsable de gestionar y facilitar la comunicación entre ISE y los dispositivos de red mediante la etiqueta de grupo de seguridad (SGT) y el protocolo de intercambio de grupos de seguridad (SXP). Desempeña un papel fundamental en el soporte de las políticas TrustSec, que se utilizan para aplicar el control de acceso a la red basado en el grupo de seguridad del dispositivo en lugar de solo las direcciones IP o MAC. El motor SXP de ISE se utiliza principalmente para el intercambio de información de grupos de seguridad, que ayuda a aplicar políticas basadas en la identidad, aplicación y ubicación del usuario o del dispositivo. Permite a los dispositivos compartir etiquetas de grupos de seguridad (SGT), que se utilizan para aplicar políticas de seguridad en los dispositivos de red, como routers y switches.

Funciones clave del servicio SXP Engine en ISE

1.Integración con TrustSec: SXP se suele implementar en entornos que aprovechan Cisco TrustSec, una solución que aplica políticas de seguridad uniformes en redes por cable e inalámbricas. El motor SXP facilita la comunicación de SGT entre dispositivos, lo que permite la aplicación de políticas dinámicas basadas en el contexto de seguridad de un dispositivo o usuario.

2. Etiquetas de grupos de seguridad (SGT): El núcleo de la aplicación de políticas de TrustSec gira en torno a las SGT. Estas etiquetas se utilizan para clasificar el tráfico de red y el protocolo SXP ayuda a compartir la asignación de estas etiquetas con usuarios o dispositivos específicos. Esto permite un control granular basado en políticas sobre el acceso a la red y el flujo de tráfico.

Verificación y solución de problemas para el servicio SXP Engine en ISE

1. De forma predeterminada, el servicio SXP Engine está deshabilitado en ISE. Para habilitarlo, vaya a **ISE GUI > Administration > Deployment, seleccione el nodo. Marque la casilla Enable SXP Service** y elija la interfaz. A continuación, verifique el estado del servicio SXP Engine desde la CLI de ISE mediante el comando **show application status ise.**

2. Si hay problemas de comunicación de red, verifique que la interfaz asignada al motor SXP tenga una dirección IP válida mediante el comando show interface en la CLI, y asegúrese de que la subred IP esté permitida en la red.

3.Compruebe los registros en directo de RADIUS para verificar los eventos de conexión SXP en ISE.

4.Habilite el componente SXP en los nodos ISE para depurar y capturar los registros y excepciones relevantes relacionados con SXP.

Servicio TC-NAC

El servicio TC-NAC (TrustSec Network Access Control) es un componente que facilita la aplicación de políticas TrustSec en dispositivos de red, garantizando que el control de acceso se basa en etiquetas de grupos de seguridad (SGT) en lugar de en direcciones IP o MAC tradicionales.

TrustSec, a su vez, es un marco desarrollado por Cisco que permite la aplicación de políticas de seguridad en toda la red en función de las funciones de los dispositivos, los usuarios o los contextos, en lugar de utilizar mecanismos heredados como VLAN o direcciones IP. Proporciona un control de acceso a la red más granular y dinámico al agrupar los dispositivos en diferentes grupos de seguridad y etiquetarlos con SGT.

Funciones clave del servicio TC-NAC en ISE

1. Integración con sistemas NAC de terceros: El servicio TC-NAC permite a ISE comunicarse e interactuar con soluciones de control de acceso a la red de terceros. Esto puede resultar útil para organizaciones que ya cuentan con una infraestructura de NAC pero desean integrarla con Cisco ISE para mejorar la funcionalidad, aprovechar las políticas de seguridad adicionales o aprovechar otras funciones de seguridad de la red de Cisco.

2. Proporcionar una aplicación de políticas sin problemas: Cuando se integra con soluciones de NAC de terceros, ISE puede hacerse cargo de determinados aspectos de la aplicación de políticas y la toma de decisiones. Esto permite un marco de políticas más unificado, lo que garantiza que las políticas aplicadas por los sistemas Cisco y no Cisco NAC sean coherentes en toda la red.

3. Compatibilidad con sistemas NAC heredados: El servicio TC-NAC ayuda a las organizaciones que ya cuentan con sistemas NAC antiguos, permitiéndoles seguir utilizando esos sistemas mientras adoptan Cisco ISE por sus funciones de seguridad mejoradas. ISE se puede integrar con soluciones de NAC anteriores y ampliar su ciclo de vida, proporcionando control de acceso, seguridad y aplicación de conformidad en conjunto.

4. Facilitación de la comunicación de proveedores de NAC de terceros: Este servicio permite a ISE facilitar la comunicación con soluciones de NAC de terceros que utilizan protocolos o estándares propios. ISE puede interactuar con sistemas NAC de terceros mediante protocolos estándar del sector (como RADIUS, TACACS+ o SNMP) o API personalizadas, en función de la solución NAC específica que se utilice.

Verificación y solución de problemas del servicio TC-NAC en ISE

1. Verifique que Threat Centric NAC esté habilitado navegando hasta **Administration > Deployment > PSN node > Enable Threat Centric NAC**.

2. Si el problema se produce con el adaptador FireAMP de SourceFire, compruebe si el **puerto 443** está permitido en la red.

3. Verifique los detalles de la sesión de terminal desde **Operations** > **Threat-Centric NAC Live Logs.**

Alarmas activadas por NAC centrado en amenazas:

- Adaptador no accesible (ID de syslog: 91002): Indica que no se puede alcanzar el adaptador.
- Error en la conexión del adaptador (ID de syslog: 91018): Indica que el adaptador es accesible pero la conexión entre el adaptador y el servidor de origen está inactiva.
- Adaptador detenido debido a un error (ID de syslog: 91006): Esta alarma se activa si el adaptador no se encuentra en el estado deseado. Si aparece esta alarma, compruebe la configuración del adaptador y la conectividad del servidor. Consulte los registros del adaptador para obtener más detalles.
- Error del adaptador (ID de syslog: 91009): Indica que el adaptador de Qualys no puede establecer una conexión ni descargar información del sitio de Qualys.

Depuraciones útiles para resolver problemas de TC-NAC:

- va-runtime (varuntime.log)
- va-service (varuntime.log y vaaggregation.log)
- TC-NAC (ise-psc.log)
- anc (ise-psc.log)

Servicio WMI de PassiveID

El servicio WMI de PassiveID es un servicio que permite a ISE realizar la creación de perfiles de dispositivos mediante Instrumental de administración de Windows (WMI) como mecanismo pasivo para identificar y crear perfiles de extremos en la red. Desempeña un papel fundamental en la creación de perfiles de dispositivos, especialmente en entornos en los que los dispositivos que ejecutan el sistema operativo Windows deben identificarse con precisión para el control de acceso a la red y la aplicación de políticas.

Funciones clave del servicio WMI PassiveID en ISE

1. Recopilación de identidad del dispositivo: El servicio WMI de PassiveID permite a ISE recopilar información de identidad de forma pasiva de los dispositivos Windows mediante el Instrumental de administración de Windows (WMI). Recopila los detalles del sistema, como el nombre de host del dispositivo, la versión del sistema operativo y otros atributos relevantes sin que sea necesario

que el dispositivo participe activamente.

2. Integración con la política de ISE: La información recopilada por el servicio WMI de PassiveID se integra en el marco de políticas de ISE. Ayuda en la aplicación dinámica de políticas basadas en atributos de dispositivos como el tipo, el sistema operativo y el cumplimiento de los estándares de seguridad.

Comprobar y solucionar problemas del servicio WMI de PassiveID

Una fuente muy segura y precisa, así como la más común, desde la que recibir información del usuario. Como sondeo, AD funciona con la tecnología WMI para proporcionar identidades de usuario autenticadas.Además, el propio AD, en lugar de sondeo, funciona como un sistema de origen (un proveedor) desde el que otros sondeos también recuperan datos de usuario.

Depuraciones útiles e información necesaria para solucionar problemas. Establezca estos atributos en el nivel de depuración para problemas WMI de PassiveID:

- PassiveID (passiveid*)
- registro en tiempo de ejecución (port-server.log)
- Active Directory (ad)_agent.log): nivel de seguimiento
- (collector.log) (en nodos PassiveID,MnT y en nodo pxGrid activo si se publican sesiones)
- pxGrid (pxgrid/) (en MnT secundario y nodo pxGrid activo si se publican las sesiones)

Información necesaria para solucionar problemas de PassiveID WMI:

1. ¿Si funcionaba antes? Cualquier cambio realizado recientemente. (Como la actualización, instalación de parches en ISE/actualización en DC)
2. ¿Funciona correctamente la conexión de prueba? (Antes de la integración, compruebe la conexión de prueba)
3. Detalles sobre el nombre de usuario utilizado para unirse a AD y el nombre de usuario utilizado para WMI. (ya sea una cuenta de administrador o no)
4. Compruebe si los eventos (4768, 4770) del DC están registrados. (Registro del visor de eventos del DC)
5. Registros de captura: Establezca el nivel de depuración para ID pasivo y registro en tiempo de ejecución y, a continuación, configure wmi para ese DC, AD - nivel de seguimiento con marca de tiempo.

Servicio de Syslog de PassiveID

El servicio de registro del sistema PassiveID es un servicio que habilita la función de generación de perfiles PassiveID para recopilar y procesar mensajes de registro del sistema de dispositivos de red en el entorno. Estos mensajes de syslog contienen información importante sobre los terminales conectados a la red, e ISE los utiliza para crear perfiles de estos dispositivos para el control de acceso a la red y la aplicación de políticas.

Funciones clave del servicio Syslog de ID pasiva

1. Autenticación pasiva: El servicio Syslog de ID pasiva permite a Cisco ISE autenticar usuarios y dispositivos de forma pasiva mediante la recopilación de mensajes de syslog de dispositivos de red (como switches o routers) que indican la actividad del usuario y del dispositivo. Esto resulta útil en situaciones en las que los métodos de autenticación activos tradicionales, como 802.1X, no son adecuados o viables.

2. Registro de eventos: El servicio Syslog de ID pasiva se basa en el protocolo syslog para recibir registros de los dispositivos de red que realizan un seguimiento del acceso y el comportamiento de los usuarios en la red. La información incluida en estos registros puede incluir elementos como intentos de inicio de sesión de dispositivos, puntos de acceso y detalles de la interfaz, que ayudan a ISE a identificar de forma pasiva el dispositivo o el usuario.

Servicio API PassiveID

El servicio API PassiveID es un servicio que permite la integración con sistemas que requieren información sobre la identidad de dispositivos o usuarios conectados a la red. Se suele utilizar en entornos en los que los administradores de red desean realizar políticas y acciones basadas en identidad sin necesidad de protocolos de autenticación de red activos, como 802.1X, para cada dispositivo.

Funciones clave del servicio API de ID pasiva

1. Integración con sistemas externos: La API de ID pasiva permite a ISE recibir información de identidad de sistemas o dispositivos de red de terceros (como switches, routers, firewalls o cualquier sistema que pueda generar eventos relacionados con la identidad). Estos sistemas externos pueden enviar información como mensajes de syslog, registros de autenticación u otros datos relevantes que pueden ayudar a ISE a identificar de forma pasiva a un usuario o dispositivo.

2. Autenticación pasiva: El servicio API de ID pasiva se utiliza para autenticar usuarios y dispositivos de forma pasiva mediante la recopilación de datos de identidad sin necesidad de autenticación activa (por ejemplo: sin necesidad de autenticación 802.1X, MAB o web). Por ejemplo, puede capturar información de dispositivos de red, registros de Active Directory o dispositivos de seguridad y utilizarla para identificar al usuario o dispositivo.

3. Asignación de información de identidad: La API de ID pasiva se puede utilizar para asignar datos de identidad a políticas de seguridad específicas. Esta información se utiliza para asignar de forma dinámica etiquetas de grupos de seguridad (SGT) o funciones a usuarios y dispositivos, lo que influye en la aplicación de los controles de acceso a la red (como las políticas de segmentación y firewall).

Servicio de agente PassiveID

El servicio de agente PassiveID es un servicio que permite la creación de perfiles de dispositivos mediante el uso de agentes PassiveID instalados en terminales (como equipos, portátiles, dispositivos móviles, etc.). El agente PassiveID permite a ISE recopilar información de definición de perfiles sobre los dispositivos de la red mediante la escucha del tráfico de los terminales, sin necesidad de análisis activos ni de interacciones directas con los dispositivos.

Funciones clave del servicio Passive ID Agent

1. Identificación pasiva de usuarios y dispositivos: El servicio Passive ID Agent es responsable de recopilar información relacionada con la identidad de forma pasiva, normalmente desde dispositivos de red o terminales, y de enviar estos datos a ISE. Este servicio permite a ISE autenticar e identificar a usuarios y dispositivos en función de sus actividades o características, sin necesidad de una autenticación activa del dispositivo (por ejemplo: sin credenciales 802.1X).

2. Integración con otros componentes de Cisco: El agente de ID pasiva trabaja en estrecha colaboración con los dispositivos de red de Cisco, como switches, controladores inalámbricos y puntos de acceso, para recopilar información relacionada con la identidad del tráfico de red, los registros del sistema u otros sistemas de gestión. También se puede integrar con Cisco TrustSec y Cisco Identity Services para asignar estos datos a etiquetas de grupos de seguridad (SGT) específicas u otras políticas basadas en identidad.

3. Control de acceso a la red contextual: El agente de ID pasiva envía esta información a Cisco ISE, que aplica las políticas de control de acceso adecuadas en función de la identidad y el contexto del usuario o dispositivo. Esto puede incluir:

- Control de acceso basado en roles.
- Asignación de VLAN dinámica.
- Segmentación de la red.
- Aplicación de políticas de seguridad basadas en la condición de seguridad del dispositivo o la función del usuario.

Servicio de terminal PassiveID

El servicio de terminales PassiveID es un servicio responsable de la identificación y creación de perfiles de los terminales (dispositivos) de la red en función de la tecnología PassiveID. Este servicio ayuda a ISE a recopilar, procesar y clasificar la información sobre los dispositivos que se conectan a la red, sin que sea necesaria una interacción activa con los propios terminales. El servicio de terminales PassiveID desempeña un papel fundamental en la definición de perfiles, el control de acceso a la red y la aplicación de políticas de seguridad.

Funciones clave del servicio de terminales PassiveID

1. Identificación pasiva de usuarios y dispositivos: El servicio de terminales PassiveID permite a Cisco ISE identificar y autenticar dispositivos en la red de forma pasiva, aprovechando la información de los registros de actividad de la red o del sistema. Esto incluye la identificación de usuarios y dispositivos en función del comportamiento o las características de la red, como la dirección MAC, la dirección IP o la información de inicio de sesión de un almacén de identidades externo como Active Directory (AD).

2. Recopilación de datos desde terminales: El servicio de terminales recopila varios tipos de datos específicos de terminales de diferentes orígenes:

- La información de inicio de sesión del usuario desde almacenes de identidad externos como

Active Directory u otros directorios.
- Características del dispositivo como las direcciones IP, las direcciones MAC y el tipo de dispositivo (por ejemplo: si el dispositivo es un PC con Windows, un teléfono móvil o un dispositivo con IoT).
- Actividad de red de terminales como solicitudes DHCP, solicitudes ARP y otras comunicaciones de capa de red.

Servicio SPAN de PassiveID

El servicio SPAN de PassiveID es un servicio que aprovecha la duplicación de puertos SPAN (analizador de puerto conmutado) en los dispositivos de red para capturar y analizar el tráfico de red con fines de definición de perfiles de terminales. Este servicio ayuda a ISE a recopilar información de forma pasiva sobre los terminales (dispositivos) de la red mediante el análisis de sus patrones de comunicación de red sin necesidad de sondeos activos ni de agentes instalados en los propios dispositivos.

Funciones clave del servicio SPAN de PassiveID

1. Recolección de identidad pasiva del tráfico SPAN: El servicio SPAN de PassiveID permite a ISE recopilar datos de identidad basados en el tráfico de red que se duplica o se copia a través de un puerto SPAN en un switch. Un puerto SPAN se utiliza normalmente para la supervisión de la red duplicando el tráfico de red de otros puertos o VLAN. Al capturar este tráfico, ISE puede recopilar información de identidad de forma pasiva, como:

- Direcciones MAC de los dispositivos.
- Direcciones IP asociadas a dispositivos.
- Solicitudes DHCP u otra información relacionada con la identidad del tráfico capturado.
- Registros de autenticación de dispositivos de red, como switches o controladores inalámbricos.

2. Captura de información de identidad de usuarios y dispositivos: El servicio SPAN esencialmente escucha el tráfico que pasa a través de la red e identifica la información de identidad clave de los paquetes de red sin necesidad de interactuar directamente con los dispositivos. Esto puede incluir datos como:

- Identidades de usuario cuando se autentican mediante protocolos como EAP (protocolo de autenticación extensible).
- Identidades de dispositivos basadas en direcciones MAC e IP.
- Roles y comportamientos de los dispositivos basados en los patrones de tráfico y eventos observados.

Verificación y solución de problemas para la pila PassiveID (servicio SPAN PassiveID, servicio Syslog PassiveID, servicio de punto final PassiveID, agente PassiveID, servicio API PassiveID)

1. La pila PassiveID es una lista de proveedores y todos los servicios de la pila PassiveID están inhabilitados de forma predeterminada. Vaya a ISE GUI > Administration > Deployment > Select the node, Enable Passive Identity Service, haga clic en Save . Para verificar el estado del servicio

de pila PassiveID, inicie sesión en la CLI del nodo ISE y ejecute el comando show application status ise.

2. Si hay problemas con el agente de ID pasiva, compruebe si el FQDN del agente se puede resolver desde el nodo ISE. Para ello, inicie sesión en la CLI de ISE y ejecute el comando nslookup < FQDN of Agent configured >.

3. Asegúrese de que el motor de indexación de ISE está activo y de que el DNS o el servidor de nombres configurado en ISE está resolviendo las búsquedas de DNS inverso y de reenvío.

4. Para garantizar una comunicación sin problemas con los proveedores de syslog, verifique que el puerto UDP 40514 y el puerto TCP 1468 estén abiertos en su red.

5. Para configurar el proveedor de SPAN en un nodo, asegúrese de que el servicio de identidad pasiva de ISE esté habilitado. Verifique que la interfaz que desea configurar en el proveedor SPAN esté disponible en ISE mediante el comando show interface de ISE CLI.

Para comprobar los registros, basados en el proveedor de ID pasiva, debe revisar passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log. Los registros mencionados se pueden proteger desde el paquete de soporte del nodo ISE.

Servidor DHCP (dhcpd)

El servicio Servidor DHCP (dhcpd) es un servicio que proporciona funcionalidad de Protocolo de configuración dinámica de host (DHCP) a los dispositivos de red. Se utiliza principalmente para asignar direcciones IP a dispositivos (terminales) que intentan conectarse a la red. En ISE, el servidor DHCP desempeña un papel fundamental a la hora de proporcionar direcciones IP a los terminales que las solicitan cuando se conectan a la red. El servicio también puede proporcionar información de configuración adicional, como servidores DNS, puerta de enlace predeterminada y otros parámetros de red.

Funciones clave del servicio de servidor DHCP (dhcpd) en ISE

1. Asignación dinámica de direcciones IP: El servicio dhcpd de ISE funciona como un servidor DHCP, que proporciona asignación de direcciones IP a los dispositivos que solicitan una dirección IP cuando se conectan a la red. Esto es importante en situaciones en las que los dispositivos se unen a la red de forma dinámica, como en entornos BYOD (Bring Your Own Device, Traiga su propio dispositivo) o cuando los dispositivos se configuran para obtener sus direcciones IP automáticamente.

2. DHCP basado en perfiles: El servicio dhcpd puede asignar direcciones IP en función del perfil del dispositivo. Si ISE ha definido el perfil del dispositivo (por ejemplo: si determina que se trata de un smartphone, un portátil o un dispositivo de IoT), puede asignar una dirección IP adecuada o aplicar otros ajustes según el tipo de dispositivo o función.

3. Soporte para DHCP Relay: ISE puede funcionar como agente de retransmisión DHCP y reenviar las solicitudes DHCP de los dispositivos a un servidor DHCP externo si ISE no gestiona la asignación de direcciones IP real. En este caso, el servicio dhcpd puede reenviar las solicitudes

de los dispositivos a un servidor DHCP central, mientras que ISE sigue aplicando políticas de red y controles de acceso.

Comprobar y solucionar problemas del servidor DHCP (dhcpd)

1. Póngase en contacto con el TAC de Cisco para comprobar si el paquete del servidor DHCP está instalado en ISE.

2. Inicie sesión en la raíz de **ISE > rpm -qi dhcp**.

Servidor DNS (con nombre)

El servicio de servidor DNS (con nombre) es un servicio que permite a ISE funcionar como servidor DNS (sistema de nombres de dominio) o resolución DNS. Es el principal responsable de resolver los nombres de dominio en direcciones IP y viceversa, facilitando la comunicación entre los dispositivos de la red.

Funciones clave del servicio de servidor DNS (con nombre) en ISE

1. Resolución DNS para la comunicación ISE: El servicio con nombre de ISE ayuda a convertir los nombres de dominio en direcciones IP. Esto es especialmente importante cuando ISE necesita conectarse a otros dispositivos de red o servicios externos (como servidores Radius, Active Directory o servidores NTP externos) mediante nombres de dominio en lugar de direcciones IP.

- Por ejemplo, cuando ISE necesita alcanzar un servidor Radius o un servicio de directorio externo (como Active Directory), debe resolver el nombre de dominio de ese servidor en una dirección IP.
- ISE consulta el servidor DNS configurado en el sistema para resolver estos nombres de dominio, lo que garantiza una comunicación fluida.

2. Resolución DNS para servicios externos: El servicio DNS permite a ISE conectarse a servicios externos que requieren nombres de dominio. Por ejemplo, ISE debe resolver los nombres de los servicios externos, como:

- Servicios basados en la nube.
- Servidores NTP (protocolo de tiempo de red).
- Autoridades de certificados (CA) o servidores LDAP.

3. Servidores DNS redundantes y multidominio: ISE se puede configurar para utilizar varios servidores DNS para obtener redundancia. En caso de que un servidor DNS deje de estar disponible, ISE puede recurrir a otro servidor DNS para garantizar el funcionamiento continuo y la resolución de DNS.

Comprobar y solucionar problemas del servidor DNS (con nombre)

1. Desde CLI del nodo ISE, verifique la disponibilidad del servidor de nombres o el servidor DNS de la implementación mediante el comando **ping <IP del servidor DNS / servidor de nombres>**.

2. Verifique la resolución DNS de los FQDN de ISE mediante el comando **nslookup <FQDN / IP address of ISE**

nodes> a través de ISE CLI.

Servicio de mensajería ISE

ISE Messaging Service es un componente que facilita la comunicación asíncrona entre diversos servicios y componentes dentro del sistema ISE. Desempeña un papel fundamental en la arquitectura general del sistema de ISE, ya que permite a las distintas partes de la plataforma enviar y recibir mensajes, gestionar tareas y sincronizar actividades.

Funciones clave del servicio de mensajería ISE

1. Comunicación entre procesos (IPC): El servicio de mensajería de ISE desempeña un papel fundamental a la hora de habilitar la comunicación entre procesos (IPC) entre los distintos servicios de ISE. Garantiza que los diferentes módulos y servicios de ISE, como la autenticación, la autorización y la aplicación de políticas, puedan intercambiar datos e instrucciones de forma coordinada.

2. Compatibilidad con entornos distribuidos: En implementaciones ISE más grandes o distribuidas (como en configuraciones de varios nodos o de alta disponibilidad), el servicio de mensajería ayuda a facilitar la comunicación entre los distintos nodos ISE. Esto garantiza que los datos, como las solicitudes de autenticación, las sesiones de usuario y las actualizaciones de políticas, se sincronizan correctamente en los diferentes nodos del sistema ISE.

3. Sincronización de políticas y configuraciones: El servicio de mensajería participa en la sincronización de configuraciones y políticas entre nodos ISE. Cuando se realizan cambios de configuración en un nodo principal, el servicio garantiza que estos cambios se propagan a nodos secundarios o de copia de seguridad en el sistema. Esto es esencial para mantener la coherencia y garantizar que las políticas de acceso a la red aplicadas en las diferentes ubicaciones o nodos ISE distribuidos permanezcan sincronizadas.

Comprobar que el servicio de mensajería ISE no se está ejecutando o inicializando

1. Verifique que el puerto TCP 8671 no esté bloqueado en el firewall, ya que este puerto se utiliza para la comunicación entre nodos entre dispositivos ISE.

2. Verifique si hay errores de link de cola y, si los hay, renueve los mensajes de ISE y los certificados de CA raíz de ISE, ya que los errores de link de cola normalmente se producirían debido a problemas de corrupción de certificados internos. Para resolver los errores de enlace de cola, renueve la mensajería ISE y el certificado de CA raíz de ISE consultando el artículo: ISE- Error de enlace de cola

3. En GUI -> Administration -> Certificates -> Select ISE Messaging Certificate. Haga clic en View (Ver) para verificar el estado del certificado.

Los registros útiles para resolver problemas del servicio de mensajería ISE son ade.log, que está disponible en el paquete de soporte o se puede seguir a través de CLI mediante el comando show logging system ade/ADE.log tail durante el problema.

4. Si el registro ADE.log muestra rabbitmq: errores de conexión rechazada, póngase en contacto

con Cisco TAC para eliminar el bloqueo del módulo Rabbitmq de la raíz de ISE.

Servicio de base de datos ISE API Gateway

El servicio de base de datos ISE API Gateway es un componente responsable de la gestión y el procesamiento de los datos relacionados con las solicitudes y respuestas API en el sistema ISE. Actúa como intermediario que conecta la puerta de enlace de la API de ISE con la base de datos de ISE, lo que garantiza que las aplicaciones personalizadas también puedan actualizar o modificar los datos de ISE (por ejemplo, ajustando las políticas de acceso o agregando o eliminando usuarios) a través de llamadas de API gestionadas por el servicio.

Funciones clave del servicio de base de datos ISE API Gateway

1. Acceso API a los datos de ISE: El servicio de base de datos ISE API Gateway actúa como un puente, lo que permite a las aplicaciones externas interactuar con la base de datos ISE a través de las API ISE RESTful. Estas API se pueden utilizar para recuperar o modificar datos almacenados en la base de datos de ISE, como:

- Registros de autenticación de usuario.
- Políticas de acceso a la red.
- Información de perfiles de dispositivos.
- Configuración y parámetros del sistema.

2. Habilitación de integraciones de sistemas externos: Este servicio desempeña un papel fundamental a la hora de integrar ISE con sistemas externos como:

- Servidores de autenticación externos (LDAP, Active Directory, RADIUS).
- Sistemas de gestión de redes (NMS).
- Soluciones de información de seguridad y gestión de eventos (SIEM).
- Aplicaciones o servicios personalizados que necesitan interactuar con los datos de ISE.

Al proporcionar acceso a API, el servicio de base de datos de gateway de API permite a estos sistemas externos consultar datos de ISE, enviar actualizaciones a ISE o desencadenar acciones específicas dentro de ISE en respuesta a eventos externos.

3. Apoyo a la comunicación API RESTful: ISE expone las API RESTful diseñadas para funcionar en HTTP/HTTPS. El servicio de base de datos de gateway de API es responsable de gestionar el flujo de solicitudes y respuestas de API, garantizando que las solicitudes se autentican y procesan, y que se devuelven los datos adecuados de la base de datos de ISE como respuesta.

Servicio ISE API Gateway

El servicio ISE API Gateway es un componente fundamental que proporciona acceso RESTful API a los servicios, datos y funcionalidades de ISE. Actúa como un puente entre ISE y los sistemas externos, lo que permite a estos sistemas interactuar mediante programación con el control de acceso a la red, la aplicación de políticas, la autenticación y otros servicios de ISE. API Gateway permite que aplicaciones de terceros, sistemas de administración de redes y

aplicaciones personalizadas interactúen con Cisco ISE sin necesidad de intervención manual o acceso directo a la interfaz de usuario de ISE.

Funciones clave del servicio ISE API Gateway

1. Habilitación del acceso API a ISE: El servicio ISE API Gateway permite que los sistemas externos accedan e interactúen de forma segura con las políticas y los datos de Cisco ISE mediante API RESTful. Esto proporciona acceso mediante programación a las funcionalidades de ISE, como la autenticación, la aplicación de políticas, la gestión de sesiones, etc.

2. Control programático: API Gateway Service permite el control programático de las funciones de ISE. Los administradores y desarrolladores pueden utilizar las API para:

- Recuperar o modificar directivas de red.
- Consultar o administrar sesiones de usuario y registros de autenticación.
- Cree y gestione reglas de control de acceso a la red.
- Acceder o actualizar perfiles de dispositivo.

Este control se puede aprovechar para la automatización o la orquestación de flujos de trabajo personalizados, como ajustar dinámicamente las políticas de acceso a la red basadas en datos en tiempo real o integrar ISE en una plataforma de automatización de la seguridad más amplia.

3. Supervisión y presentación de informes: El servicio de gateway de API permite que los sistemas externos recopilen datos de los registros operativos de ISE, el historial de sesiones y los detalles de aplicación de políticas. Esto es importante para:

- Informes de conformidad.
- Supervisión de la seguridad.
- Respuesta ante incidentes.

Las llamadas a API se pueden utilizar para extraer registros, información de auditoría y eventos, lo que permite a los equipos de seguridad supervisar las actividades de ISE desde un panel centralizado o una herramienta de generación de informes.

Verificación y solución de problemas del servicio ISE API Gateway y del servicio ISE API Gateway Database

1. Compruebe si el certificado de administrador del nodo ISE está activo y es válido. Vaya a Administration > Certificates > Select the node > Select Admin Certificate . Haga clic en Ver para verificar el estado del certificado de administrador del nodo de ISE.

2. Establezca los componentes ise-api-gateway, api-gateway, apiservice en debug y los registros se pueden seguir utilizando estos comandos:

- show logging application ise-psc.log tail
- show logging application api-gateway.log tail

Servicio ISE pxGrid Direct

El servicio ISE pxGrid Direct es un componente fundamental que admite la funcionalidad pxGrid (Platform Exchange Grid) en ISE. pxGrid es una tecnología de Cisco que facilita el uso compartido de datos seguro, estandarizado y escalable, así como la integración entre las soluciones de seguridad de red de Cisco y las aplicaciones, servicios y dispositivos de terceros. El servicio ISE pxGrid Direct permite la comunicación directa entre ISE y otros sistemas compatibles con pxGrid sin necesidad de dispositivos o servicios intermediarios.

Funciones clave del servicio ISE pxGrid Direct

1. Integración directa con sistemas de terceros: El servicio ISE pxGrid Direct permite a ISE integrarse directamente con sistemas de seguridad de red de terceros, como firewalls, routers, soluciones NAC, plataformas SIEM y otros appliances de seguridad. Permite a estos sistemas intercambiar información relativa a eventos de acceso a la red, incidentes de seguridad y datos contextuales de la red.

2. Intercambio de contexto: Una de las funciones principales de pxGrid es el uso compartido de información contextual (como las identidades de los dispositivos, las funciones de los usuarios, el estado de la seguridad y la información de acceso a la red). Con el servicio pxGrid Direct, ISE puede compartir directamente este contexto con otros dispositivos o aplicaciones sin depender de métodos tradicionales como RADIUS o TACACS+.

3. Comunicación simplificada: Gracias a pxGrid, ISE puede comunicarse e intercambiar información con soluciones de terceros mediante un protocolo estandarizado. Esto simplifica el proceso de integración, ya que no es necesario que los sistemas cuenten con integraciones personalizadas para cada solución de terceros.

4. Seguridad y cumplimiento mejorados: El servicio pxGrid Direct también mejora el estado de la seguridad y el cumplimiento de normativas al garantizar que todos los sistemas del ecosistema de la red tengan acceso a los mismos datos contextuales en tiempo real acerca de los usuarios, los dispositivos y las políticas de seguridad. Esto garantiza una aplicación más coordinada de las políticas de seguridad de la red en todo el entorno.

Verificar y solucionar problemas del servicio ISEPxgrid Direct

1. Póngase en contacto con Cisco TAC para verificar si **edda*.lock*** está presente en la carpeta /tmp. Si la respuesta es sí, Cisco TAC elimina el bloqueo y reinicia el servicio Pxgrid Direct desde la raíz.

2. Establezca el componente **PxGrid Direct** en debug en el nodo ISE para la solución de problemas. Los registros se pueden proteger mediante el paquete de soporte de ISE o la CLI de ISE mediante el uso de estos comandos:

show logging application pxgriddirect-service.log

show logging application pxgriddirect-connector.log

Los registros mencionados proporcionan información sobre los datos del terminal obtenidos y recibidos por Cisco ISE, junto con el estado de la conectividad de Pxgrid Connector.

Servicio de políticas de segmentación

El servicio de políticas de segmentación es un componente clave responsable de aplicar las políticas de segmentación de red basadas en la identidad del usuario, el estado del dispositivo u otra información contextual. Ayuda a controlar el acceso de usuarios y dispositivos a segmentos de red específicos, lo que garantiza que solo los usuarios autorizados o los dispositivos compatibles puedan acceder a determinadas partes de la red. La segmentación de la red es esencial para reducir la superficie de ataque de la red, evitar el movimiento lateral de las amenazas y garantizar el cumplimiento de las normativas. El servicio de políticas de segmentación de ISE se utiliza para aplicar estas reglas de segmentación de red de forma dinámica y flexible en toda la red.

Funciones clave del servicio de políticas de segmentación

1. Definición de Segmentos de Red: El servicio de políticas de segmentación de ISE permite a los administradores definir varios segmentos de red (subredes o VLAN) en función de las características de los usuarios o los dispositivos. Por ejemplo:

- Los dispositivos con diferentes estrategias de seguridad se pueden asignar a diferentes segmentos (por ejemplo: dispositivos de confianza en una VLAN y dispositivos no fiables en otra).
- Los usuarios de distintos departamentos o roles se pueden asignar a diferentes segmentos de red para aplicar el menor privilegio posible y restringir el acceso a recursos confidenciales.

2. Segmentación dinámica: Este servicio permite la segmentación dinámica de la red, lo que significa que los segmentos de red o las VLAN pueden cambiar en función de las condiciones en tiempo real. Por ejemplo:

- Un usuario se puede asignar a una VLAN específica en función de su rol o estado de salud del dispositivo.
- Un dispositivo que se considera no compatible o que ejecuta un sistema operativo obsoleto se puede mover a una cuarentena o a una VLAN de invitado hasta que se corrija.

3. Aplicación Basada En Políticas: El servicio de políticas de segmentación utiliza políticas para tomar decisiones sobre en qué segmento se debe colocar un dispositivo o usuario. Estas políticas pueden tener en cuenta varios factores, tales como:

- Identidad de usuario: En función del rol o atributos del usuario.
- Estado del dispositivo: El estado o el estado de cumplimiento del dispositivo (por ejemplo: ¿utiliza el software antivirus más reciente?).
- Ubicación: La ubicación física del usuario o dispositivo en la red (por ejemplo: oficina, área de invitados, acceso remoto).
- Hora de acceso: La hora del día o del día de la semana en que se realiza la solicitud de acceso.

4. Aplicación de las políticas de seguridad: El servicio de políticas de segmentación garantiza que las políticas de seguridad se aplican de forma uniforme en todos los dispositivos de red (como switches, routers y firewalls) aprovechando los estándares del sector, como la asignación de

VLAN y RADIUS. Esto permite que Cisco ISE se comunique con los dispositivos de infraestructura de la red para aplicar las políticas de segmentación necesarias.

Verificación y Troubleshooting del Servicio de Políticas de Segmentación

1. Verifique si la segmentación está configurada correctamente navegando hasta Centros de trabajo > TrustSec > Descripción general > Panel.

2. Centros de trabajo > TrustSec > Informes, seleccione informes TrustSec para verificar el estado y los informes del servicio de políticas de segmentación.

Servicio de autenticación REST

El servicio de autenticación REST es un servicio que proporciona funciones de autenticación mediante API RESTful. Permite que las aplicaciones y los sistemas externos autentiquen a los usuarios o dispositivos interactuando con ISE a través de HTTP(S) mediante protocolos REST estándar. Este servicio permite una integración perfecta de la funcionalidad de autenticación de Cisco ISE con aplicaciones o sistemas de terceros que necesitan autenticar usuarios o dispositivos pero que no pueden utilizar los métodos tradicionales (como RADIUS o TACACS+).

Funciones clave del servicio de autenticación REST

1. Autenticación RESTful: El servicio de autenticación REST habilita las solicitudes de autenticación a través del protocolo API REST. Esto permite utilizar sistemas externos (por ejemplo: aplicaciones, dispositivos de red de terceros o servicios) para autenticar a usuarios o dispositivos mediante ISE como servidor de autenticación, pero a través de llamadas de servicio web RESTful en lugar de los protocolos de autenticación tradicionales como RADIUS o TACACS+.

2. Integración con aplicaciones externas: Este servicio está diseñado para aplicaciones externas que necesitan autenticar usuarios o dispositivos, pero que no utilizan métodos de autenticación tradicionales (como RADIUS o TACACS+). En su lugar, pueden interactuar con ISE a través de las API REST, lo que simplifica la integración de la autenticación de ISE en aplicaciones basadas en la Web o nativas de la nube.

3. Autenticación flexible y escalable: El servicio de autenticación REST proporciona un método escalable de autenticación que no se limita solo a los dispositivos de red o las soluciones en las instalaciones. Pueden utilizarlo los servicios en la nube, las aplicaciones móviles y otras plataformas basadas en la Web que necesiten autenticar a usuarios o dispositivos consultando a ISE para obtener credenciales y políticas.

4. Fácil de aplicar: La API REST ofrece una interfaz estandarizada, que es más fácil de aplicar e integrar con software y aplicaciones modernas en comparación con los métodos tradicionales. Proporciona respuestas con formato JSON y utiliza métodos HTTP como GET, POST, PUT y DELETE, lo que hace que sea más accesible para los desarrolladores web y los sistemas que integran ISE para la autenticación.

Verificación y Troubleshooting de Rest Auth

1. Para resolver problemas relacionados con la API abierta, establezca el componente apiservice en debug.

2. Para resolver problemas relacionados con la API ERS, establezca el componente ers en debug.

Si la página GUI del servicio API: https://{iseip}:{port}/api/swagger-ui/index.html o https://{iseip}:9060/ers/sdk es accesible, concluye que el servicio API funciona según lo esperado.

Consulte Documentación de API para obtener más información sobre API.

Conector SSE

El conector SSE (Secure Software-Defined Edge Connector) es un servicio que integra ISE con la solución Cisco Secure Software-Defined Access (SD-Access). El conector SSE permite que ISE se comunique de forma segura con Cisco DNA Center, lo que permite la administración automatizada de políticas de red, segmentación y seguridad en el perímetro en un entorno de acceso SD.

Funciones clave del conector SSE

1. Integración con sistemas de seguridad de terceros: El conector SSE facilita la integración de Cisco ISE con sistemas de seguridad de terceros, como firewalls, sistemas de prevención de intrusiones (IPS), soluciones de control de acceso a la red (NAC) y sistemas de gestión de eventos e información de seguridad (SIEM). Permite a estos sistemas externos enviar o recibir datos de ISE de forma segura, lo que se puede utilizar para una aplicación de políticas más dinámica.

2. Inteligencia de amenazas en tiempo real: Al conectar ISE con otros sistemas de seguridad, el conector SSE permite el intercambio de inteligencia de amenazas en tiempo real. Esta información puede incluir actividad sospechosa, terminales comprometidos o comportamientos maliciosos detectados por otros sistemas de seguridad, lo que permite a ISE ajustar dinámicamente las políticas de acceso en función de los niveles de amenaza actuales o del estado del dispositivo.

3. Remediación automatizada: La integración habilitada por el conector SSE puede admitir flujos de trabajo de corrección automatizados. Por ejemplo, si un dispositivo de seguridad externo marca un sistema como comprometido, ISE puede aplicar automáticamente políticas que bloqueen el acceso a la red o redirijan el terminal a un segmento de red de corrección para una investigación más detallada.

Verifique y resuelva problemas del conector SSE

1. El conector SSE solo está habilitado cuando el servicio PassiveID está habilitado en ISE.

2. el componente sse-connector (connector.log) en la depuración proporciona más información sobre los mensajes relacionados con el conector SSE.

Hermes (pxGrid Cloud Agent)

Hermes (pxGrid Cloud Agent) es un componente que facilita la integración entre ISE y el ecosistema pxGrid (Platform Exchange Grid) en un entorno de nube. Hermes es el agente basado en la nube que se utiliza para habilitar la comunicación entre ISE y los servicios o plataformas basados en la nube. Es compatible con el marco pxGrid para compartir información contextual entre diferentes sistemas de red y seguridad.

Características y funciones clave de Hermes (pxGrid Cloud Agent)

1. Integración de la nube en las instalaciones: Hermes (pxGrid Cloud Agent) está diseñado para facilitar la integración perfecta entre los servicios basados en la nube y la infraestructura de ISE in situ. Amplía el poder de pxGrid más allá de los entornos de red in situ tradicionales, lo que permite el intercambio seguro de datos y la aplicación de políticas en aplicaciones y servicios basados en la nube.

2. Compatibilidad con el ecosistema pxGrid: pxGrid es una plataforma de Cisco para compartir de forma segura contexto e información entre las soluciones de seguridad de la red. Hermes actúa como agente de nube para pxGrid, lo que permite una comunicación segura y en tiempo real entre ISE y varios servicios basados en la nube. Esta integración permite que las políticas de seguridad de la red sean uniformes en los entornos in situ y en la nube, lo que facilita la gestión y la aplicación de la seguridad.

3. Visibilidad de terminales basada en la nube: Una de las principales ventajas de Hermes es que proporciona visibilidad en los terminales basados en la nube, de forma similar a como ISE proporciona visibilidad en los terminales in situ. Puede recopilar datos sobre los dispositivos y los usuarios en la nube, como su estado de conformidad, estado de seguridad e información de identidad. Esto permite a ISE aplicar políticas de acceso a la red en los terminales en la nube del mismo modo que lo haría para los dispositivos en las instalaciones.

4. Ampliación perfecta de ISE a entornos de nube: Una de las principales ventajas de Hermes es que proporciona un puente perfecto entre el entorno in situ de ISE y el creciente número de aplicaciones nativas de la nube. Esto facilita la ampliación de las políticas de seguridad, los métodos de autenticación y los controles de acceso de ISE a los servicios en la nube sin que sea necesario realizar una revisión completa de la infraestructura existente.

Verificar y solucionar problemas Hermes (agente de nube Pxgrid)

1. De forma predeterminada, el servicio Hermes está deshabilitado, la conexión de ISE con la nube de Cisco PxGrid habilita el servicio Hermes. Por lo tanto, si el servicio Hermes está deshabilitado en ISE, verifique si la opción Pxgrid Cloud está habilitada desde **ISE GUI > Administration > Deployment, seleccione el nodo ISE**. Edite y **habilite Pxgrid Cloud.**

2. Las depuraciones útiles para solucionar problemas relacionados con la nube de Pxgrid son **hermes.log** y

pxcloud.log. Estas depuraciones están disponibles únicamente en el nodo Pxgrid donde está habilitada Pxgrid Cloud.

McTrust (servicio Meraki Sync)

McTrust (servicio Meraki Sync) es un servicio que permite la integración entre los sistemas Cisco ISE y Cisco Meraki, específicamente para sincronizar y gestionar dispositivos de red y políticas de acceso. El servicio McTrust actúa como un conector que sincroniza la información de usuarios y dispositivos entre la infraestructura de red gestionada en la nube de Meraki y los sistemas de gestión de políticas e identidad in situ de ISE.

Características y funciones clave de McTrust (servicio Meraki Sync)

1. Integración perfecta con los dispositivos Meraki: McTrust permite a ISE sincronizarse e integrarse con los dispositivos gestionados en la nube de Meraki. Esto incluye dispositivos como puntos de acceso, switches y appliances de seguridad Meraki que forman parte de la cartera de productos de Meraki. Permite a ISE comunicarse directamente con la infraestructura de Meraki, lo que facilita la aplicación de políticas de control de acceso a la red a los dispositivos gestionados por Meraki.

2. Sincronización automática de dispositivos: El servicio Meraki Sync sincroniza automáticamente las políticas de ISE con los dispositivos de red Meraki. Esto significa que cualquier cambio realizado en las políticas de control de acceso a la red en ISE se refleja automáticamente en los dispositivos Meraki, sin necesidad de intervención manual. Esto facilita a los administradores la gestión del acceso a la red en las plataformas Meraki e ISE.

3. Aplicación de políticas para dispositivos gestionados por Meraki: McTrust permite a ISE aplicar políticas de acceso a la red en dispositivos Meraki en función de la autenticación y el estado del dispositivo. Puede asignar políticas de forma dinámica a elementos de la red Meraki, como ajustar las asignaciones de VLAN, aplicar listas de control de acceso (ACL) o restringir el acceso a determinados recursos de la red, en función de la condición en materia de seguridad del dispositivo o del usuario que solicite el acceso.

4. Integración de paneles de Meraki: McTrust integra ISE directamente con el panel de Meraki, proporcionando una interfaz de gestión unificada. Gracias a esta integración, los administradores pueden ver y gestionar las políticas de red y las reglas de control de acceso tanto de los dispositivos Meraki como de los recursos gestionados por ISE, todo ello desde la interfaz gestionada en la nube de Meraki.

Verificación y solución de problemas de McTrust (servicio Meraki Sync)

1. Inicie sesión en la GUI de ISE -> Centros de trabajo -> TrustSec -> Integraciones -> Estado de sincronización. Verifique cualquier problema o error observado.

2. Asegúrese de que todos los certificados de administrador de los nodos ISE estén activos y sean válidos.

La depuración útil para la resolución de problemas del servicio Meraki Sync es meraki-

connector.log.

Exportador de nodos de ISE

El servicio Exportador de nodos de ISE es un componente que se utiliza para supervisar y recopilar métricas de rendimiento del sistema ISE, específicamente de los nodos ISE (ya se trate de nodos de administración, de supervisión o de servicios de políticas).

Características y funciones clave del exportador de nodos de ISE

1.Exportación de la métrica: El Exportador de nodos de ISE proporciona diversas métricas relacionadas con el rendimiento, como el uso de la CPU, el uso de la memoria, el uso de discos, las estadísticas de red, la carga del sistema y otras métricas a nivel del sistema operativo. Estas métricas se utilizan para supervisar el estado y el rendimiento del nodo de ISE y se pueden visualizar en un panel de control como Grafana.

2. Supervisión del estado del sistema: Al exportar los datos de rendimiento a Prometheus, el Exportador de nodos de ISE permite una supervisión continua del estado y el estado operativo del nodo de ISE. Los administradores pueden crear alertas basadas en umbrales predefinidos para notificarles la degradación del rendimiento o los problemas del sistema.

3. Integración de Prometeo: El Exportador de nodos de ISE se suele utilizar junto con Prometheus, un kit de herramientas de supervisión y alertas de código abierto diseñado para ofrecer fiabilidad y escalabilidad. El Exportador de nodos expone métricas a nivel del sistema que Prometeo puede desechar para recopilar y almacenar datos de series temporales.

Servicio ISE Prometheus

El servicio ISE Prometheus es un servicio que integra Prometheus con ISE para permitir la supervisión y la recopilación de métricas de rendimiento del sistema ISE. Prometheus es un kit de herramientas de supervisión y alertas de código abierto que se utiliza para recopilar, almacenar y analizar datos de series temporales. Además, el servicio ISE Prometheus permite a ISE exponer sus métricas internas a Prometheus para fines de supervisión.

Características y funciones clave del servicio ISE Prometheus

1. Recopilación de indicadores para la supervisión: El servicio ISE Prometheus está diseñado para exportar diversas métricas operativas y de rendimiento relacionadas con el sistema ISE. Estas métricas normalmente incluyen, entre otras, la utilización de la CPU y la carga del sistema, el uso de la memoria, el uso del disco y el rendimiento de E/S, las estadísticas de red, las estadísticas de solicitud de autenticación, las estadísticas de aplicación de políticas, los datos de estado y tiempo de actividad del sistema

2. Integración de Prometeo: El servicio Prometheus permite que ISE exponga los datos en un formato compatible con Prometheus, que los recopila a intervalos regulares. A continuación, Prometheus almacena los datos en una base de datos de series temporales, lo que permite realizar un seguimiento de las tendencias y el rendimiento histórico del sistema ISE.

3. Visualización e informes con Grafana: El servicio Prometheus de ISE se integra a la perfección con Grafana, una popular herramienta de visualización de código abierto. Después de exportar las métricas a Prometheus, los administradores pueden utilizar paneles de Grafana para visualizar los datos en tiempo real. Esto permite identificar fácilmente los cuellos de botella de rendimiento, las tendencias del sistema y los posibles problemas en la implementación de ISE.

Servicio ISE Grafana

El servicio ISE Grafana es un servicio que proporciona visualización de las métricas de rendimiento del sistema mediante Grafana, una plataforma de código abierto para la supervisión y visualización de datos. Se integra con Prometheus para mostrar datos históricos y en tiempo real recopilados de ISE, lo que permite a los administradores crear paneles interactivos que proporcionan información sobre el estado, el rendimiento y el uso del sistema ISE.

Características y funciones clave del servicio ISE Grafana

1. Paneles personalizables: Grafana es altamente personalizable, lo que permite a los administradores crear y modificar tableros de acuerdo a sus necesidades específicas de monitoreo. Se pueden crear consultas personalizadas para extraer puntos de datos específicos de Prometeo, y esas consultas se pueden visualizar en varios formatos como gráficos, tablas, mapas de calor y más.

2. Supervisión centralizada para implementaciones ISE distribuidas: En el caso de las implementaciones ISE distribuidas, en las que se implementan varios nodos ISE en distintas ubicaciones, Grafana proporciona una vista centralizada de todas las métricas del sistema recopiladas de cada nodo. Esto permite a los administradores supervisar el rendimiento de toda la implementación de ISE desde una única ubicación.

3. Datos históricos y análisis de tendencias: Con los datos almacenados en Prometheus, Grafana permite el análisis histórico de las métricas del sistema, lo que permite a los administradores realizar un seguimiento de las tendencias a lo largo del tiempo. Por ejemplo, pueden supervisar cómo ha cambiado el uso de la CPU durante el último mes o cómo han fluctuado las tasas de éxito de autenticación. Estos datos históricos son valiosos para la planificación de la capacidad, el análisis de tendencias y la identificación de problemas a largo plazo.

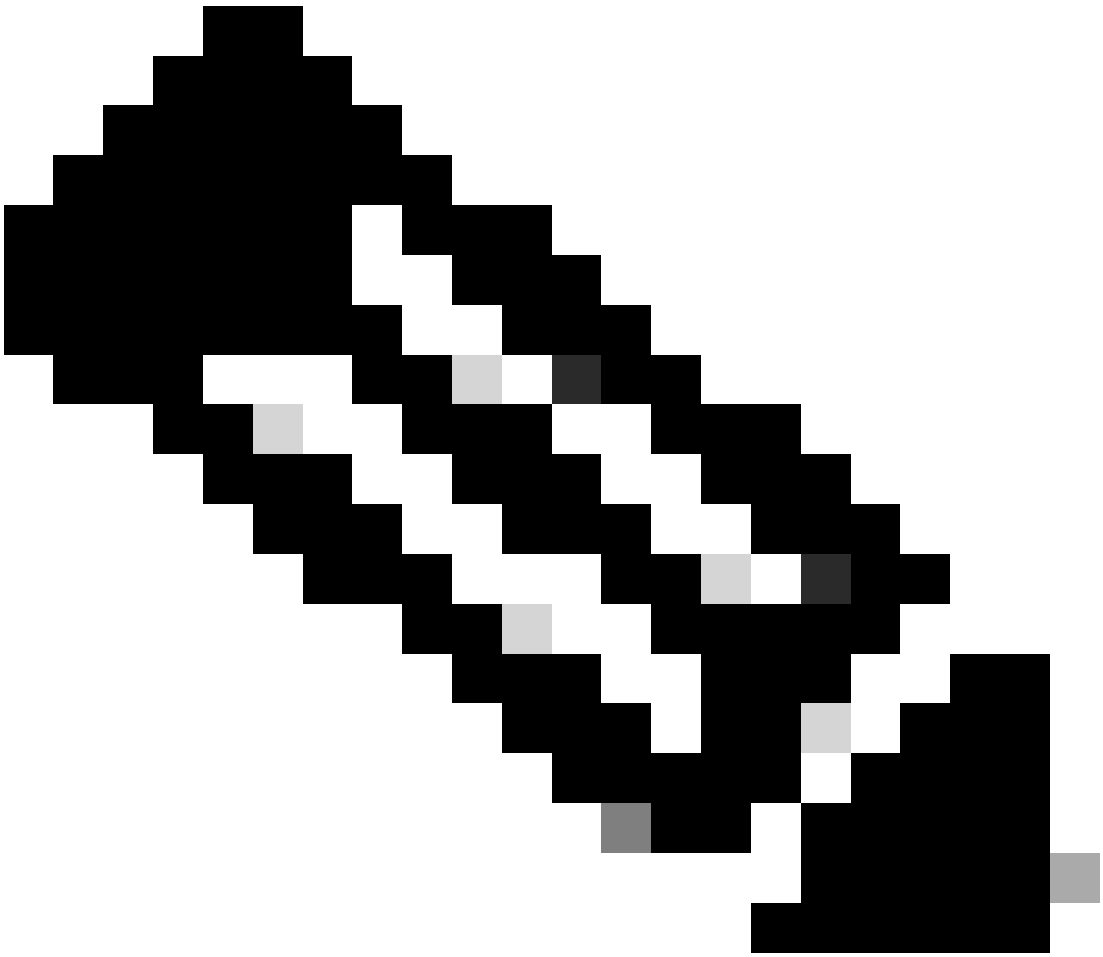
Verificar y solucionar problemas de ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter

1. El servicio ISE Grafana, el servicio ISE Prometheus y el servicio ISE Node Exporter funcionan juntos y se denominan servicios de pila Grafana. No hay depuraciones específicas que habilitar para solucionar problemas de estos servicios. Sin embargo, estos comandos ayudan en la resolución de problemas.

show logging application ise-prometheus/prometheus.log

show logging application ise-node-exporter/node-exporter.log

show logging application ise-grafana/grafana.log



Nota: Cuando la supervisión está activada, el exportador de nodos de ISE, el servicio ISE Prometheus y el servicio ISE Grafana deben estar en ejecución y la interrupción de cualquiera de estos servicios puede causar problemas durante la recopilación de datos.

ISE MNT LogAnalytics Elasticsearch

ISE MNT LogAnalytics Elasticsearch es un componente que integra Elasticsearch con las funciones de ISE Monitoring and Troubleshooting (MNT). Se utiliza para la agregación de registros, las búsquedas y los análisis relacionados con los registros y los eventos de ISE. Elasticsearch es un motor de análisis y búsqueda distribuido y ampliamente utilizado. Cuando se integra con ISE, mejora la capacidad del sistema para almacenar, analizar y visualizar los datos de registro generados por los componentes de ISE.

Características y funciones clave de ISE MNT LogAnalytics Elasticsearch

1. Almacenamiento e indexación de registros: El servicio Elastic Search de ISE es responsable de almacenar e indexar los datos de registro generados por ISE. Elasticsearch es un motor de análisis y búsqueda distribuida que permite almacenar los registros de ISE de forma que se

puedan realizar búsquedas rápidas, realizar consultas y recuperar eventos, errores o actividades del sistema específicos.

2. Integración con Log Analytics: ISE MNT LogAnalytics Elasticsearch funciona junto con Log Analytics para proporcionar una solución de registro completa. Permite a ISE recopilar datos de registro relacionados con la autenticación, la aplicación de políticas, las operaciones del sistema y otras actividades. Estos datos se almacenan en Elasticsearch, lo que facilita la realización de análisis detallados y la obtención de información sobre el comportamiento de ISE.

3. Registro centralizado: Al integrarse con Elasticsearch, ISE proporciona una solución de registro centralizada, lo que resulta crucial para los entornos que requieren una recopilación de registros distribuida. Esto permite a los administradores ver y analizar los registros de varios nodos de ISE en una única interfaz unificada, lo que facilita la solución de problemas y la supervisión del rendimiento de ISE.

4. Análisis de registro y solución de problemas: El servicio ISE MNT LogAnalytics Elasticsearch ayuda a los administradores a analizar el comportamiento del sistema y a solucionar problemas facilitando el acceso a los datos de registro. Por ejemplo, si se produce un pico repentino de errores de autenticación o una interrupción inesperada del sistema, Elasticsearch permite una consulta rápida de los datos de registro para identificar la causa raíz.

Verificar y solucionar problemas de ISE M&T LogAnalytics Elasticsearch

1. La desactivación y reactivación del servicio de análisis de registro en ISE debe ser de ayuda. Vaya a Operaciones > Sistema 360 > Configuración > Análisis de registro (desactivar y activar mediante la opción de alternancia).

2. El reinicio de M&T LogAnalytics desde la raíz de ISE resuelve el problema. Póngase en contacto con el TAC de Cisco para realizar esta acción.

Defectos conocidos

ID de bug de Cisco ·66198

Servicio Logstash de ISE

ISE Logstash Service es un componente que integra Logstash, una canalización de procesamiento de datos de código abierto, con ISE para la recopilación, transformación y reenvío de registros. Logstash actúa como recopilador de registros y reenviador de registros, lo que permite procesar los registros de ISE y enviarlos a otros sistemas para su análisis, almacenamiento y supervisión. Logstash es una potente herramienta de código abierto que recopila, analiza y reenvía registros u otros datos de diferentes fuentes a una ubicación central para su almacenamiento, análisis y visualización. En el contexto de ISE, el servicio ISE Logstash se utiliza para procesar y reenviar registros en un formato estructurado a un sistema de registro centralizado, donde se pueden analizar, supervisar y visualizar con más detalle.

Características y funciones clave del servicio ISE Logstash

1. Recopilación y reenvío de registros: La función principal del servicio ISE Logstash es recopilar datos de registro de varios componentes de ISE (como registros de autenticación, registros del sistema, registros de aplicación de políticas, etc.) y reenviarlos a una ubicación central (normalmente Elasticsearch u otro sistema de gestión de registros) para su almacenamiento y análisis.

2. Análisis de registro: Logstash puede analizar los registros recopilados en formatos estructurados. Procesa datos de registro sin procesar y extrae información significativa de ellos, transformando las entradas de registro en un formato que es más fácil de consultar y analizar. Esto puede implicar filtrar, analizar y enriquecer los datos antes de reenviarlos a Elasticsearch u otros sistemas.

Verificar y solucionar problemas del servicio ISE Logstash

1. No hay depuraciones específicas que habilitar. Sin embargo, **show logging application ise-logstash/logstash.log** proporciona información sobre el estado del servicio.

2. La desactivación y reactivación del servicio de análisis de registro en ISE debe ser de ayuda. Vaya a **Operaciones > Sistema 360 > Configuración > Análisis de registro** (deshabilitar y habilitar mediante la opción de alternancia).

Defectos conocidos relacionados con el servicio Logstash

ID de bug de Cisco ·74832

ID de bug de Cisco ·58596

Servicio ISE Kibana

ISE Kibana Service es un componente que integra Kibana, una herramienta de visualización de datos de código abierto, con la infraestructura de registro y supervisión de ISE. Kibana trabaja en conjunto con Elasticsearch (que almacena e indexa los datos de registro) para proporcionar una potente plataforma para visualizar, buscar y analizar los registros de ISE y las métricas de rendimiento.

Características y funciones clave del servicio ISE Kibana

1. Visualización de datos: El servicio ISE Kibana permite a los administradores crear representaciones visuales de los datos de registro recopilados de ISE. Esto puede incluir:

- Gráficos, gráficos y tablas para conocer las tendencias de autenticación, aplicación de políticas, actividad de los usuarios y estado del sistema.
- Gráficos circulares, gráficos de líneas y gráficos de barras para realizar un seguimiento de métricas específicas como el número de inicios de sesión fallidos, la duración de la sesión o los errores a lo largo del tiempo.

Verificación y solución de problemas del servicio ISE Kibana

1. Si el servicio de ISE kibana no se está ejecutando, desactive y vuelva a habilitar el análisis de

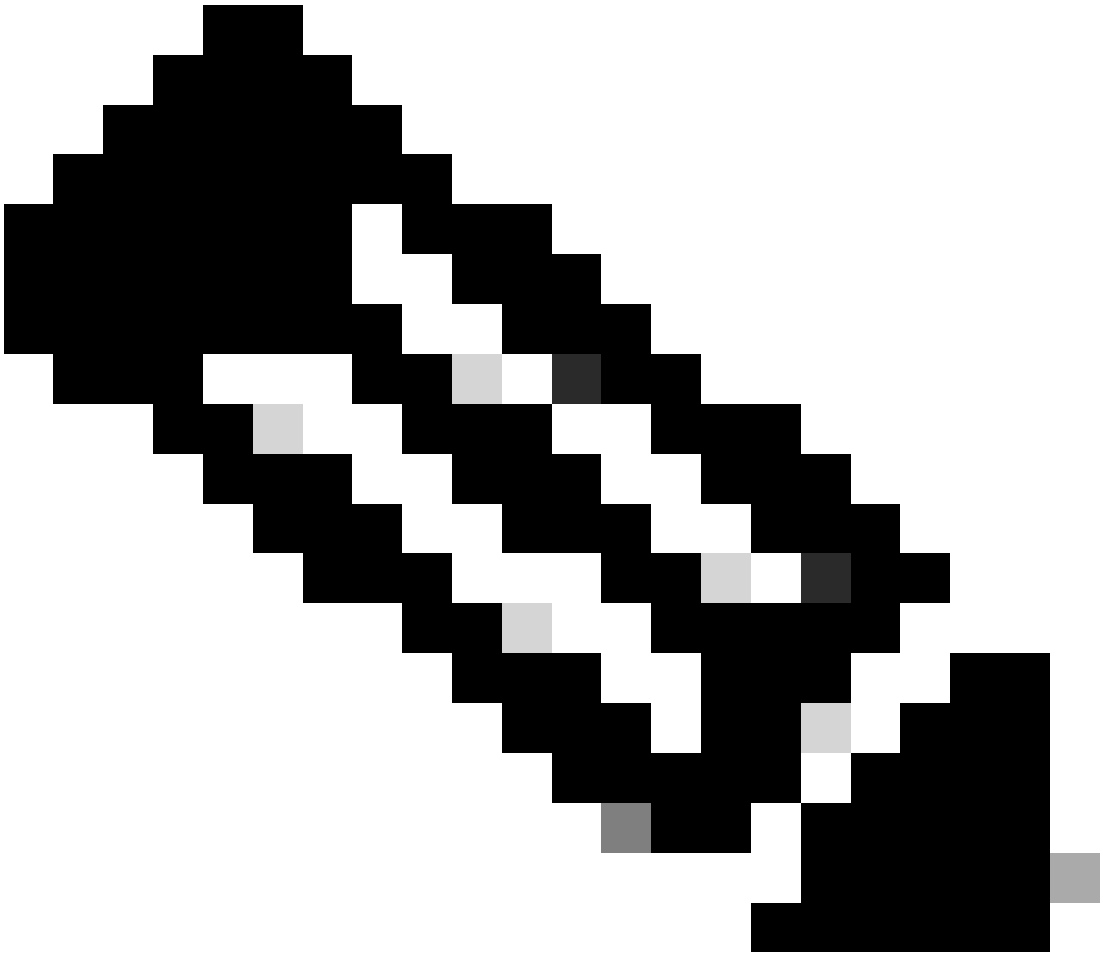
registros en ISE, navegue hasta Operaciones > Sistema 360 > Configuración, Análisis de registros (deshabilitar y habilitar mediante la opción de alternancia).

2. En muchos escenarios, puede haber una entrada duplicada en la carpeta /etc/hosts que debe estar causando un problema. Póngase en contacto con el TAC para eliminar la entrada duplicada.

Defectos conocidos relacionados con la cuestión de Kibana

ID de bug de Cisco ·78050

ID de bug de Cisco ·59848



Nota: Cuando Análisis de registro está habilitado, ISE MNT LogAnalytics Elasticsearch, ISE Logstash Service, ISE Kibana Service deben estar en ejecución y la interrupción de cualquiera de estos servicios genera problemas durante la recopilación de datos.

Servicio IPSec nativo de ISE

El servicio IPSec nativo de ISE hace referencia a la compatibilidad integrada con IPSec (seguridad de protocolo de Internet), que proporciona una comunicación segura entre nodos de ISE o entre ISE y otros dispositivos de red. IPSec es un conjunto de protocolos que se utilizan para proteger las comunicaciones de red mediante la autenticación y el cifrado de cada paquete IP en una sesión de comunicación.El servicio IPSec nativo forma parte del marco más amplio de seguridad y gestión de acceso a la red. Proporciona funciones para gestionar y gestionar conexiones VPN IPsec, lo que garantiza que los datos transmitidos entre el sistema ISE y los terminales remotos sean seguros. Esto podría implicar interacciones con dispositivos cliente, dispositivos de acceso a la red (como routers o firewalls) o incluso otros nodos ISE, donde el cifrado IPsec y la tunelización son necesarios para proteger la información confidencial.

Características y funciones clave del servicio IPSec nativo de ISE

1. Comunicación segura a través de IPsec: La función principal del servicio IPSec nativo de ISE es establecer y mantener canales de comunicación seguros mediante IPsec. Esto implica el uso de mecanismos de cifrado y autenticación para garantizar que los datos transmitidos entre ISE y otros dispositivos estén protegidos contra la interceptación, la manipulación y el acceso no autorizado.

2. Conectividad VPN IPsec: El servicio IPSec nativo de ISE ayuda a facilitar las conexiones VPN que utilizan el protocolo IPsec para proporcionar un túnel seguro y cifrado para la transmisión de datos. Esto resulta especialmente útil para los trabajadores remotos, las sucursales u otras ubicaciones que necesiten acceder de forma segura al entorno de ISE a través de redes no fiables (como Internet).

3. Soporte para VPN de acceso remoto: El servicio IPSec nativo puede participar en configuraciones VPN de acceso remoto, en las que los usuarios o dispositivos ubicados fuera de las instalaciones (como empleados remotos u oficinas de sucursales) se conectan de forma segura al sistema ISE a través de túneles IPsec. Este servicio garantiza que todo el tráfico de acceso remoto se cifra y autentica antes de llegar al entorno ISE.

4.Compatibilidad de cliente VPN IPsec: El servicio IPSec nativo de ISE garantiza la compatibilidad con los clientes VPN IPsec. Admite configuraciones de cliente comunes, lo que permite que los dispositivos se conecten de forma segura a la red sin exponer los datos confidenciales a riesgos.

Verificar y solucionar problemas del servicio IPSec nativo

1. No hay depuraciones específicas que habilitar para el servicio IPSec nativo. Verifique los registros mediante el comando show logging application strongswan/charon.log tail a través de ISE CLI.

2. Si se observa algún problema para el túnel, verifique el estado del establecimiento del túnel mediante GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec.

Profiler de MFC

El generador de perfiles de MFC es un componente especializado que se utiliza para crear

perfiles de dispositivos de red y terminales. La definición de perfiles es una parte clave del control de acceso a la red, ya que permite a ISE identificar los dispositivos de la red, clasificarlos y aplicar las políticas de red adecuadas en función del tipo de dispositivo y del comportamiento.

Características y funciones clave del servicio MFC Profiler en ISE

1. Perfiles de tráfico: El servicio MFC Profiler de ISE es responsable de recopilar y elaborar perfiles de los datos de tráfico. Supervisa el comportamiento de los terminales en la red, incluidos los tipos de aplicaciones que se utilizan, los servicios a los que se accede y los patrones de tráfico que muestran los dispositivos. Estos datos ayudan a crear un perfil para cada terminal.

2. Perfiles de terminales: El servicio MFC Profiler permite a ISE identificar y categorizar los terminales en función de su comportamiento. Por ejemplo, detecta si un terminal es una impresora, un equipo o un dispositivo móvil en función de los patrones de tráfico. Esto puede ayudar a aplicar políticas más específicas para diferentes tipos de dispositivos, lo que mejora la seguridad y la eficacia operativa.

Verificar y solucionar problemas del servicio de generador de perfiles MFC

1. Vaya a ISE GUI -> Administration -> Profiling -> MFC Profiling and AI rules, y verifique si el servicio está habilitado.

2. Si el servicio está habilitado pero se muestra como deshabilitado/no se está ejecutando mediante el comando show application status ise en ISE CLI. Deshabilite y vuelva a habilitar el servicio de generación de perfiles de MFC en ISE haciendo referencia al paso 1.

Depuraciones útiles para la resolución de problemas: componente del generador de perfiles MFC en depuración. Los registros se pueden verificar desde el paquete de soporte o finalizar los registros mediante el comando show logging application ise-pi-profiler.log tail a través de ISE CLI.

Defecto conocido del generador de perfiles MFC que muestra que no se está ejecutando en lugar del estado deshabilitado:

ID de bug de Cisco ·72853

Puntos clave

1. Para recuperar los servicios, reinicie los servicios mediante los comandos application stop ise y application start ise a través de ISE CLI.

2. Cuando se produzca un problema, asegúrese de que se está recopilando un paquete de soporte de la GUI de ISE/CLI de ISE para realizar una verificación adicional del problema. Enlace de referencia para la creación del paquete de asistencia de ISE a través de la GUI y la CLI: paquete de asistencia de recogida en Identity Services Engine

3. Si los problemas están relacionados con los recursos, la carga media, la utilización de disco, etc., es obligatorio recopilar el volcado de subprocesos y el volcado de montón para el análisis.

4. Antes de realizar la recarga del nodo, póngase en contacto con el TAC de Cisco y proporcione registros seguros para un análisis adicional.

Preocupaciones habituales de ISE

Aparte de los problemas con los servicios de ISE, estos son algunos de los problemas que se encuentran en los nodos de ISE, junto con los pasos básicos de solución de problemas necesarios.

Verificación de carga media alta, problemas de uso de recursos (CPU / MEMORIA / DISCO), recursos insuficientes

1. Verifique que los recursos recomendados por Cisco estén asignados al nodo mediante el comando show Inventory a través de ISE CLI.

2. Desde la CLI del nodo ISE, ejecute el comando tech top para verificar la utilización de recursos de ISE.

3. Verifique el uso del disco mediante el comando show disk a través de ISE CLI.

4. Purgue los terminales inactivos, borre el disco local del nodo y realice limpiezas de actualización.

Si el problema continúa, comuníquese con el TAC de Cisco y proporcione el paquete de soporte seguro, el volcado de pila y el volcado de subprocesos del nodo que está experimentando el problema.

Para proteger el volcado de montón, inicie sesión en la CLI del nodo ISE y ejecute el comando **application configure ise**. Seleccione la opción 22.

Para proteger el volcado de subprocesos, inicie sesión en la CLI del nodo ISE, ejecute el comando **application configure ise** y seleccione la **opción 23.** El volcado de subprocesos se incluye en el paquete de soporte o se puede seguir a través de la CLI de ISE mediante el comando **show logging application appserver/catalina.out**.

Verificar y solucionar problemas de supervisión

La función de supervisión y resolución de problemas (MnT) de ISE es uno de los principales bloques de la arquitectura de ISE que proporciona capacidades de supervisión, generación de informes y alertas.

ISE muestra información de supervisión en muchos lugares, incluidos:

- Página de inicio de Cisco ISE
- Vistas de visibilidad de contexto
- Registros y sesiones en directo de RADIUS
- Búsqueda global
- Registros activos de NAC centrados en las amenazas
- Registros en directo de TACACS

Problemas generales observados en la categoría Supervisión y resolución de problemas:

1. Registros en directo de Radius/ TACACS no disponibles

2. Sesiones en directo no disponibles
3. Resumen de estado no disponible
4. Problemas de rendimiento (CPU/memoria elevadas) observados en los nodos de MnT

Las depuraciones que se deben habilitar en los nodos MnT para reducir el problema:

1. Cisco-mnt
2. Recopilador
3. Cpm-mnt
4. registro en tiempo de ejecución

Además de los componentes mencionados en debug, esta información puede ayudar en la resolución de problemas:

1. ¿Las sesiones en directo también se ven afectadas o solo los registros en directo?
2. ¿Se ven afectados los registros de Radius o TACACS o ambos?
3. ¿Observa un uso elevado de la CPU o un uso elevado del espacio de intercambio en los nodos de MnT?
4. ¿Cuántos archivos de búfer ve en los nodos MnT? Los archivos de búfer se pueden encontrar en: /opt/CSCOcpm/mnt/data/collector.
5. ¿Están habilitadas las reservas de memoria y CPU? Si no es así, habilítelas.
6. ¿Se ha reiniciado la base de datos de sesión/config/MnT en el pasado reciente?
7. ¿Está observando el envío de registros del sistema desde los nodos PSN a los nodos MnT?

Si está utilizando los servicios Syslog para MnT, esta información es necesaria para resolver problemas:

1. ¿Está utilizando un destino de syslog seguro? Si no es así, inhabilítelo, ya que se sabe que causa interbloqueos en los subprocesos que hacen que el recopilador deje de funcionar?
2. ¿Utiliza un destino de syslog seguro? Asegúrese de que la asignación de certificados está configurada correctamente en Administración->Registro->Destinos de registro remoto->Recopilador de registro de sistema seguro 1 y 2
3. Verifique si las categorías de registro son adecuadas (se recomienda eliminar las categorías de registro no utilizadas/no deseadas; esto reduce la carga en los nodos MnT) y si los destinos de registro están configurados correctamente.
4. Verifique los archivos awrrep*.html del paquete de soporte para comprender y obtener una pista de qué componente está enviando syslogs más frecuentes; por ejemplo, si se ven tablas TACACS con consultas de inserción o actualización, podemos verificar los logs del colector para correlacionarlos y entender qué syslogs se están enviando con más frecuencia

Si el problema está relacionado con el rendimiento en el nodo MnT, necesitamos esta información:

1. tech top output de la ISE CLI del nodo MnT.

2. Si la CPU es alta, ¿también observa una alta utilización de memoria o de espacio de intercambio alto?

3. Paquete de soporte con volcado de pila y volcado de rosca asegurado.

Referencia

- Guía del administrador de Cisco Identity Services Engine, versión 3.3
- Solucionar problemas y habilitar depuraciones en ISE

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

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

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