Entender os serviços, a finalidade e a solução de problemas do ISE

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Entendendo e solucionando problemas de serviços ISE
  - Ouvinte de banco de dados
    - Pontos principais sobre o serviço de escuta de banco de dados no ISE
  - Servidor de banco de dados
    - Pontos principais sobre o serviço de servidor de banco de dados no ISE
    - Verificar e Solucionar Problemas de que o Ouvinte de Banco de Dados e os Serviços do Servidor de Banco de Dados estão Inicializando ou Não Estão em Execução
  - Servidor do aplicativo
    - Pontos principais sobre o serviço do servidor de aplicativos no ISE
    - Verificação de que o Servidor de Aplicativos está Inicializando ou Não Está em Execução
  - Banco de dados do Profiler
    - Pontos principais sobre o serviço de banco de dados do Profiler no ISE
    - Verificar e solucionar problemas dos serviços de criação de perfil do ISE
  - Mecanismo de indexação do ISE
    - Verifique se o mecanismo de indexação do ISE não está em execução ou inicializando
  - Conector AD
    - Principais funções do serviço do conector do AD no ISE
  - Banco de dados de sessão M&T
    - Principais funções do serviço de banco de dados da sessão M&T no ISE
    - Verificar e solucionar problemas do banco de dados da sessão M&T no ISE
  - Processador de Log M&T
    - Principais funções do serviço do processador de registro M&T no ISE
    - Verificar e solucionar problemas do serviço M&T Log Processor no ISE
  - Serviço de Autoridade de Certificação
    - Principais funções do serviço da autoridade de certificação no ISE
  - Serviço EST
    - Principais funções do serviço EST no ISE
    - Verifique se a Autoridade de certificação e o serviço EST não estão em execução/inicializando
  - Serviço do mecanismo SXP
    - Principais funções do serviço do mecanismo SXP no ISE
    - Verificação e solução de problemas para o serviço do mecanismo SXP no ISE
  - Serviço TC-NAC
    - Principais funções do serviço TC-NAC no ISE
    - Verificar e solucionar problemas do serviço TC-NAC no ISE
  - Serviço WMI PassiveID

- Principais funções do serviço WMI PassiveID no ISE
- Verificar e solucionar problemas do serviço WMI PassiveID

Serviço Syslog PassiveID

- Principais funções do serviço de syslog de ID passiva

Serviço de API PassiveID

- Principais funções do serviço de API de ID passiva

Serviço PassiveID Agent

- Principais funções do serviço de agente de identificação passiva

Serviço de Ponto de Extremidade PassiveID

- Principais Funções do Serviço de Ponto de Extremidade PassiveID

Serviço PassiveID SPAN

- Principais funções do PassiveID SPAN Service
- Verificação e solução de problemas da pilha PassiveID (serviço PassiveID SPAN, serviço PassiveID Syslog, serviço PassiveID Endpoint, PassiveID Agent, serviço PassiveID API)

Servidor DHCP (dhcpd)

- Principais funções do serviço do servidor DHCP (dhcpd) no ISE
- Verificar e solucionar problemas do servidor DHCP (dhcpd)

Servidor DNS (Nomeado)

- Principais funções do serviço do servidor DNS (nomeado) no ISE
- Verificar e solucionar problemas do servidor DNS (nomeado)

Serviço de mensagens do ISE

- Principais funções do serviço de mensagens do ISE
- Verifique se o serviço de mensagens do ISE não está em execução ou inicializando

Serviço de Banco de Dados do Gateway da API do ISE

- Principais funções do serviço de banco de dados do ISE API Gateway
- Serviço de gateway de API do ISE
- Principais funções do serviço de gateway de API do ISE
- Verificar e Solucionar Problemas do Serviço de Gateway da API do ISE e do Serviço de Banco de Dados do Gateway da API do ISE

Serviço ISE pxGrid Direct

- Principais funções do serviço ISE pxGrid Direct
- Verificar e solucionar problemas do ISEPxgrid Direct Service

Serviço de política de segmentação

- Principais funções do serviço de política de segmentação
- Verificar e Solucionar Problemas do Serviço de Política de Segmentação

Serviço de Autenticação REST

- Principais funções do serviço de autenticação REST
- Verificação e solução de problemas para Rest Auth

Conector SSE

- Principais funções do conector SSE
- Verificar e solucionar problemas do conector SSE

Hermes (Agente de nuvem pxGrid)

- Principais recursos e funções do Hermes (pxGrid Cloud Agent)
- Verificar e solucionar problemas do Hermes (Pxgrid Cloud Agent)

McTrust (Serviço de sincronização Meraki)

- Principais recursos e funções do McTrust (Meraki Sync Service)
- Verifique e solucione problemas do McTrust (Meraki Sync Service)

Exportador de nó do ISE

- Principais recursos e funções do ISE Node Exporter

Serviço Prometheus do ISE

- Principais recursos e funções do ISE Prometheus Service
- Serviço ISE Grafana
  - Principais recursos e funções do ISE Grafana Service
  - Verificar e solucionar problemas do ISE Grafana Service, do ISE Prometheus Service, do ISE Node Exporter
- LogAnalytics de MNT do ISEPesquisa elástica
  - Principais recursos e funções do ISE MNT LogAnalytics Elasticsearch
  - Verificar e solucionar problemas do LogAnalytics do ISE M&T Elasticsearch
- Serviço Logstash ISE
  - Principais recursos e funções do serviço Logstash do ISE
  - Verificar e solucionar problemas do serviço Logstash do ISE
- Serviço ISE Kibana
  - Principais recursos e funções do ISE Kibana Service
  - Verificar e solucionar problemas do serviço Kibana do ISE
- Serviço IPSec nativo do ISE
  - Principais recursos e funções do serviço IPSec nativo do ISE
  - Verificar e solucionar problemas do serviço IPSec nativo
- MFC Profiler
  - Principais recursos e funções do serviço MFC Profiler no ISE
  - Verificar e Solucionar Problemas do Serviço do Profiler do MFC
- Pontos principais

Preocupações padrão no ISE

- Verificação para Média de Carga Alta, Problemas de Utilização de Recursos (CPU / MEMÓRIA / DISCO), Recursos Insuficientes
- Verificar e solucionar problemas de monitoramento

Referência

Introdução

Este documento descreve os serviços, a finalidade e a solução de problemas do ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça o Cisco Identity Services Engine.

Componentes Utilizados

O documento não está restrito a nenhuma versão específica de software e hardware do Cisco Identity Services Engine.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Identity Services Engine (ISE) é uma solução abrangente projetada para fornecer segurança de rede avançada por meio de gerenciamento de política centralizado, autenticação, autorização e contabilidade (AAA). Ele permite que as organizações gerenciem o acesso à rede para usuários, dispositivos e aplicativos, ao mesmo tempo em que garante segurança, conformidade e experiências de usuário contínuas.

Para atingir essas metas, o Cisco ISE utiliza uma variedade de serviços, cada um responsável por tarefas específicas que permitem que o sistema funcione de forma eficiente. Esses serviços trabalham em conjunto para garantir acesso seguro à rede, aplicação robusta de políticas, registro detalhado, integrações perfeitas com sistemas externos e criação eficiente de perfis de dispositivos.

Cada serviço no ISE desempenha um papel vital na manutenção da integridade e da disponibilidade da solução. Alguns serviços lidam com funções essenciais, como gerenciamento e autenticação de bancos de dados, enquanto outros permitem recursos avançados, como criação de perfis de dispositivos, gerenciamento de certificados e monitoramento.

Este artigo fornece uma visão geral dos vários serviços no Cisco ISE, explicando seu objetivo, importância e possíveis etapas de solução de problemas se eles tiverem problemas. Seja você um administrador ou um profissional de segurança de rede, entender esses serviços ajuda a garantir que a implantação do ISE funcione sem problemas e com segurança.

Entendendo e solucionando problemas de serviços ISE

Os serviços mencionados na captura de tela são utilizados pelo ISE para suportar sua funcionalidade. Verifique o status ou os serviços disponíveis no ISE usando o comando show application status ise via CLI do nó do ISE. Este é um exemplo de saída que mostra o status ou os serviços disponíveis no 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
```

Serviços disponíveis no ISE.

Agora, examine cada serviço em detalhes.

Ouvinte de banco de dados

O serviço Database Listener é um componente crítico que ajuda a gerenciar a comunicação entre o ISE e o servidor de banco de dados. Ele atende e processa solicitações relacionadas ao banco de dados, garantindo que o sistema ISE possa ler e gravar no banco de dados subjacente.

Pontos principais sobre o serviço de escuta de banco de dados no ISE

1. Interface de comunicação: Ele atua como uma ponte de comunicação entre o ISE e o servidor de banco de dados, permitindo que o sistema recupere e armazene dados como credenciais de usuário, informações de sessão, políticas de rede e muito mais.

2. Suporte a Banco de Dados Externo: O ISE pode ser configurado para usar um banco de dados externo (como Oracle ou Microsoft SQL Server) para autenticação de usuário e armazenamento de política. O Serviço de escuta de banco de dados garante que o ISE possa se conectar e interagir com esse banco de dados externo de forma segura e eficiente.

3. Tratamento de dados: O serviço escuta consultas de banco de dados do sistema ISE e as converte em ações apropriadas no banco de dados externo. Ele pode lidar com solicitações como inserção, atualização ou exclusão de registros, bem como recuperar informações do banco de dados.

4. Monitoramento de integridade do banco de dados: Além de fornecer o canal de comunicação, ele também ajuda a garantir que a conexão com o banco de dados externo seja estável e operacional. Se a conexão falhar, o ISE voltará para o armazenamento local ou entrará em um modo degradado, dependendo da configuração.

Servidor de banco de dados

O serviço Servidor de Banco de Dados é responsável por gerenciar o armazenamento e a recuperação dos dados usados pelo sistema. Ele lida com a interação com o banco de dados subjacente que o ISE usa para armazenar a configuração, as informações de política, os dados do usuário, os logs de autenticação, os perfis de dispositivo e outras informações necessárias.

Pontos principais sobre o serviço de servidor de banco de dados no ISE

1. Armazenamento interno de dados: O Serviço de servidor de banco de dados gerencia principalmente o banco de dados interno incorporado que o ISE usa para armazenar dados operacionais localmente. Isso inclui dados como registros de autenticação e autorização, perfis de usuário, políticas de acesso à rede, informações de dispositivo e endpoint, informações de sessão.

2. Banco de dados incorporado: Na maioria das implantações do Cisco ISE, o sistema usa um banco de dados PostgreSQL incorporado para armazenamento local. O Serviço de Servidor de Banco de Dados garante que esse banco de dados opere sem problemas e manipule todas as consultas, atualizações e tarefas de gerenciamento relacionadas aos dados armazenados nele.

3. Integridade da base de dados: O serviço garante que todas as transações sejam processadas corretamente e que a integridade do banco de dados seja mantida. Ele lida com tarefas como bloqueio de registros, gerenciamento de conexões de banco de dados e execução de consultas de banco de dados.

Verificar e Solucionar Problemas de que o Ouvinte de Banco de Dados e os Serviços do Servidor de Banco de Dados estão Inicializando ou Não Estão em Execução

O Database Listener e o Database Server são serviços essenciais que devem ser executados juntos para que todos os outros serviços funcionem corretamente. Se esses serviços não estiverem em execução ou estiverem travados durante a inicialização, essas etapas de solução de problemas ajudarão na recuperação.

1. Reinicie os serviços do ISE usando os comandos application stop ise e application start ise.

2. Se este for um nó de VM, a reinicialização do nó a partir da VM deverá ajudar na recuperação de serviços.

3. Se o nó for um nó físico, reiniciar/recarregar o nó a partir do CIMC deve ajudar na recuperação de serviços.

4. Se o banco de dados estiver corrompido, entre em contato com o TAC da Cisco para obter mais soluções de problemas.

O Ouvinte do Banco de Dados e o Servidor de Banco de Dados geralmente ficam inativos ou não são iniciados quando há uma discrepância no banco de dados ou quando o banco de dados não pode ser inicializado corretamente. Nesses casos, executar a redefinição do aplicativo usando o comando application reset-config ise deve ajudar na recuperação e na nova iniciação do banco de dados. Executar o comando application reset-config ise remove configurações e certificados, mas os detalhes do endereço IP e do nome do domínio são mantidos. É recomendável entrar em contato com o TAC da Cisco para obter mais informações e entender o impacto potencial antes de aplicar esse comando em qualquer nó na implantação.

Servidor do aplicativo

O servidor de aplicativos é um componente-chave responsável pela execução e pelo gerenciamento da funcionalidade e dos serviços principais da plataforma ISE. Ele hospeda a lógica comercial, as interfaces de usuário e os serviços que permitem que o ISE desempenhe sua função no controle de acesso à rede, autenticação, autorização, contabilidade e gerenciamento de políticas.

Pontos principais sobre o serviço do servidor de aplicativos no ISE

1. Interface do Usuário (IU): O Serviço do Servidor de Aplicativos é responsável por processar a interface do usuário baseada na Web do ISE. Isso permite que os administradores configurem e gerenciem políticas, visualizem logs e relatórios e interajam com outros recursos do ISE.

2. Gerenciamento de Serviços: Ele é responsável por lidar com os diferentes serviços que o ISE

fornece, incluindo gerenciamento de políticas, tarefas administrativas e comunicação com outros nós do ISE em uma implantação distribuída.

3. Processamento centralizado: O serviço do servidor de aplicativos desempenha um papel central na arquitetura do ISE, fornecendo a lógica que considera as políticas, as solicitações de autenticação e os dados de dispositivos de rede, diretórios e serviços externos.

Verificação de que o Servidor de Aplicativos está Inicializando ou Não Está em Execução

O servidor de aplicativos depende de alguns aplicativos da Web, como certificados, recursos, implantação e licenciamento. Quando qualquer um dos aplicativos Web falha ao inicializar, o servidor de aplicativos permanece preso no estado de inicialização. O servidor de aplicativos leva de 15 a 35 minutos para sair do estado **Não está em execução → Inicializando → em execução**, dependendo dos dados de configuração no nó.

1. Verifique se o certificado Admin do ISE é válido e está ativo na implantação para todos os nós.
2. Verifique se todos os nós na implantação estão em sincronia com o nó Admin primário.
3. Se o nó for uma VM, verifique se os recursos recomendados estão alocados ao nó.

Verifique o status do servidor de aplicativos usando o comando **show application status ise** da CLI do nó do ISE. A maioria dos logs relacionados ao servidor de aplicativos está disponível no

Arquivos Catalina.Out e Localhost.log.

Se as condições mencionadas forem atendidas e o servidor de aplicativos permanecer preso no estado de inicialização, proteja o pacote de suporte da CLI/GUI do ISE. Recupere/reinicie os serviços usando os comandos application stop ise e application start ise .

Banco de dados do Profiler

O banco de dados do Profiler é um banco de dados especializado usado para armazenar informações sobre dispositivos de rede, endpoints e perfis de dispositivo descobertos pelo serviço Profiler. O Profiler é um componente crítico do ISE que identifica e classifica automaticamente dispositivos de rede (como computadores, smartphones, impressoras, dispositivos da IoT e assim por diante) com base nas características e comportamentos da rede.

Pontos principais sobre o serviço de banco de dados do Profiler no ISE

1. Criação de perfis de dispositivos: A principal função do serviço de banco de dados do Profiler é oferecer suporte ao processo de criação de perfil. O ISE usa esse serviço para armazenar as informações coletadas durante a criação de perfis, como:

- Tipo de dispositivo (por exemplo: smartphone, laptop, impressora, dispositivo da IoT)
- Sistema operacional do dispositivo (Por exemplo: Windows®, macOS®, Cisco IOS®, Android®)
- Fabricante do dispositivo
- Comportamentos ou padrões de rede que ajudam a classificar dispositivos

2. Informações do Profiler: Ele armazena atributos do profiler, como os perfis de hardware e

software do dispositivo, que são usados para associar dispositivos a políticas predefinidas. Essas informações também são usadas para atribuir dinamicamente dispositivos às políticas de acesso à rede ou VLANs corretas com base em seus perfis.

3. Processo de criação de perfil: O processo de criação de perfil normalmente se baseia em:

- Criação de perfil ativa: O ISE consulta ativamente os dispositivos na rede para obter informações.
- Criação de perfil passiva: O ISE reúne passivamente dados do tráfego de rede, como solicitações DHCP, atributos RADIUS, cabeçalhos HTTP e outros protocolos de rede, para determinar o tipo de dispositivo.

Verificar e solucionar problemas dos serviços de criação de perfil do ISE

1. Na CLI do ISE, execute o comando show application status ise para verificar se o serviço de banco de dados do profiler está em execução.

2. Na GUI do nó do administrador principal, navegue para Administração > Implantação > selecione o nó. Clique em Editar e verifique se os serviços de sessão e os serviços de criação de perfil estão ativados.

3. Agora, navegue para Administração > Implantação > Selecione o nó. Vá para a configuração do Profiler e verifique se os testadores necessários estão ativados para proteger os dados dos pontos de extremidade.

4. Navegue até Administration > System > Profiling e verifique as configurações do profiler configuradas para CoA.

5. Em Visibilidade de contexto > Pontos finais > Selecione os pontos finais e verifique os atributos coletados por diferentes testes para pontos finais.

Depurações úteis para solucionar problemas de criação de perfil:

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

Mecanismo de indexação do ISE

O mecanismo de indexação é um serviço responsável por pesquisar, indexar e recuperar com eficiência os dados armazenados no banco de dados do ISE. Ela melhora o desempenho e a escalabilidade do ISE, especialmente quando se trata de lidar com grandes volumes de dados e fornecer acesso rápido às informações necessárias para tarefas de autenticação, autorização, monitoramento e emissão de relatórios.

Pontos principais sobre o mecanismo de indexação do ISE no ISE

1. Indexação de dados: O ISE Indexing Engine cria índices para vários tipos de dados

armazenados no ISE, como logs de autenticação, logs de sessão, acertos de política, dados de criação de perfil e registros de acesso à rede. A indexação ajuda a organizar esses dados de forma a tornar a pesquisa e a consulta mais eficientes.

2. Gerenciamento e geração de relatórios de registros: Esse serviço desempenha um papel fundamental no gerenciamento de registros, melhorando o desempenho dos relatórios e das consultas de registro. Por exemplo, ao procurar eventos de autenticação específicos, o mecanismo de indexação permite a recuperação mais rápida dos registros desejados, o que é crucial para o monitoramento de segurança e a emissão de relatórios de conformidade.

3.Recuperação de dados: O mecanismo de indexação também é responsável por garantir que o ISE possa recuperar com eficiência os dados indexados de seu banco de dados subjacente, quando necessário. Isso permite que o ISE forneça respostas rápidas a consultas da interface do usuário, ferramentas externas ou APIs.

Verifique se o mecanismo de indexação do ISE não está em execução ou inicializando

1. Verifique se as pesquisas de DNS direto e reverso estão funcionando para todos os nós no cluster via CLI usando o comando **nslookup <FQDN / IP address of the ISE node >**.
2. Verifique se os Certificados de Administrador do ISE são válidos e ativos para todos os nós no cluster.
3. Verifique se o NTP está funcionando e em sincronia com os nós do ISE via CLI usando o comando **show ntp**.

O mecanismo de indexação é usado pela Visibilidade de contexto e o mecanismo de indexação precisa estar ativo e em execução para que a visibilidade de contexto funcione. Os logs úteis que podem ajudar com a solução de problemas do mecanismo de indexação são os arquivos **ADE.log** que podem ser protegidos do pacote de suporte ou controlados pela CLI usando o comando **show logging system ade/ADE.log tail** durante o problema.

Conector AD

O Conector do AD (Ative Diretory Connector) é um serviço que permite que o ISE se integre ao Microsoft Ative Diretory (AD), permitindo que o ISE autentique, autorize e gerencie usuários com base em suas credenciais do AD e associações a grupos. O conector AD serve como uma ponte entre o ISE e o Ative Diretory, permitindo que o ISE utilize o AD para controle de acesso à rede (NAC) e aplicação de políticas.

Principais funções do serviço do conector do AD no ISE

1. Integração com o Ative Diretory: O AD Connector Service atua como uma ponte entre o ISE e o Ative Diretory. Ele permite que o ISE se conecte com segurança ao AD, possibilitando que o ISE utilize o AD como um armazenamento de identidade centralizado para autenticação de usuário e aplicação de política.

2. Sincronização: O Serviço do Conector do AD oferece suporte à sincronização de dados de usuários e grupos do Ative Diretory para o ISE. Isso garante que o ISE tenha informações atualizadas sobre usuários e grupos, o que é crucial para a aplicação precisa de políticas.

3. Comunicação segura: O Serviço do Conector AD estabelece canais de comunicação seguros

entre o ISE e o Ative Diretory, geralmente usando protocolos como LDAP sobre SSL (LDAPS) para garantir a privacidade e a integridade dos dados durante os processos de autenticação e consulta.

4. Suporte a Vários Domínios do Ative Diretory: O serviço pode suportar conexões a vários domínios do Ative Diretory. Isso é particularmente útil em ambientes grandes ou de vários domínios, onde o ISE precisa autenticar usuários de diferentes florestas ou domínios do AD.

5. Pesquisa de Usuário e Grupo: Ele permite que o ISE consulte o AD para obter informações de usuário e grupo. Isso pode incluir detalhes como nomes de usuário, associações a grupos e outros atributos de usuário que podem ser usados para aplicar políticas de acesso à rede. Por exemplo, as políticas de acesso à rede podem ser aplicadas com base em uma associação de grupo do AD do usuário (Por exemplo: concedendo diferentes níveis de acesso a usuários em diferentes grupos).

1. Verifique se o NTP está em sincronia com os nós e se a diferença de tempo entre o AD e o ISE deve ser inferior a 5 minutos.

2. Verifique se o servidor DNS pode resolver os FQDNs e domínios relacionados ao AD.

3. Navegue até **Operações** > **Relatórios** > **Relatórios** > **Diagnósticos** > **Operações do conector AD**, verifique os eventos ou relatórios relacionados ao AD.

Os logs úteis para solução de problemas são **ad_agent.log** com logs de depuração para o componente **runtime**.

Banco de dados de sessão M&T

O Banco de Dados de Sessões M&T (Monitoring and Troubleshooting Session Database) desempenha um papel crítico no armazenamento e gerenciamento de dados relacionados a sessões para eventos de acesso à rede. O Banco de Dados da Sessão M&T contém informações sobre sessões ativas, incluindo autenticações de usuário, conexões de dispositivo e eventos de acesso à rede, que são essenciais para monitorar, solucionar problemas e analisar a atividade da rede.

Principais funções do serviço de banco de dados da sessão M&T no ISE

1. Armazenamento de Dados da Sessão: O serviço M&T Session Database é responsável por armazenar e indexar dados sobre sessões de usuários e dispositivos na rede. Isso inclui as horas de início e término da sessão, os resultados da autenticação, a identidade do usuário ou dispositivo e as políticas associadas (como atribuições de função ou atribuições de VLAN). Os dados também incluem informações de tarifação RADIUS que detalham o ciclo de vida da sessão, incluindo autenticação inicial e quaisquer mensagens de tarifação que rastreiam eventos da sessão.

2. Dados em tempo real e históricos: O serviço fornece acesso a dados de sessão em tempo real (sessões ativas) e dados de sessão históricos (sessões passadas). Isso permite que os administradores não apenas monitorem o acesso contínuo do usuário, mas também consultem os logs de sessão anteriores para investigar problemas ou validar eventos de acesso. O monitoramento de sessão em tempo real pode ajudar a garantir que nenhum dispositivo não

autorizado esteja na rede no momento.

3. Monitoramento aprimorado: Fornece informações sobre a atividade do usuário e do dispositivo, incluindo as políticas aplicadas às sessões, ajudando a detectar possíveis preocupações de segurança ou acesso não autorizado.

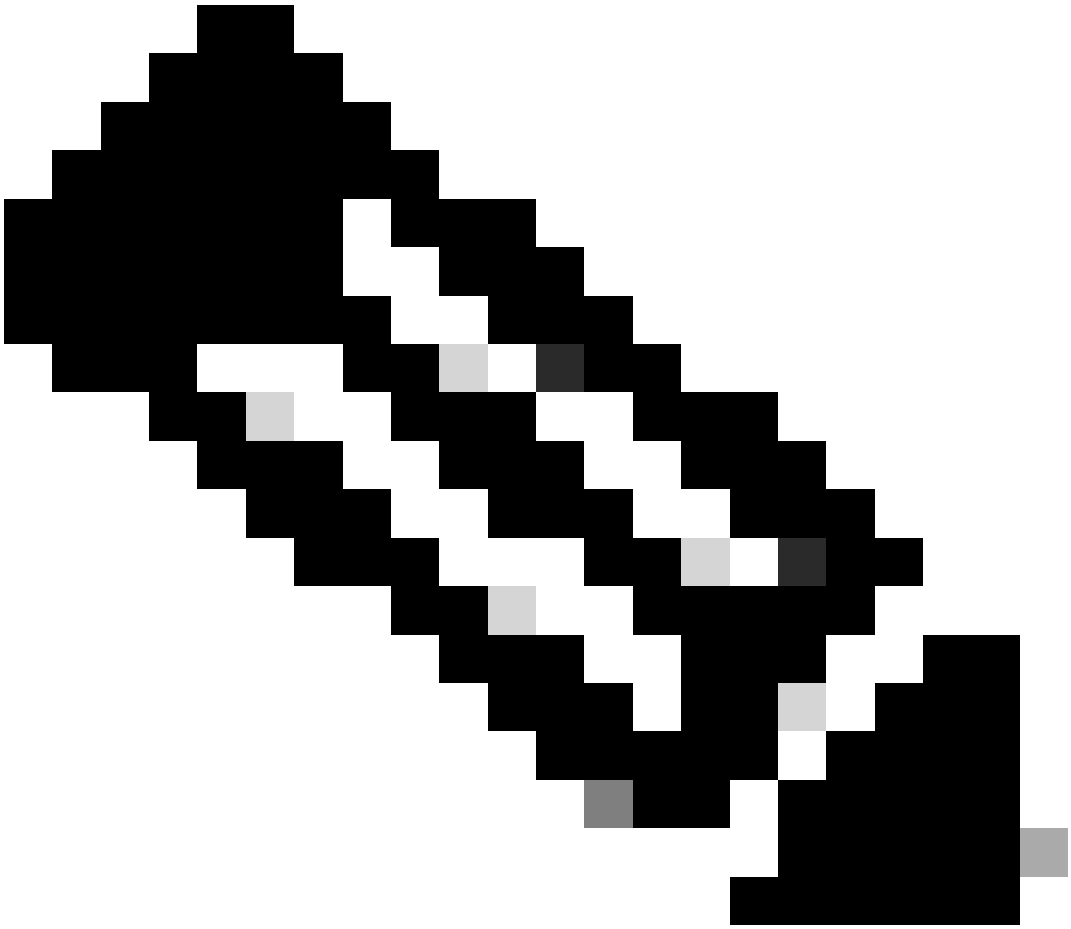
4. Auditoria e relatórios: Facilita a auditoria e a geração de relatórios de conformidade, armazenando um histórico de eventos de acesso à rede e fornecendo dados para a geração de relatórios regulatórios.

Verificar e solucionar problemas do banco de dados da sessão M&T no ISE

1. Verifique se o nó está alocado com os recursos recomendados.

2. **Suporte técnico show seguro** do ISE CLI para verificação adicional do problema.

3. Reinicie o banco de dados da sessão M&T executando o comando **application configure ise** via ISE CLI e selecione a opção **1**.



Note: A redefinição do banco de dados M&T deve ser feita somente após a verificação do impacto potencial na implantação. Entre em contato com o TAC da Cisco para verificação adicional.

Defeitos conhecidos

Identificação de bug da Cisco ·32364

Processador de Log M&T

O M&T Log Processor (Monitoring and Troubleshooting Log Processor) é um componente responsável pela coleta, processamento e gerenciamento de dados de registro gerados por vários serviços no ISE. É uma parte importante da estrutura de Monitoramento e Solução de Problemas (M&T), que ajuda os administradores a monitorar e solucionar problemas de eventos de acesso à rede, tentativas de autenticação, aplicação de políticas e outras atividades no sistema ISE. O M&T Log Processor lida especificamente com o processamento de entradas de registro, garantindo que o ISE possa armazenar, analisar e apresentar as informações necessárias para emissão de relatórios, auditoria e solução de problemas.

Principais funções do serviço do processador de registro M&T no ISE

1. Coleta e Processamento de Logs: O Serviço Processador de Log M&T coleta e processa logs gerados por vários componentes do ISE, como solicitações de autenticação, decisões de autorização, mensagens de contabilidade e atividades de aplicação de política. Esses registros incluem informações detalhadas sobre usuários, dispositivos e tentativas de acesso à rede, como carimbos de data/hora, IDs de usuário, tipos de dispositivos, políticas aplicadas, sucesso ou falha de solicitações de acesso e motivos para falhas.

2. Relatórios e conformidade: Os registros processados por esse serviço são cruciais para o relatório de conformidade. Muitas regulamentações exigem que as organizações mantenham registros de acesso de usuários e eventos de segurança. O serviço M&T Log Processor garante que todos os registros relevantes sejam processados e estejam disponíveis para auditorias de conformidade normativa. Ele ajuda a gerar relatórios detalhados com base nos dados de registro, como logs de acesso de usuário, taxas de êxito/falha de autenticação ou logs de aplicação de política.

Verificar e solucionar problemas do serviço M&T Log Processor no ISE

1. Certifique-se de que o nó do ISE esteja implantado com os recursos recomendados de acordo com o Guia de Instalação da Cisco.

2. Para verificar o problema, execute o comando **show logging system ade/ADE.log tail** via ISE CLIpara exceções/erros relevantes.

Defeitos conhecidos

Identificação de bug da Cisco ·15130

Serviço de Autoridade de Certificação

O Serviço de Autoridade de Certificação (CA) é um componente crítico que ajuda a gerenciar certificados digitais para proteger dispositivos de comunicação e autenticação, usuários e serviços de rede. Os certificados digitais são essenciais para estabelecer conexões confiáveis e garantir a comunicação segura entre clientes (computadores, smartphones, dispositivos de rede) e componentes de infraestrutura de rede (switches, pontos de acesso sem fio, gateways VPN). O serviço CA no Cisco ISE funciona em conjunto com os certificados X.509, que são usados para várias finalidades na segurança de rede, incluindo autenticação 802.1X, acesso VPN, comunicação segura e criptografia SSL/TLS.

Principais funções do serviço da autoridade de certificação no ISE

1. Gestão de Certificados: O Serviço de autoridade de certificação é responsável pela criação, emissão, gerenciamento e renovação de certificados digitais no ISE. Esses certificados são usados para vários protocolos de autenticação e propósitos de criptografia na rede. Ele pode atuar como autoridade de certificação interna ou integrar-se a uma CA externa (por exemplo: Microsoft AD CS, CAs públicas (como VeriSign ou DigiCert) para emitir certificados.

2. Emissão de certificados: Para ambientes que exigem EAP-TLS ou métodos similares de autenticação baseados em certificado, o ISE pode emitir certificados para dispositivos de acesso à rede (NADs), usuários ou terminais. O ISE pode gerar e implantar automaticamente certificados para dispositivos e usuários de autenticação ou pode solicitar certificados de uma CA externa.

3. Registro de Certificado: O Serviço de Autoridade de Certificação oferece suporte à inscrição de certificados para endpoints, como laptops, telefones e outros dispositivos de rede, que precisam se autenticar na rede usando certificados. O ISE usa protocolos como SCEP (Simple Certificate Enrollment Protocol) ou ACME (Automated Certificate Management Environment) para facilitar o registro de certificados para dispositivos.

4. Renovação do certificado: O serviço automatiza a renovação de certificados que expiram para dispositivos e usuários. Ele garante que os certificados estejam sempre válidos e atualizados, evitando interrupções de serviço causadas por certificados expirados.

5. Integração com Autoridades de Certificação Externas: Embora o ISE possa atuar como sua própria CA, é mais comum integrar-se com uma CA externa (por exemplo: Serviços de Certificados do Microsoft Ative Diretory). O serviço CA pode gerenciar a interação entre o ISE e a CA externa, solicitando certificados para usuários, dispositivos e recursos de rede, conforme necessário.

Serviço EST

O Enrollment over Secure Transport (EST) Service é um protocolo usado para emitir com segurança certificados digitais para dispositivos de rede e usuários em um ambiente de autenticação baseado em certificado. O EST é um protocolo de registro de certificado que permite que os dispositivos solicitem certificados de uma CA (Autoridade de Certificação) de forma segura e automatizada. O Serviço EST é particularmente útil para autenticação de dispositivos, como em

ambientes 802.1X, conexões VPN ou cenários BYOD (Bring Your Own Device), em que os dispositivos precisam se autenticar na rede usando certificados.

Principais funções do serviço EST no ISE

1.Inscrição de certificado: O Serviço EST é responsável por habilitar o registro seguro de certificados para dispositivos (como switches, pontos de acesso ou terminais) que exigem certificados para fins de autenticação. A inscrição é feita por meio de um transporte seguro (normalmente HTTPS), garantindo que o processo seja criptografado e protegido contra acesso não autorizado.

2. Revogação e renovação de certificados: Depois que os certificados são inscritos, o Serviço EST também desempenha um papel no gerenciamento da revogação ou renovação de certificados. Por exemplo, os dispositivos precisam solicitar um novo certificado quando o atual expirar, e o EST pode ajudar a automatizar esse processo.

3. Controle de Acesso à Rede Aprimorado: Ao permitir que os dispositivos se autentiquem usando certificados, o Serviço EST reforça a postura de segurança da rede, especialmente em ambientes que usam autenticação 802.1X.

Verifique se a Autoridade de certificação e o serviço EST não estão em execução/inicializando

1. Navegue até **Administration > System > Certificates > Certificate Authority > Internal CA settings.** Verifique se CA, EST e OCSP Responder Status estão Sorted e Enabled.
2. As depurações úteis que podem ajudar na solução de problemas são set , provisioning , ca-service e ca-service-cert. Consulte toise-psc.log , catalina.out , caservice.log e arquivos error.log.
3. Verifique se a CA raiz do ISE e os certificados de mensagens do ISE são válidos na implantação. Se a renovação da CA raiz do ISE for necessária, navegue para **Administração > Certificados > Solicitações de assinatura de certificado > Gerar solicitação de assinatura de certificado,** selecione uso como CA raiz do ISE. **Clique em** renew **ISE Root CA**.

Serviço do mecanismo SXP

O serviço do mecanismo SXP é responsável por gerenciar e facilitar a comunicação entre o ISE e os dispositivos de rede usando o Security Group Tag (SGT) e o Security Group Exchange Protocol (SXP). Ele desempenha um papel crítico no suporte a políticas TrustSec, que são usadas para aplicar o controle de acesso à rede com base no Grupo de Segurança do dispositivo, em vez de apenas endereços IP ou endereços MAC. O Mecanismo SXP no ISE é usado principalmente para a troca de informações do grupo de segurança, que ajuda na aplicação de políticas com base na identidade, no aplicativo e na localização do usuário ou dispositivo. Ele permite que os dispositivos compartilhem tags de grupos de segurança (SGTs), que são usadas para aplicar políticas de segurança em dispositivos de rede, como roteadores e switches.

Principais funções do serviço do mecanismo SXP no ISE

1.Integração com o TrustSec: O SXP geralmente é implantado em ambientes que utilizam o Cisco TrustSec, uma solução que aplica políticas de segurança consistentes em redes com e sem fio. O mecanismo SXP facilita a comunicação de SGTs entre dispositivos, permitindo a aplicação

dinâmica de políticas com base no contexto de segurança de um dispositivo ou usuário.

2. Tags de grupos de segurança (SGTs): O núcleo da aplicação de políticas do TrustSec gira em torno de SGTs. Essas marcas são usadas para classificar o tráfego de rede, e o protocolo SXP ajuda a compartilhar o mapeamento dessas marcas para usuários ou dispositivos específicos. Isso permite um controle granular e orientado por políticas sobre o acesso à rede e o fluxo de tráfego.

Verificação e solução de problemas para o serviço do mecanismo SXP no ISE

1. Por padrão, o serviço do Mecanismo SXP é desabilitado no ISE. Para ativá-la, vá para **ISE GUI > Administração > Implantação, selecione o nó. Marque a caixa Enable SXP Service** e escolha a interface. Em seguida, verifique o status do serviço do mecanismo SXP a partir da CLI do ISE usando o comando **show application status ise**.

2. Se houver problemas de comunicação de rede, verifique se a interface atribuída ao mecanismo SXP tem um endereço IP válido usando o comando show interface na CLI e verifique se a sub-rede IP é permitida na rede.

3. Verifique os registros ao vivo RADIUS para verificar os eventos de conexão SXP no ISE.

4. Ative o componente SXP nos nós do ISE para depurar e capturar logs relevantes e exceções relacionadas ao SXP.

Serviço TC-NAC

O serviço TC-NAC (TrustSec Network Access Control) é um componente que facilita a aplicação de políticas TrustSec em dispositivos de rede, garantindo que o controle de acesso seja baseado em tags de grupos de segurança (SGTs), em vez de endereços IP ou MAC tradicionais.

O TrustSec, por sua vez, é uma estrutura desenvolvida pela Cisco que permite a aplicação de políticas de segurança em toda a rede com base em funções de dispositivo, usuários ou contextos, em vez de usar mecanismos legados como VLANs ou endereços IP. Ele fornece um controle de acesso à rede mais granular e dinâmico, agrupando dispositivos em diferentes grupos de segurança e marcando-os com SGTs.

Principais funções do serviço TC-NAC no ISE

1. Integração com sistemas NAC de terceiros: O serviço TC-NAC permite que o ISE se comunique e interaja com soluções de controle de acesso à rede de terceiros. Isso pode ser útil para empresas que têm infraestrutura NAC existente, mas desejam integrá-la ao Cisco ISE para melhorar a funcionalidade, aproveitar políticas de segurança adicionais ou aproveitar outros recursos de segurança de rede da Cisco.

2. Proporcionar uma aplicação uniforme das políticas: Quando integrado a soluções NAC de terceiros, o ISE pode assumir determinados aspectos da aplicação de políticas e da tomada de decisões. Isso permite uma estrutura de política mais unificada, garantindo que as políticas aplicadas pelos sistemas Cisco e não Cisco NAC sejam consistentes em toda a rede.

3. Suporte para sistemas NAC antigos: O serviço TC-NAC ajuda as empresas que têm sistemas NAC antigos implantados, permitindo que continuem usando esses sistemas enquanto adotam o Cisco ISE para seus recursos de segurança aprimorados. O ISE pode se integrar a soluções NAC mais antigas e ampliar seu ciclo de vida, fornecendo controle de acesso, segurança e aplicação de conformidade em conjunto.

4. Facilitando a comunicação com fornecedores de NAC de terceiros: Esse serviço permite que o ISE facilite a comunicação com soluções NAC de terceiros que usam protocolos ou padrões proprietários. O ISE pode interagir com sistemas NAC de terceiros por meio de protocolos padrão do setor (como RADIUS, TACACS+ ou SNMP) ou APIs personalizadas, dependendo da solução NAC específica que está sendo usada.

Verificar e solucionar problemas do serviço TC-NAC no ISE

1. Verifique se o NAC centrado em ameaças está habilitado navegando até **Administração > Implantação > nó PSN > Habilitar NAC centrado em ameaças**.

2. Se o problema estiver no adaptador do SourceFireAMP, verifique se a **porta 443** é permitida em sua rede.

3. Verifique os detalhes da sessão do endpoint em **Operations** > **Threat-Centric NAC Live Logs.**

Alarmes disparados pelo NAC centrado em ameaças:

- Adaptador não alcançável (ID do syslog: 91002): Indica que o adaptador não pode ser alcançado.
- Falha na conexão do adaptador (ID do syslog: 91018): Indica que o adaptador pode ser alcançado, mas a conexão entre o adaptador e o servidor de origem está inativa.
- Adaptador interrompido devido a erro (ID do syslog: 91006): Este alarme será acionado se o adaptador não estiver no estado desejado. Se este alarme for exibido, verifique a configuração do adaptador e a conectividade do servidor. Consulte os registros do adaptador para obter mais detalhes.
- Erro do adaptador (ID do syslog: 91009): Indica que o adaptador Qualys não pode estabelecer uma conexão ou baixar informações do site da Qualys.

Depurações úteis para solucionar problemas do TC-NAC:

- va-runtime (varuntime.log)
- va-service (varuntime.log e vaaggregation.log)
- TC-NAC (ise-psc.log)
- CNA (ise-psc.log)

Serviço WMI PassiveID

O Serviço WMI PassiveID é um serviço que permite que o ISE execute a criação de perfis de dispositivos usando a Instrumentação de Gerenciamento do Windows (WMI) como um mecanismo passivo para identificar e criar perfis de pontos de extremidade na rede. Ele

desempenha um papel crucial na criação de perfis de dispositivos, particularmente em ambientes onde os dispositivos que executam o sistema operacional Windows precisam ser identificados com precisão para o controle de acesso à rede e a aplicação de políticas.

Principais funções do serviço WMI PassiveID no ISE

1. Coleção de Identidades do Dispositivo: O serviço WMI PassiveID permite que o ISE colete passivamente informações de identidade de dispositivos Windows usando a Instrumentação de Gerenciamento do Windows (WMI). Ele reúne detalhes do sistema, como o nome do host do dispositivo, a versão do SO e outros atributos relevantes, sem exigir que o dispositivo participe ativamente.

2. Integração com a política do ISE: As informações coletadas pelo serviço WMI PassiveID são integradas à estrutura de política do ISE. Ele ajuda na aplicação dinâmica de políticas com base em atributos de dispositivo, como tipo, SO e conformidade com padrões de segurança.

Verificar e solucionar problemas do serviço WMI PassiveID

Uma fonte altamente segura e precisa, bem como a mais comum, a partir da qual receber informações do usuário. Como uma sonda, o AD trabalha com a tecnologia WMI para fornecer identidades de usuário autenticadas. Além disso, o próprio AD, em vez da sonda, funciona como um sistema de origem (um provedor) a partir do qual outras sondas também recuperam dados de usuário.

Depurações úteis e informações necessárias para fins de solução de problemas. Defina estes atributos para o nível de depuração para problemas WMI de PassiveID:

- PassiveID (passiveid*)
- runtime-logging (prrt-server.log)
- Ative Diretory (ad)_agent.log) - Nível de rastreamento
- coletor (collector.log) (nos nós PassiveID,MnT e no nó pxGrid ativo se as sessões forem publicadas)
- pxGrid (pxgrid/) (no MnT secundário e no nó pxGrid ativo se as sessões forem publicadas)

Informações necessárias para solucionar problemas do PassiveID WMI:

1. Se estava funcionando antes? Qualquer alteração feita recentemente. (Como atualização, instalação de patch no ISE/ atualização no DC)
2. A conexão de teste funciona bem (antes da integração, verifique a conexão de teste)
3. Detalhes sobre o nome de usuário usado para Ingressar no AD e o nome de usuário usado para o WMI. (se a conta é admin ou não admin)
4. Verifique se os eventos (4768, 4770) no DC estão registrados. (Log do visualizador de eventos do DC)
5. Logs de captura: Defina o nível de depuração para a id passiva e o registro em tempo de execução e, em seguida, configure o wmi para esse DC, AD - nível de rastreamento com carimbo de data/hora.

Serviço Syslog PassiveID

O serviço de syslog PassiveID é um serviço que permite que o recurso de criação de perfil PassiveID colete e processe mensagens de syslog de dispositivos de rede no ambiente. Essas mensagens de syslog contêm informações importantes sobre os endpoints conectados à rede, e o ISE as usa para criar o perfil desses dispositivos para controle de acesso à rede e aplicação de políticas.

Principais funções do serviço de syslog de ID passiva

1. Autenticação Passiva: O serviço Passive ID Syslog permite que o Cisco ISE autentique usuários e dispositivos de forma passiva, coletando mensagens de syslog de dispositivos de rede (como switches ou roteadores) que indicam a atividade do usuário e do dispositivo. Isso é útil em situações onde os métodos ativos tradicionais de autenticação, como 802.1X, não são adequados ou viáveis.

2. Registro de Eventos: O serviço Passive ID Syslog depende do protocolo syslog para receber logs de dispositivos de rede que rastreiam o acesso do usuário e o comportamento na rede. As informações contidas nesses registros podem incluir itens como tentativas de logon do dispositivo, pontos de acesso e detalhes da interface, que ajudam o ISE a identificar passivamente o dispositivo ou usuário.

Serviço de API PassiveID

O PassiveID API Service é um serviço que permite a integração com sistemas que exigem informações sobre a identidade de dispositivos ou usuários conectados à rede. Ele é geralmente usado em ambientes onde os administradores de rede desejam executar políticas e ações baseadas em identidade sem exigir protocolos de autenticação de rede ativos, como 802.1X para cada dispositivo.

Principais funções do serviço de API de ID passiva

1. Integração com sistemas externos: A API Passive ID permite que o ISE receba informações de identidade de sistemas de terceiros ou dispositivos de rede (como switches, roteadores, firewalls ou qualquer sistema que possa gerar eventos relacionados à identidade). Esses sistemas externos podem enviar informações como mensagens de syslog, logs de autenticação ou outros dados relevantes que podem ajudar o ISE a identificar passivamente um usuário ou dispositivo.

2. Autenticação Passiva: O serviço de API de ID Passiva é usado para autenticar usuários e dispositivos de forma passiva, coletando dados de identidade sem exigir autenticação ativa (por exemplo: sem necessidade de 802.1X, MAB ou autenticação da Web). Por exemplo, ele pode capturar informações de dispositivos de rede, logs do Ative Diretory ou dispositivos de segurança e usá-las para identificar o usuário ou dispositivo.

3. Mapeando Informações de Identidade: A API de ID Passiva pode ser usada para mapear dados de identidade para políticas de segurança específicas. Essas informações são usadas para atribuir dinamicamente tags de grupos de segurança (SGTs) ou funções a usuários e dispositivos,

o que influencia a aplicação de controles de acesso à rede (como políticas de segmentação e firewall).

Serviço PassiveID Agent

O Serviço do Agente PassiveID é um serviço que permite a criação de perfis de dispositivos através do uso de Agentes PassiveID instalados em endpoints (como computadores, laptops, dispositivos móveis e assim por diante). O PassiveID Agent permite que o ISE colete informações de criação de perfil sobre dispositivos na rede ouvindo o tráfego de endpoints, sem exigir verificações ativas ou interações diretas com os dispositivos.

Principais funções do serviço de agente de identificação passiva

1. Identificação Passiva de Usuários e Dispositivos: O serviço Passive ID Agent é responsável por coletar passivamente informações relacionadas à identidade, geralmente de dispositivos de rede ou endpoints, e enviar esses dados ao ISE. Esse serviço permite que o ISE autentique e identifique usuários e dispositivos com base em suas atividades ou características, sem precisar de autenticação ativa do dispositivo (por exemplo: sem que credenciais 802.1X sejam fornecidas).

2. Integração com Outros Componentes da Cisco: O Passive ID Agent trabalha em conjunto com dispositivos de rede da Cisco, como switches, controladores sem fio e pontos de acesso, para coletar informações relacionadas à identidade do tráfego de rede, registros de syslog ou outros sistemas de gerenciamento. Ele também pode ser integrado ao Cisco TrustSec e ao Cisco Identity Services para mapear esses dados para tags de grupos de segurança (SGTs) específicas ou outras políticas baseadas em identidade.

3. Controle de Acesso à Rede Contextual: O Passive ID Agent envia essas informações ao Cisco ISE, que aplica as políticas de controle de acesso apropriadas com base na identidade e no contexto do usuário ou dispositivo. Isso pode incluir:

- Controle de acesso baseado em funções.
- Atribuição de VLAN dinâmica.
- Segmentação de rede.
- Aplicação de políticas de segurança com base na função do usuário ou na postura de segurança do dispositivo.

Serviço de Ponto de Extremidade PassiveID

O PassiveID Endpoint Service é um serviço que é responsável pela identificação e criação de perfis de endpoints (dispositivos) na rede com base na tecnologia PassiveID. Esse serviço ajuda o ISE a coletar, processar e classificar informações sobre dispositivos conectados à rede, sem exigir interação ativa com os próprios endpoints. O PassiveID Endpoint Service desempenha um papel crítico na criação de perfis, no controle de acesso à rede e na aplicação de políticas de segurança.

Principais Funções do Serviço de Ponto de Extremidade PassiveID

1. Identificação Passiva de Usuários e Dispositivos: O PassiveID Endpoint Service permite que o Cisco ISE identifique e autentique dispositivos na rede de forma passiva, aproveitando as informações da atividade da rede ou dos registros do sistema. Isso inclui a identificação de usuários e dispositivos com base no comportamento ou nas características da rede, como endereço MAC, endereço IP ou informações de logon de um armazenamento de identidade externo, como o Ative Diretory (AD).

2. Coleta de dados de endpoints: O Serviço de Ponto de Extremidade coleta vários tipos de dados específicos de ponto de extremidade de diferentes fontes:

- Informações de logon do usuário de repositórios de identidades externos, como o Ative Diretory ou outros diretórios.
- Características do dispositivo, como endereços IP, endereços MAC e tipo de dispositivo (por exemplo: se o dispositivo é um PC com Windows, um celular ou um dispositivo da IoT).
- Atividade de rede do endpoint, como solicitações DHCP, solicitações ARP e outras comunicações da camada de rede.

Serviço PassiveID SPAN

O PassiveID SPAN Service é um serviço que utiliza o espelhamento de porta SPAN (Switched Port Analyzer) em dispositivos de rede para capturar e analisar o tráfego de rede para fins de criação de perfil de endpoint. Esse serviço ajuda o ISE a reunir passivamente informações sobre endpoints (dispositivos) na rede, analisando seus padrões de comunicação de rede sem exigir sondas ativas ou agentes instalados nos próprios dispositivos.

Principais funções do PassiveID SPAN Service

1. Coleta de Identidade Passiva do Tráfego SPAN: O serviço PassiveID SPAN permite que o ISE colete dados de identidade com base no tráfego de rede espelhado ou copiado através de uma porta SPAN em um switch. Uma porta SPAN é normalmente usada para monitoramento de rede, espelhando o tráfego de rede de outras portas ou VLANs. Ao capturar esse tráfego, o ISE pode reunir passivamente informações de identidade, como:

- Endereços MAC dos dispositivos.
- Endereços IP associados a dispositivos.
- O DHCP solicita ou outras informações relacionadas à identidade do tráfego capturado.
- Registros de autenticação de dispositivos de rede, como switches ou controladores sem fio.

2. Captura de Informações de Identidade do Usuário e do Dispositivo: O serviço de SPAN basicamente escuta o tráfego que passa pela rede e identifica as principais informações de identidade dos pacotes de rede sem a necessidade de interagir diretamente com os dispositivos. Isso pode incluir dados como:

- Identidades de usuário quando autenticam através de protocolos como EAP (Extensible Authentication Protocol).
- Identidades de dispositivo baseadas em endereços MAC e endereços IP.
- Funções e comportamentos do dispositivo com base nos padrões e eventos de tráfego

observados.

Verificação e solução de problemas da pilha PassiveID (serviço PassiveID SPAN, serviço PassiveID Syslog, serviço PassiveID Endpoint, PassiveID Agent, serviço PassiveID API)

1. PassiveID stack é uma lista de provedores e todos os serviços na pilha PassiveID stack são desabilitados por padrão. Navegue até ISE GUI > Administração > Implantação > Selecione o nó, Ativar Passive Identity Service, clique em Salvar. Para verificar o status do serviço de pilha PassiveID, faça login na CLI do nó do ISE e execute o comando show application status ise.

2. Se houver problemas com o Passive ID Agent, verifique se o FQDN do agente pode ser resolvido no nó do ISE. Para fazer isso, faça login na CLI do ISE e execute o comando nslookup < FQDN do Agente configurado >.

3. Verifique se o mecanismo de indexação do ISE está ativo e se as pesquisas de DNS reverso e de encaminhamento estão sendo resolvidas pelo DNS ou pelo servidor de nomes configurado no ISE.

4. Para garantir uma comunicação direta com os provedores de syslog, verifique se a porta UDP 40514 e a porta TCP 11468 estão abertas em sua rede.

5. Para configurar o Provedor de SPAN em um nó, certifique-se de que o ISE Passive Identity Service esteja ativado. Verifique se a interface que você deseja configurar no provedor de SPAN está disponível no ISE usando o comando show interface da CLI do ISE.

Para verificar os logs, com base no provedor Passive ID, você precisa revisar passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log. Os registros mencionados podem ser protegidos do pacote de suporte do nó ISE.

Servidor DHCP (dhcpd)

O serviço do servidor DHCP (dhcpd) é um serviço que fornece a funcionalidade do protocolo DHCP aos dispositivos de rede. É usado principalmente para atribuir endereços IP a dispositivos (endpoints) que estão tentando se conectar à rede. No ISE, o servidor DHCP desempenha um papel crucial no fornecimento de endereços IP aos endpoints que os solicitam quando se conectam à rede. O serviço também pode fornecer informações adicionais de configuração, como servidores DNS, gateway padrão e outras configurações de rede.

Principais funções do serviço do servidor DHCP (dhcpd) no ISE

1. Alocação Dinâmica de Endereços IP: O serviço dhcpd no ISE funciona como um servidor DHCP, que fornece alocação de endereço IP para dispositivos que solicitam um endereço IP quando se conectam à rede. Isso é importante em cenários onde os dispositivos se conectam à rede dinamicamente, como em ambientes BYOD (Bring Your Own Device) ou quando os dispositivos são configurados para obter seus endereços IP automaticamente.

2. DHCP baseado em perfil: O serviço dhcpd pode alocar endereços IP com base no perfil do dispositivo. Se o ISE tiver criado o perfil do dispositivo (por exemplo: ao determinar se é um

smartphone, laptop, dispositivo da IoT), ele pode atribuir um endereço IP apropriado ou aplicar outras configurações com base no tipo de dispositivo ou função.

3. Suporte para Retransmissão DHCP: O ISE pode funcionar como um agente de retransmissão de DHCP, encaminhando solicitações de DHCP de dispositivos para um servidor DHCP externo se o ISE não estiver tratando da atribuição de endereço IP real. Nesse caso, o serviço dhcpd pode encaminhar solicitações de dispositivos para um servidor DHCP central, enquanto o ISE continua a aplicar políticas de rede e controles de acesso.

Verificar e solucionar problemas do servidor DHCP (dhcpd)

1. Entre em contato com o TAC da Cisco para verificar se o pacote do servidor DHCP está instalado no ISE.

2. Faça login na raiz do **ISE > rpm -qi dhcp**.

Servidor DNS (Nomeado)

O Serviço de Servidor DNS (nomeado) é um serviço que permite que o ISE funcione como um servidor DNS (Sistema de Nomes de Domínio) ou resolvedor DNS. Ele é o principal responsável por resolver nomes de domínio em endereços IP e vice-versa, facilitando a comunicação entre dispositivos na rede.

Principais funções do serviço do servidor DNS (nomeado) no ISE

1. Resolução DNS para Comunicação ISE: O serviço nomeado no ISE ajuda a resolver nomes de domínio para endereços IP. Isso é especialmente importante quando o ISE precisa se conectar a outros dispositivos de rede ou serviços externos (como servidores Radius, Ative Diretory ou servidores NTP externos) usando nomes de domínio em vez de endereços IP.

- Por exemplo, quando o ISE precisa acessar um servidor Radius ou um serviço de diretório externo (como o Ative Diretory), ele precisa resolver o nome de domínio desse servidor para um endereço IP.
- O ISE consulta o servidor DNS configurado no sistema para resolver esses nomes de domínio, garantindo uma comunicação tranquila.

2. Resolução DNS para Serviços Externos: O serviço DNS permite que o ISE se conecte a serviços externos que exigem nomes de domínio. Por exemplo, o ISE precisa resolver os nomes de serviços externos como:

- Serviços baseados em nuvem.
- Servidores NTP (Network Time Protocol).
- Autoridades de Certificação (CAs) ou servidores LDAP.

3. Servidores DNS Multidomínio e Redundantes: O ISE pode ser configurado para usar vários servidores DNS para redundância. Caso um servidor DNS fique indisponível, o ISE pode recorrer a outro servidor DNS para garantir a operação contínua e a resolução de DNS.

Verificar e solucionar problemas do servidor DNS (nomeado)

1. A partir do CLI do nó ISE, verifique a acessibilidade ao servidor de nomes ou ao servidor DNS da implantação usando o comando **ping <IP do servidor DNS / servidor de nomes>** .

2. Verifique a resolução DNS dos FQDNs ISE usando o comando **nslookup <FQDN / endereço IP dos nós ISE>** via CLI do ISE.

Serviço de mensagens do ISE

O serviço de mensagens do ISE é um componente que facilita a comunicação assíncrona entre vários serviços e componentes dentro do sistema ISE. Ele desempenha um papel crucial na arquitetura geral do sistema do ISE, permitindo que diferentes partes da plataforma enviem e recebam mensagens, gerenciem tarefas e sincronizem atividades.

Principais funções do serviço de mensagens do ISE

1. Comunicação Interprocessos (IPC): O serviço de mensagens do ISE desempenha um papel fundamental na comunicação entre processos (IPC) entre vários serviços do ISE. Ele garante que diferentes módulos e serviços do ISE, como autenticação, autorização e aplicação de políticas, possam trocar dados e instruções de maneira coordenada.

2. Suporte a Ambiente Distribuído: Em implantações maiores ou distribuídas do ISE (como em configurações de vários nós ou de alta disponibilidade), o serviço de mensagens ajuda a facilitar a comunicação entre os vários nós do ISE. Isso garante que os dados, como solicitações de autenticação, sessões de usuário e atualizações de política, sejam sincronizados corretamente em nós diferentes no sistema ISE.

3. Sincronização de Políticas e Configurações: O serviço de mensagens está envolvido na sincronização de configurações e políticas entre os nós do ISE. Quando são feitas alterações de configuração em um nó primário, o serviço garante que essas alterações sejam propagadas para nós secundários ou de backup no sistema. Isso é essencial para manter a consistência e garantir que as políticas de acesso à rede aplicadas em diferentes locais ou nós distribuídos do ISE permaneçam sincronizados.

Verifique se o serviço de mensagens do ISE não está em execução ou inicializando

1. Verifique se a porta TCP 8671 não está bloqueada no firewall, pois essa porta é usada para comunicação entre nós entre dispositivos ISE.

2. Verifique se há erros de link de fila e, se houver algum, renove as mensagens do ISE e os certificados da CA raiz do ISE, pois os erros de link de fila normalmente ocorreriam devido a problemas internos de corrupção de certificado. Para resolver erros de link de fila, renove o ISE Messaging e o certificado ISE Root CA consultando o artigo: ISE - Queue Link Error

3. Em GUI -> Administração -> Certificados -> Selecione Certificado de Mensagens do ISE. Clique em Exibir para verificar o status do certificado.

Registros úteis para solucionar problemas do ISE Messaging Service são feitos.log, que está disponível no pacote de suporte ou pode ser seguido via CLI usando o comando show logging system ade/ADE.log tail durante o problema.

4. Se o rabbitmq de showup de log ADE.log: conexão recusou erros, entre em contato com o Cisco TAC para remover o bloqueio para o módulo Rabbitmq da raiz ISE.

Serviço de Banco de Dados do Gateway da API do ISE

O Serviço de banco de dados do gateway de API do ISE é um componente responsável por gerenciar e processar dados relacionados a solicitações e respostas de API no sistema ISE. Ele atua como um intermediário que conecta o gateway de API do ISE ao banco de dados do ISE, garantindo que os aplicativos personalizados também possam atualizar ou modificar dados no ISE (por exemplo, ajustando políticas de acesso ou adicionando/removendo usuários) por meio de chamadas de API gerenciadas pelo serviço.

Principais funções do serviço de banco de dados do ISE API Gateway

1. Acesso da API aos Dados do ISE: O Serviço de banco de dados do gateway da API do ISE atua como uma ponte, permitindo que aplicativos externos interajam com o banco de dados do ISE por meio das APIs RESTful do ISE. Essas APIs podem ser usadas para recuperar ou modificar dados armazenados no banco de dados do ISE, como:

- Logs de autenticação do usuário.
- Políticas de acesso à rede.
- Informações de perfil do dispositivo.
- Configuração e definições do sistema.

2. Ativando Integrações de Sistema Externo: Esse serviço desempenha um papel crucial na integração do ISE com sistemas externos, como:

- Servidores de autenticação externos (LDAP, Ative Diretory, RADIUS).
- Sistemas de gerenciamento de rede (NMS).
- Soluções de SIEM (Security Information and Event Management, gerenciamento de eventos e informações de segurança).
- Aplicativos ou serviços personalizados que precisam interagir com os dados do ISE.

Ao fornecer acesso à API, o Serviço de banco de dados do gateway da API permite que esses sistemas externos consultem dados do ISE, enviem atualizações ao ISE ou acionem ações específicas no ISE em resposta a eventos externos.

3. Suporte à Comunicação de API RESTful: O ISE expõe APIs RESTful projetadas para funcionar em HTTP/HTTPS. O Serviço de banco de dados do gateway de API é responsável por gerenciar o fluxo de solicitações e respostas de API, garantindo que as solicitações sejam autenticadas, processadas e que os dados apropriados do banco de dados do ISE sejam retornados em resposta.

Serviço de gateway de API do ISE

O ISE API Gateway Service é um componente crucial que fornece acesso RESTful API a serviços, dados e funcionalidades do ISE. Ele atua como uma ponte entre o ISE e os sistemas externos, permitindo que esses sistemas interajam programaticamente com o controle de acesso à rede, a aplicação de políticas, a autenticação e outros serviços do ISE. O gateway de API permite que aplicativos de terceiros, sistemas de gerenciamento de rede e aplicativos personalizados interajam com o Cisco ISE sem a necessidade de intervenção manual ou acesso direto à interface de usuário do ISE.

Principais funções do serviço de gateway de API do ISE

1. Habilitando o acesso à API para o ISE: O Serviço de gateway de API do ISE permite que sistemas externos acessem e interajam com segurança com os dados e políticas do Cisco ISE usando APIs RESTful. Isso fornece acesso programático às funcionalidades do ISE, como autenticação, aplicação de políticas, gerenciamento de sessões e muito mais.

2. Fornecimento de controle programático: O Serviço de Gateway de API permite o controle programático das funções do ISE. Os administradores e desenvolvedores podem usar APIs para:

- Recuperar ou modificar políticas de rede.
- Consulte ou gerencie sessões de usuário e logs de autenticação.
- Crie e gerencie regras de controle de acesso à rede.
- Acessar ou atualizar perfis de dispositivo.

Esse controle pode ser aproveitado para automação ou orquestração personalizada de fluxo de trabalho, como ajuste dinâmico de políticas de acesso à rede com base em dados em tempo real ou integração do ISE em uma plataforma de automação de segurança mais ampla.

3. Monitorização e comunicação de informações: O Serviço de Gateway de API permite que sistemas externos coletem dados de logs operacionais do ISE, histórico de sessões e detalhes de aplicação de políticas. Isso é importante para:

- Relatórios de conformidade.
- Monitoramento de segurança.
- Resposta a incidentes.

As chamadas de API podem ser usadas para receber logs, informações de auditoria e eventos, permitindo que as equipes de segurança monitorem as atividades do ISE a partir de um painel centralizado ou de uma ferramenta de relatório.

Verificar e Solucionar Problemas do Serviço de Gateway da API do ISE e do Serviço de Banco de Dados do Gateway da API do ISE

1. Verifique se o Certificado Admin do nó ISE está ativo e válido. Navegue até Administração > Certificados > Selecione o nó > Selecionar certificado administrativo. Clique em Exibir para verificar o status do Certificado Admin do nó ISE.

2. Defina os componentes ise-api-gateway, api-gateway, apiservice para depurar e os logs podem ser ajustados usando estes comandos:

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

Serviço ISE pxGrid Direct

O ISE pxGrid Direct Service é um componente crítico que suporta a funcionalidade pxGrid (Platform Exchange Grid) no ISE. O pxGrid é uma tecnologia da Cisco que facilita o compartilhamento e a integração de dados seguros, padronizados e escaláveis entre as soluções de segurança de rede da Cisco e aplicativos, serviços e dispositivos de terceiros. O ISE pxGrid Direct Service permite a comunicação direta entre o ISE e outros sistemas compatíveis com pxGrid sem a necessidade de dispositivos ou serviços intermediários.

Principais funções do serviço ISE pxGrid Direct

1. Integração direta com sistemas de terceiros: O ISE pxGrid Direct Service permite que o ISE se integre diretamente a sistemas de segurança de rede de terceiros, como firewalls, roteadores, soluções NAC, plataformas SIEM e outros dispositivos de segurança. Ele permite que esses sistemas troquem informações sobre eventos de acesso à rede, incidentes de segurança e dados contextuais da rede.

2. Compartilhamento de Contexto: Uma das principais funções do pxGrid é o compartilhamento de informações contextuais (como identidades de dispositivo, funções de usuário, postura de segurança e informações de acesso à rede). Com o serviço pxGrid Direct, o ISE pode compartilhar diretamente esse contexto com outros dispositivos ou aplicativos sem depender de métodos tradicionais como RADIUS ou TACACS+.

3. Comunicação simplificada: Usando o pxGrid, o ISE pode se comunicar e trocar informações com soluções de terceiros usando um protocolo padronizado. Isso simplifica o processo de integração, pois os sistemas não precisam ter integrações personalizadas para cada solução individual de terceiros.

4. Segurança e conformidade aprimoradas: O pxGrid Direct Service também melhora a postura de segurança e a conformidade, garantindo que todos os sistemas no ecossistema da rede tenham acesso aos mesmos dados contextuais e em tempo real sobre usuários, dispositivos e políticas de segurança. Isso garante uma aplicação mais coordenada das políticas de segurança de rede em todo o ambiente.

Verificar e solucionar problemas do ISEPxgrid Direct Service

1. Entre em contato com o TAC da Cisco para verificar se **edda*.lock*** está presente na pasta /tmp. Se sim, o Cisco TAC remove o bloqueio e reinicia o serviço Pxgrid Direct da raiz.

2. Defina o componente **PxGrid Direct** para depurar no nó ISE para solução de problemas. Os registros podem ser protegidos através do pacote de suporte do ISE ou da CLI do ISE usando estes comandos:

show logging application pxgriddirect-service.log

show logging application pxgriddirect-connector.log

Os registros mencionados fornecem informações sobre os dados de endpoint buscados e recebidos pelo Cisco ISE junto com o status de conectividade do Pxgrid Connector.

Serviço de política de segmentação

O Serviço de política de segmentação é um componente-chave responsável por aplicar políticas de segmentação de rede com base na identidade do usuário, na postura do dispositivo ou em outras informações contextuais. Ele ajuda a controlar o acesso de usuários e dispositivos a segmentos específicos da rede, garantindo que somente usuários autorizados ou dispositivos compatíveis possam acessar determinadas partes da rede. A segmentação da rede é essencial para reduzir a superfície de ataque da rede, evitando a movimentação lateral de ameaças e garantindo a conformidade com as regulamentações. O Serviço de política de segmentação no ISE é usado para aplicar essas regras de segmentação de rede de forma dinâmica e flexível em toda a rede.

Principais funções do serviço de política de segmentação

1. Definindo Segmentos de Rede: O Serviço de política de segmentação no ISE permite que os administradores definam vários segmentos de rede (sub-redes ou VLANs) com base nas características de usuários ou dispositivos. Por exemplo:

- Dispositivos com posturas de segurança diferentes podem ser atribuídos a segmentos diferentes (Por exemplo: dispositivos confiáveis em uma VLAN e dispositivos não confiáveis em outra).
- Usuários de diferentes departamentos ou funções podem ser atribuídos a diferentes segmentos de rede para aplicar o privilégio mínimo e restringir o acesso a recursos confidenciais.

2. Segmentação Dinâmica: Esse serviço permite a segmentação dinâmica da rede, o que significa que os segmentos de rede ou as VLANs podem mudar com base em condições em tempo real. Por exemplo:

- Um usuário pode ser atribuído a uma VLAN específica com base em sua função ou status de integridade do dispositivo.
- Um dispositivo considerado não compatível ou que esteja executando um sistema operacional desatualizado pode ser movido para uma VLAN de quarentena ou de convidado até que seja corrigido.

3. Aplicação baseada em políticas: O Serviço de política de segmentação usa políticas para tomar decisões sobre em qual segmento um dispositivo ou usuário deve ser colocado. Essas políticas podem levar em conta vários fatores, como:

- Identidade do usuário: Com base na função ou atributos do usuário.
- Postura do dispositivo: O status de integridade ou conformidade do dispositivo (Por

exemplo: ele está executando o software antivírus mais recente?).
- Local: A localização física do usuário ou dispositivo na rede (Por exemplo: escritório, área de convidados, acesso remoto).
- Hora do acesso: A hora do dia ou dia da semana em que a solicitação de acesso é feita.

4. Aplicação das políticas de segurança: O Serviço de política de segmentação garante que as políticas de segurança sejam aplicadas de forma consistente em todos os dispositivos de rede (como switches, roteadores, firewalls), aproveitando os padrões do setor, como atribuição de RADIUS e VLAN. Isso permite que o Cisco ISE se comunique com dispositivos de infraestrutura de rede para aplicar as políticas de segmentação necessárias.

Verificar e Solucionar Problemas do Serviço de Política de Segmentação

1. Verifique se a segmentação está configurada corretamente navegando até Centros de trabalho > TrustSec > Visão geral > Painel de controle.

2. Centros de trabalho > TrustSec > Relatórios, selecione relatórios TrustSec para verificar o status e os relatórios do serviço de política de segmentação.

Serviço de Autenticação REST

O Serviço de Autenticação REST é um serviço que fornece recursos de autenticação usando APIs RESTful. Ele permite que aplicativos e sistemas externos autentiquem usuários ou dispositivos interagindo com o ISE sobre HTTP(S) usando protocolos REST padrão. Esse serviço permite a integração perfeita da funcionalidade de autenticação do Cisco ISE com aplicativos ou sistemas de terceiros que precisam autenticar usuários ou dispositivos, mas não podem usar os métodos tradicionais (como RADIUS ou TACACS+).

Principais funções do serviço de autenticação REST

1. Autenticação RESTful: O Serviço de Autenticação REST habilita solicitações de autenticação no protocolo REST API. Isso permite sistemas externos (por exemplo: aplicativos, dispositivos de rede de terceiros ou serviços) para autenticar usuários ou dispositivos usando o ISE como o servidor de autenticação, mas através de chamadas de serviço Web RESTful em vez de protocolos de autenticação tradicionais como RADIUS ou TACACS+.

2. Integração com Aplicações Externas: Esse serviço foi projetado para aplicativos externos que precisam autenticar usuários ou dispositivos, mas não usam métodos de autenticação tradicionais (como RADIUS ou TACACS+). Em vez disso, eles podem interagir com o ISE por meio de APIs REST, simplificando a integração da autenticação do ISE em aplicativos baseados na Web ou nativos da nuvem.

3. Autenticação Flexível e Escalável: O Serviço de Autenticação REST fornece um método escalável de autenticação que não se limita apenas a dispositivos de rede ou soluções locais. Ele pode ser usado por serviços em nuvem, aplicativos móveis e outras plataformas baseadas na Web que precisam autenticar usuários ou dispositivos consultando o ISE para obter credenciais e políticas.

4. Fácil de Aplicar: A API REST oferece uma interface padronizada, que é mais fácil de aplicar e integrar com software e aplicativos modernos em comparação com os métodos tradicionais. Ele fornece respostas formatadas JSON e usa métodos HTTP como GET, POST, PUT e DELETE, tornando-o mais acessível para desenvolvedores web e sistemas integrando ISE para autenticação.

Verificação e solução de problemas para Rest Auth

1. Para solucionar problemas relacionados à API aberta, defina o componente apiservice como debug.

2. Para solucionar problemas relacionados à API ERS, defina o componente ers como debug.

Se a página da GUI do serviço de API: https://{iseip}:{port}/api/swagger-ui/index.html ou https://{iseip}:9060/ers/sdk está acessível, ele conclui que o serviço de API está funcionando conforme esperado.

Consulte a Documentação da API para obter mais informações sobre a API.

Conector SSE

O conector SSE (Secure Software-Defined Edge Connector) é um serviço que integra o ISE com a solução Cisco Secure Software-Defined Access (SD-Access). O conector SSE permite que o ISE se comunique com segurança com o Cisco DNA Center, permitindo políticas de rede automatizadas, segmentação e gerenciamento de segurança de borda em um ambiente de acesso SD.

Principais funções do conector SSE

1. Integração com sistemas de segurança de terceiros: O conector SSE facilita a integração do Cisco ISE com sistemas de segurança de terceiros, como firewalls, sistemas de prevenção contra invasões (IPS), soluções de controle de acesso à rede (NAC) e sistemas de gerenciamento de eventos e informações de segurança (SIEM). Ele permite que esses sistemas externos enviem ou recebam dados do ISE de maneira segura, que pode ser usada para aplicação de política mais dinâmica.

2. Inteligência de ameaças em tempo real: Ao conectar o ISE com outros sistemas de segurança, o conector SSE permite a troca de inteligência de ameaças em tempo real. Essas informações podem incluir atividade suspeita, endpoints comprometidos ou comportamentos mal-intencionados detectados por outros sistemas de segurança, permitindo que o ISE ajuste dinamicamente as políticas de acesso com base nos níveis de ameaça atuais ou no status do dispositivo.

3. Correção Automatizada: A integração habilitada pelo Conector SSE pode oferecer suporte a fluxos de trabalho de correção automatizados. Por exemplo, se um sistema é sinalizado como comprometido por um dispositivo de segurança externo, o ISE pode aplicar automaticamente políticas que bloqueiam o acesso à rede ou redirecionam o endpoint para um segmento de rede

de remediação para investigação adicional.

Verificar e solucionar problemas do conector SSE

1. O conector SSE é habilitado apenas quando o serviço PassiveID está habilitado no ISE.

2. O componente sse-connector (connector.log) na depuração fornece mais informações sobre mensagens relacionadas ao Conector SSE.

Hermes (Agente de nuvem pxGrid)

Hermes (pxGrid Cloud Agent) é um componente que facilita a integração entre o ISE e o ecossistema pxGrid (Platform Exchange Grid) em um ambiente de nuvem. Hermes é o agente baseado em nuvem usado para permitir a comunicação entre o ISE e serviços ou plataformas baseados em nuvem, oferecendo suporte à estrutura pxGrid para compartilhamento de informações contextuais em diferentes sistemas de rede e segurança.

Principais recursos e funções do Hermes (pxGrid Cloud Agent)

1. Integração entre a nuvem e o local: O Hermes (pxGrid Cloud Agent) foi projetado para facilitar a integração perfeita entre os serviços baseados em nuvem e a infraestrutura ISE local. Ele estende o poder do pxGrid além dos ambientes de rede locais tradicionais, permitindo a troca segura de dados e a aplicação de políticas em aplicativos e serviços baseados em nuvem.

2. Suporte ao ecossistema do pxGrid: O pxGrid é uma plataforma da Cisco para o compartilhamento seguro de contexto e informações em soluções de segurança de rede. Hermes atua como o agente de nuvem do pxGrid, permitindo a comunicação segura e em tempo real entre o ISE e vários serviços baseados em nuvem. Essa integração permite que as políticas de segurança de rede sejam consistentes em ambientes no local e em nuvem, facilitando o gerenciamento e a aplicação da segurança.

3. Visibilidade de endpoint baseada em nuvem: Uma das principais vantagens do Hermes é que ele oferece visibilidade em endpoints baseados em nuvem, semelhante à maneira como o ISE oferece visibilidade em endpoints locais. Ele pode coletar dados sobre dispositivos e usuários na nuvem, como sua postura de conformidade, status de segurança e informações de identidade. Isso permite que o ISE aplique políticas de acesso à rede em endpoints na nuvem da mesma forma que faria com dispositivos locais.

4. Extensão integrada do ISE para ambientes de nuvem: Um dos principais benefícios do Hermes é que ele fornece uma ponte perfeita entre o ambiente local do ISE e o número crescente de aplicativos nativos da nuvem. Isso facilita a extensão das políticas de segurança, dos métodos de autenticação e dos controles de acesso do ISE aos serviços em nuvem sem exigir uma revisão completa da infraestrutura existente.

Verificar e solucionar problemas do Hermes (Pxgrid Cloud Agent)

1. Por padrão, o serviço Hermes está desabilitado, conectando o ISE à nuvem Cisco PxGrid, o serviço Hermes é

habilitado. Portanto, se o serviço Hermes estiver desabilitado no ISE, verifique se a opção Pxgrid Cloud está habilitada em **ISE GUI > Administração > Implantação, selecione o nó ISE**. Edite , **habilite o Pxgrid Cloud.**

2. As depurações úteis para solucionar problemas relacionados à nuvem Pxgrid são **hermes.log** e **pxcloud.log**. Essas depurações estão disponíveis somente no nó Pxgrid em que a nuvem Pxgrid está habilitada.

McTrust (Serviço de sincronização Meraki)

O McTrust (Meraki Sync Service) é um serviço que permite a integração entre os sistemas Cisco ISE e Cisco Meraki, especificamente para sincronizar e gerenciar dispositivos de rede e políticas de acesso. O serviço McTrust atua como um conector que sincroniza as informações do usuário e do dispositivo entre a infraestrutura de rede gerenciada em nuvem da Meraki e os sistemas de gerenciamento de identidade e políticas locais do ISE.

Principais recursos e funções do McTrust (Meraki Sync Service)

1. Integração perfeita com dispositivos Meraki: O McTrust permite que o ISE sincronize e se integre aos dispositivos gerenciados em nuvem da Meraki. Isso inclui dispositivos como access points, switches e dispositivos de segurança da Meraki que fazem parte do portfólio da Meraki. Ele permite que o ISE se comunique diretamente com a infraestrutura da Meraki, facilitando a aplicação de políticas de controle de acesso à rede para dispositivos gerenciados pela Meraki.

2. Sincronização Automatizada de Dispositivos: O Meraki Sync Service sincroniza automaticamente as políticas do ISE com os dispositivos de rede da Meraki. Isso significa que quaisquer alterações feitas nas políticas de controle de acesso à rede no ISE são refletidas automaticamente nos dispositivos Meraki, sem exigir intervenção manual. Isso facilita o gerenciamento do acesso à rede pelos administradores nas plataformas Meraki e ISE.

3. Aplicação de políticas para dispositivos gerenciados pela Meraki: O McTrust permite que o ISE aplique políticas de acesso à rede em dispositivos Meraki com base na autenticação e na postura do dispositivo. Ele pode atribuir dinamicamente políticas aos elementos de rede da Meraki, como ajustar atribuições de VLAN, aplicar listas de controle de acesso (ACLs) ou restringir o acesso a determinados recursos de rede, dependendo da postura de segurança do dispositivo ou do usuário que solicita o acesso.

4. Integração do painel Meraki: O McTrust integra o ISE diretamente ao painel da Meraki, fornecendo uma interface de gerenciamento unificada. Por meio dessa integração, os administradores podem visualizar e gerenciar políticas de rede e regras de controle de acesso para dispositivos Meraki e recursos gerenciados pelo ISE, tudo a partir da interface gerenciada em nuvem da Meraki.

Verifique e solucione problemas do McTrust (Meraki Sync Service)

1. Faça login na GUI do ISE -> Centros de trabalho -> TrustSec -> Integrações -> Status de sincronização. Verifique todos os problemas/erros observados.

2. Verifique se todos os certificados de administrador dos nós do ISE estão ativos e válidos.

A depuração útil para solucionar problemas do Meraki Sync Service é meraki-connector.log.

Exportador de nó do ISE

O serviço Exportador de Nós do ISE é um componente usado para monitorar e coletar métricas de desempenho do sistema ISE, especificamente dos nós do ISE (sejam eles nós de administração, nós de monitoramento ou nós de serviço de política).

Principais recursos e funções do ISE Node Exporter

1.Exportação de métricas: O ISE Node Exporter fornece uma variedade de métricas relacionadas ao desempenho, como uso da CPU, uso da memória, utilização do disco, estatísticas da rede, carga do sistema e outras métricas do sistema operacional. Essas métricas são usadas para monitorar a integridade e o desempenho do nó do ISE e podem ser visualizadas em um painel de monitoramento como o Grafana.

2. Monitoramento da Integridade do Sistema: Ao exportar os dados de desempenho para Prometheus, o ISE Node Exporter permite o monitoramento contínuo da integridade e do status operacional do nó do ISE. Os administradores podem criar alertas com base em limites predefinidos para notificá-los de degradação de desempenho ou problemas do sistema.

3. Integração Prometheus: O ISE Node Exporter é normalmente usado em conjunto com o Prometheus, um kit de ferramentas de monitoramento e alerta de código aberto projetado para confiabilidade e escalabilidade. O Node Exporter expõe métricas de nível de sistema que podem ser raspadas por Prometheus para coletar e armazenar dados de séries temporais.

Serviço Prometheus do ISE

O ISE Prometheus Service é um serviço que integra o Prometheus com o ISE para permitir o monitoramento e a coleta de métricas de desempenho do sistema ISE. O Prometheus é um kit de ferramentas de monitoramento e alerta de código aberto usado para coletar, armazenar e analisar dados de séries temporais, e o ISE Prometheus Service permite que o ISE exponha suas métricas internas ao Prometheus para fins de monitoramento.

Principais recursos e funções do ISE Prometheus Service

1. Coleta de Métricas para Monitoramento: O serviço Prometheus do ISE foi projetado para exportar várias métricas operacionais e de desempenho relacionadas ao sistema ISE. Essas métricas normalmente incluem, sem limitação, utilização da CPU e carga do sistema, uso de memória, uso de disco e desempenho de E/S, estatísticas de rede, estatísticas de solicitação de autenticação, estatísticas de aplicação de política, dados de integridade e tempo de atividade do sistema

2. Integração Prometheus: O Prometheus Service permite que o ISE exponha dados em um formato compatível com o Prometheus, que remove esses dados em intervalos regulares. Prometheus então armazena os dados em um banco de dados de série temporal, tornando possível rastrear tendências e o desempenho histórico do sistema ISE.

3. Visualização e Reportagem com Grafana: O Prometheus Service no ISE integra-se perfeitamente ao Grafana, uma ferramenta de visualização de código aberto popular. Depois de exportar as métricas para Prometheus, os administradores podem usar painéis Grafana para visualizar os dados em tempo real. Isso permite a fácil identificação de gargalos de desempenho, tendências do sistema e possíveis problemas na implantação do ISE.

Serviço ISE Grafana

O ISE Grafana Service é um serviço que fornece visualização de métricas de desempenho do sistema usando Grafana, uma plataforma de código aberto para monitoramento e visualização de dados. Ele se integra ao Prometheus para exibir dados históricos e em tempo real coletados do ISE, permitindo que os administradores criem painéis interativos que forneçam informações sobre a integridade, o desempenho e o uso do sistema ISE.

Principais recursos e funções do ISE Grafana Service

1. Painéis personalizáveis: O Grafana é altamente personalizável, permitindo que os administradores criem e modifiquem painéis de acordo com suas necessidades específicas de monitoramento. Consultas personalizadas podem ser criadas para extrair pontos de dados específicos de Prometheus, e essas consultas podem ser visualizadas em vários formatos como gráficos, tabelas, mapas de calor, e muito mais.

2. Monitoramento centralizado para implantações distribuídas do ISE: Para implantações distribuídas do ISE, em que vários nós do ISE são implantados em locais diferentes, o Grafana fornece uma visão centralizada de todas as métricas do sistema coletadas de cada nó. Isso permite que os administradores monitorem o desempenho de toda a implantação do ISE a partir de um único local.

3. Dados históricos e análise de tendências: Com os dados armazenados em Prometeu, o Grafana permite a análise histórica de métricas do sistema, permitindo que os administradores acompanhem as tendências ao longo do tempo. Por exemplo, eles podem monitorar como o uso da CPU mudou no mês passado ou como as taxas de sucesso de autenticação flutuaram. Esses dados históricos são valiosos para o planejamento de capacidade, a análise de tendências e a identificação de problemas de longo prazo.

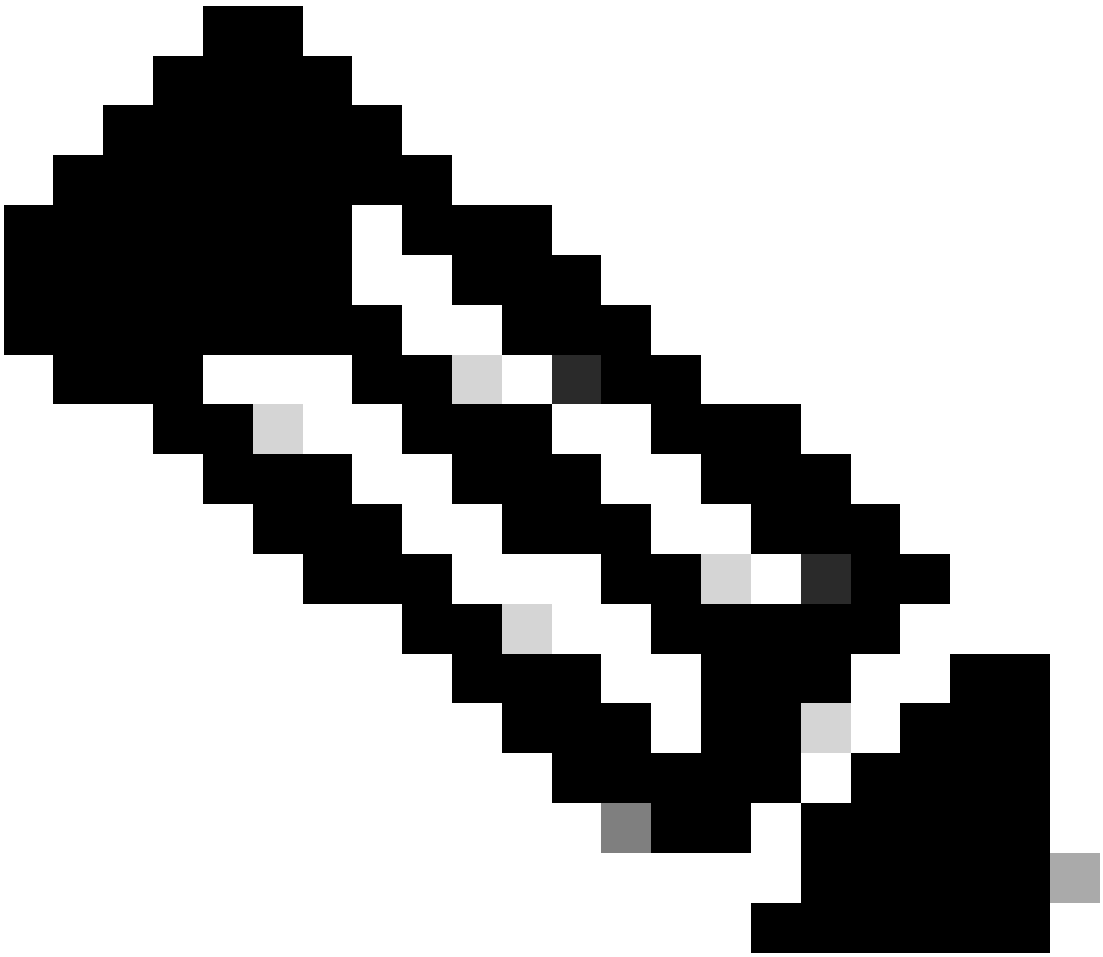
Verificar e solucionar problemas do ISE Grafana Service, do ISE Prometheus Service, do ISE Node Exporter

1. Os serviços ISE Grafana, ISE Prometheus e ISE Node Exporter funcionam juntos e são chamados de serviços de pilha do Grafana. Não há depurações específicas a serem habilitadas para solucionar problemas desses serviços. No entanto, esses comandos ajudam na solução 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



Note: Quando a monitoração está ativada, o ISE Node Exporter, o ISE Prometheus Service e o ISE Grafana Service devem estar em execução e a interrupção de qualquer um desses serviços pode causar problemas durante a coleta de dados.

LogAnalytics de MNT do ISEPesquisa elástica

O Elasticsearch do ISE MNT LogAnalytics é um componente que integra o Elasticsearch aos recursos de Monitoramento e Solução de Problemas (MNT) do ISE. Ele é usado para agregação, pesquisa e análise de logs relacionados a eventos e logs do ISE. O Elasticsearch é um mecanismo de pesquisa e análise amplamente utilizado e distribuído e, quando integrado ao ISE, aumenta a capacidade do sistema de armazenar, analisar e visualizar dados de registro gerados pelos componentes do ISE.

Principais recursos e funções do ISE MNT LogAnalytics Elasticsearch

1. Armazenamento e Indexação de Logs: O serviço Elasticsearch no ISE é responsável por armazenar e indexar os dados de log gerados pelo ISE. O Elasticsearch é um mecanismo distribuído de pesquisa e análise e permite que os logs do ISE sejam armazenados de forma a

permitir pesquisa rápida, consulta e recuperação de eventos, erros ou atividades do sistema específicos.

2. Integração com o Log Analytics: O ISE MNT LogAnalytics Elasticsearch funciona em conjunto com o Log Analytics para fornecer uma solução de registro abrangente. Ele permite que o ISE colete dados de registro relacionados à autenticação, aplicação de políticas, operações do sistema e outras atividades. Esses dados são armazenados no Elasticsearch, facilitando a realização de análises detalhadas e a obtenção de informações sobre o comportamento do ISE.

3. Registro centralizado: Integrando-se ao Elasticsearch, o ISE fornece uma solução de registro centralizado, que é crucial para ambientes que exigem coleta de registros distribuídos. Isso permite que os administradores visualizem e analisem registros de vários nós do ISE em uma única interface unificada, facilitando a solução de problemas e o monitoramento do desempenho do ISE.

4. Análise de Log e Solução de Problemas: O serviço ISE MNT LogAnalytics Elasticsearch ajuda os administradores a analisar o comportamento do sistema e solucionar problemas tornando os dados de registro facilmente acessíveis. Por exemplo, se houver um pico repentino nas falhas de autenticação ou uma interrupção inesperada do sistema, o Elasticsearch permitirá uma consulta rápida dos dados de log para identificar a causa raiz.

Verificar e solucionar problemas do LogAnalytics do ISE M&T Elasticsearch

1. A desativação e reativação do serviço de análise de log no ISE deve ajudar. Navegue até Operations > System 360 > Settings > Log analytics (desabilitar e habilitar usando a opção de alternância).

2. Reiniciar o LogAnalytics M&T a partir da Raiz ISE resolve o problema. Entre em contato com o TAC da Cisco para executar essa ação.

Defeitos conhecidos

Identificação de bug da Cisco ·66198

Serviço Logstash ISE

O ISE Logstash Service é um componente que integra o Logstash, um pipeline de processamento de dados de código aberto, com o ISE para coleta, transformação e encaminhamento de logs. O Logstash atua como coletor e encaminhador de registros, permitindo que os registros do ISE sejam processados e enviados a outros sistemas para análise, armazenamento e monitoramento. O Logstash é uma ferramenta poderosa de código aberto que coleta, analisa e encaminha logs ou outros dados de diferentes fontes para um local central para armazenamento, análise e visualização. No contexto do ISE, o serviço Logstash do ISE é usado para processar e encaminhar logs em um formato estruturado para um sistema de registro centralizado, onde eles podem ser analisados, monitorados e visualizados posteriormente.

Principais recursos e funções do serviço Logstash do ISE

1. Coleta e encaminhamento de logs: A principal função do serviço Logstash do ISE é coletar dados de log de vários componentes do ISE (como logs de autenticação, logs do sistema, logs de aplicação de políticas etc.) e encaminhá-los para um local central (normalmente Elasticsearch ou outro sistema de gerenciamento de logs) para armazenamento e análise.

2. Análise do Log: O Logstash pode analisar os logs coletados em formatos estruturados. Ele processa dados brutos de registro e extrai informações significativas deles, transformando as entradas de registro em um formato mais fácil de consultar e analisar. Isso pode envolver filtragem, análise e enriquecimento dos dados antes de encaminhá-los para o Elasticsearch ou outros sistemas.

Verificar e solucionar problemas do serviço Logstash do ISE

1. Nenhuma depuração específica a ser habilitada. No entanto, **show logging application ise-logstash/logstash.log** fornece insights sobre o status do serviço.

2. A desativação e reativação do serviço de análise de log no ISE deve ajudar. Navegue para **Operations > System 360 > Settings > Log analytics** (desabilite e habilite usando a opção de alternância).

Defeitos conhecidos relacionados ao serviço Logstash

Identificação de bug da Cisco ·74832

Identificação de bug da Cisco ·58596

Serviço ISE Kibana

O ISE Kibana Service é um componente que integra o Kibana, uma ferramenta de visualização de dados de código aberto, com a infraestrutura de monitoramento e registro do ISE. Kibana trabalha em conjunto com Elasticsearch (que armazena e indexa dados de registro) para fornecer uma plataforma poderosa para visualizar, pesquisar e analisar registros ISE e métricas de desempenho.

Principais recursos e funções do ISE Kibana Service

1. Visualização de Dados: O Serviço Kibana do ISE permite que os administradores criem representações visuais dos dados de registro coletados do ISE. Isso pode incluir:

- Gráficos, tabelas e tabelas para tendências em autenticação, aplicação de políticas, atividade do usuário e integridade do sistema.
- Gráficos de pizza, linhas e barras para controlar métricas específicas, como o número de falhas de login, duração da sessão ou erros ao longo do tempo.

Verificar e solucionar problemas do serviço Kibana do ISE

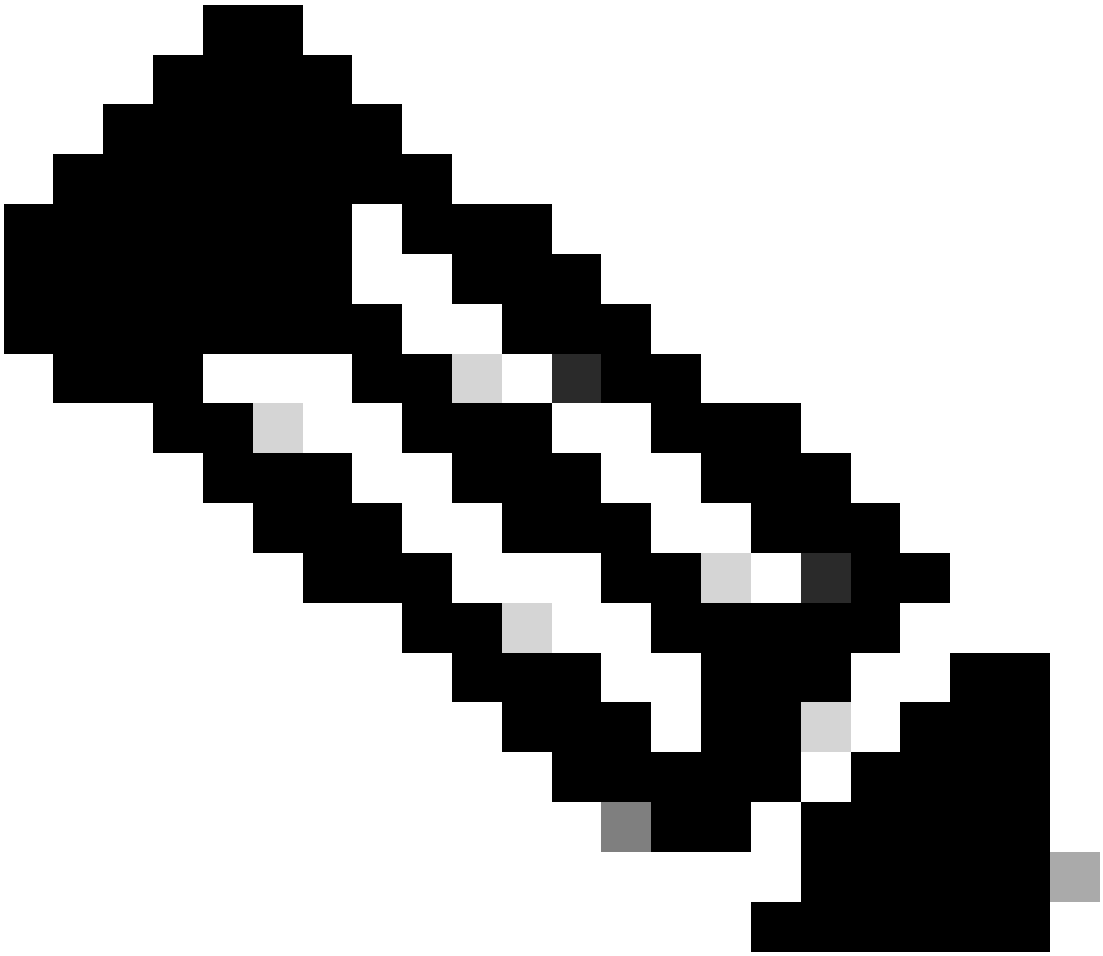
1. Se o serviço kibana do ISE não estiver em execução, desabilite e habilite novamente a análise de log no ISE, navegue para Operações > System 360 > Configurações, Análise de log (desabilite e habilite usando a opção de alternância).

2. Em muitos cenários, pode haver uma entrada duplicada na pasta /etc/hosts que deve estar causando um problema. Entre em contato com o TAC para remover a entrada duplicada.

Defeitos conhecidos relacionados ao problema Kibana

Identificação de bug da Cisco ·78050

Identificação de bug da Cisco ·59848



> Note: Quando a análise de log está habilitada, o ISE MNT LogAnalytics Elasticsearch, o ISE Logstash Service e o ISE Kibana Service devem estar em execução e a interrupção de qualquer um desses serviços cria problemas durante a coleta de dados.

Serviço IPSec nativo do ISE

O Serviço IPSec Nativo do ISE refere-se ao suporte integrado para IPSec (Internet Protocol Security), que fornece comunicação segura entre os nós do ISE ou entre o ISE e outros dispositivos de rede. O IPSec é um conjunto de protocolos usado para proteger as comunicações

de rede, autenticando e criptografando cada pacote IP em uma sessão de comunicação.o Serviço IPSec Nativo faz parte da estrutura de gerenciamento de segurança e acesso à rede mais ampla. Ele fornece recursos para manipular e gerenciar conexões VPN IPsec, garantindo que os dados transmitidos entre o sistema ISE e endpoints remotos sejam seguros. Isso pode envolver interações com dispositivos clientes, dispositivos de acesso à rede (como roteadores ou firewalls) ou até mesmo outros nós do ISE, onde a criptografia e o encapsulamento IPsec são necessários para proteger informações confidenciais.

Principais recursos e funções do serviço IPSec nativo do ISE

1. Comunicação Segura via IPsec: A função principal do ISE Native IPSec Service é estabelecer e manter canais de comunicação seguros usando IPsec. Isso envolve o uso de mecanismos de criptografia e autenticação para garantir que os dados transmitidos entre o ISE e outros dispositivos estejam protegidos contra interceptação, violação e acesso não autorizado.

2. Conectividade VPN IPsec: O Serviço IPSec Nativo do ISE ajuda a facilitar as conexões VPN que usam o protocolo IPsec para fornecer um túnel seguro e criptografado para a transmissão de dados. Isso é especialmente útil para funcionários remotos, filiais ou outros locais que precisem acessar com segurança o ambiente do ISE em redes não confiáveis (como a Internet).

3. Suporte para VPN de Acesso Remoto: O Serviço IPSec Nativo pode estar envolvido em configurações de VPN de acesso remoto, onde usuários ou dispositivos localizados fora do local (como funcionários remotos ou filiais) se conectam com segurança ao sistema ISE através de túneis IPsec. Esse serviço garante que todo o tráfego de acesso remoto seja criptografado e autenticado antes de acessar o ambiente do ISE.

4.Compatibilidade do IPsec VPN Client: O ISE Native IPSec Service garante compatibilidade com clientes VPN IPsec. Ele suporta configurações comuns de clientes, permitindo que os dispositivos se conectem com segurança à rede sem expor dados confidenciais a riscos.

Verificar e solucionar problemas do serviço IPSec nativo

1. Não há depurações específicas a serem habilitadas para o serviço IPSec Nativo. Verifique os logs usando o comando show logging application strongswan/charon.log tail via ISE CLI.

2. Se algum problema for observado para o túnel, verifique o status do estabelecimento do túnel via GUI > Administração > Sistema > Configurações > Protocolos > IPSec > IPSec Nativo.

MFC Profiler

O MFC Profiler é um componente especializado usado para criar perfis de dispositivos de rede e endpoints. A criação de perfis é uma parte importante do controle de acesso à rede, pois permite que o ISE identifique dispositivos na rede, os classifique e aplique políticas de rede apropriadas com base no tipo de dispositivo e comportamento.

Principais recursos e funções do serviço MFC Profiler no ISE

1. Definição de perfis de tráfego: O serviço MFC Profiler no ISE é responsável por coletar e criar o perfil dos dados de tráfego. Ele monitora como os endpoints se comportam na rede, incluindo os tipos de aplicativos que estão sendo usados, os serviços acessados e os padrões de tráfego exibidos pelos dispositivos. Esses dados ajudam a criar um perfil para cada endpoint.

2. Criação de perfis de endpoint: O serviço MFC Profiler permite que o ISE identifique e classifique os endpoints com base em seu comportamento. Por exemplo, ele detecta se um endpoint é uma impressora, um computador ou um dispositivo móvel com base nos padrões de tráfego. Isso pode ajudar a aplicar políticas mais específicas para diferentes tipos de dispositivos, melhorando a segurança e a eficiência operacional.

Verificar e Solucionar Problemas do Serviço do Profiler do MFC

1. Navegue até ISE GUI -> Administration -> Profiling -> MFC profiling e AI rules, verifique se o serviço está habilitado.

2. Se o serviço estiver habilitado, mas estiver sendo exibido como desabilitado / não sendo executado através do comando show application status ise na CLI do ISE. Desabilite e reabilite o serviço de criação de perfil do MFC no ISE, consultando a Etapa 1.

Depurações úteis para solução de problemas: Componente do MFC Profiler em depuração. Os registros podem ser verificados a partir do pacote de suporte ou da parte final dos registros usando o comando show logging application ise-pi-profiler.log tail via CLI do ISE.

Defeito conhecido para o MFC Profiler mostrando que não está em execução em vez de estado desabilitado:

Identificação de bug da Cisco ·72853

Pontos principais

1. Para recuperar os serviços, reinicie-os usando os comandos application stop ise e application start ise via CLI do ISE.

2. Quando houver um problema, certifique-se de que haja um pacote de suporte sendo capturado da GUI/CLI do ISE para verificação adicional do problema. Link de referência para criação do pacote de suporte ISE via GUI e CLI: Coletar pacote de suporte no Identity Services Engine

3. Se os Problemas estiverem relacionados a recursos, média de carga, utilização do disco e assim por diante, será obrigatório coletar despejo de thread e despejo de pilha para análise.

4. Antes de executar o recarregamento do nó, entre em contato com o Cisco TAC e forneça registros protegidos para análise adicional.

Preocupações padrão no ISE

Além dos problemas com os serviços do ISE, essas são algumas das preocupações encontradas nos nós do ISE, juntamente com as etapas básicas necessárias para a solução de problemas.

Verificação para Média de Carga Alta, Problemas de Utilização de Recursos (CPU / MEMÓRIA / DISCO), Recursos Insuficientes

1. Verifique se os recursos recomendados pela Cisco estão alocados para o nó usando o comando show inventory via CLI do ISE.

2. Na CLI do nó do ISE, execute o comando tech top para verificar a utilização de recursos do ISE.

3. Verifique a utilização do disco usando o comando show disk via CLI do ISE.

4. Limpe os pontos finais inativos, limpe o disco local do nó e execute limpezas de atualização.

Se o problema persistir, entre em contato com o TAC da Cisco e forneça o pacote de suporte seguro, o despejo de pilha e o despejo de thread do nó que está tendo o problema.

Para proteger o despejo de pilha, faça login na CLI do nó ISE, execute o comando **application configure ise**. Selecione a **opção 22.**

Para proteger o despejo de thread, faça login na CLI do nó do ISE, execute o comando **application configure ise**, selecione a **opção 23.** O despejo de thread está incluído no pacote de suporte ou pode ser realizado via CLI do ISE usando o comando **show logging application appserver/catalina.out**.

Verificar e solucionar problemas de monitoramento

A função de Monitoramento e solução de problemas (MnT) do ISE é um dos principais blocos da arquitetura do ISE que fornece recursos de monitoramento, geração de relatórios e alertas.

O ISE exibe informações de monitoramento em vários locais, incluindo:

- Página inicial do Cisco ISE
- Visualizações de Visibilidade de contexto
- Sessões ao vivo e registros ao vivo RADIUS
- Pesquisa global
- Registros dinâmicos do NAC centrados em ameaças
- Registros ao vivo TACACS

Problemas gerais observados na Categoria Monitoramento e Solução de Problemas:

1. Logs ao vivo do Radius/ TACACS não disponíveis
2. Sessões ao vivo não disponíveis
3. Resumo da integridade não disponível
4. Problemas de desempenho (alta utilização da CPU/memória) observados nos nós MnT

Depurações a serem habilitadas nos nós MnT para restringir o problema:

1. Cisco-mnt
2. Coletor
3. Cpm-mnt
4. runtime-logging

Além dos componentes mencionados em debug, essas informações podem ajudar na solução de problemas:

1. As sessões ao vivo também são afetadas ou apenas os logs ao vivo?
2. Os registros Radius ou TACACS são afetados ou ambos?
3. Você vê alta utilização da CPU ou alto uso de espaço de troca em nós MnT?
4. Quantos arquivos de buffer você vê nos nós MnT. Os arquivos de buffer podem ser encontrados em: /opt/CSCOcpm/mnt/data/collector.
5. As reservas de memória e CPU estão habilitadas? Caso contrário, habilite-as.
6. A redefinição de MnT/config/session DB foi realizada recentemente?
7. Você está vendo syslogs sendo enviados de PSNs para nós MnT?

Se você estiver usando serviços Syslog para MnT, estas informações serão necessárias para fins de solução de problemas:

1. Você está usando um destino de syslog seguro? Caso contrário, desabilite-o, pois sabe-se que ele causa deadlocks nos threads, fazendo com que o coletor pare de funcionar?
2. Você está usando um destino syslog seguro, verifique se o mapeamento de certificado está definido corretamente em Administração -> Registro -> Destinos de registro remoto -> Coletor Syslog seguro 1 e 2
3. Verifique se as categorias de log estão definidas adequadamente (recomendado para remover categorias de log não utilizadas/indesejadas - isso reduz a carga nos nós MnT) e se os destinos de log estão configurados corretamente.
4. Verifique os arquivos awrrep*.html do pacote de suporte para entender e obter uma dica de qual componente está enviando syslogs mais frequentes, por exemplo, se as tabelas TACACS estiverem sendo visualizadas com consultas de inserção ou atualização, podemos verificar os logs do coletor para correlacionar e entender quais syslogs estão sendo enviados com mais frequência

Se o problema estiver relacionado ao desempenho no nó MnT, precisamos destas informações:

1. saída técnica superior do ISE CLI do nó MnT.

2. Se a CPU estiver alta, você também observará alta utilização de memória ou de espaço de troca?

3. Pacote de suporte com despejo de pilha e despejo de thread protegidos.

Referência

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.3
- Solucionar problemas e ativar depurações no ISE

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.