Understand ISE Services Purpose and Troubleshooting

Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Background Information
- Understanding and Troubleshooting ISE Services
  - Database Listener
    - Key Points on the Database Listener Service in ISE
  - Database Server
    - Key Points on the Database Server Service in ISE
    - Verify and Troubleshoot the Database Listener and Database Server Services are Initializing or not Running
  - Application Server
    - Key Points on the Application Server Service in ISE
    - Verification for Application Server is Initializing or Not Running
  - Profiler Database
    - Key Points about the Profiler Database Service in ISE
    - Verify and Troubleshoot ISE Profiling Services
  - ISE Indexing Engine
    - Key Points about the ISE Indexing Engine in ISE
    - Verify the ISE Indexing Engine is not Running or Initializing
  - AD Connector
    - Key Functions of the AD Connector Service in ISE
  - M&T Session Database
    - Key Functions of M&T Session Database Service in ISE
    - Verify and Troubleshoot M&T Session Database in ISE
  - M&T Log Processor
    - Key Functions of the M&T Log Processor Service in ISE
    - Verify and Troubleshoot M&T Log Processor Service in ISE
  - Certificate Authority Service
    - Key Functions of Certificate Authority Service in ISE
  - EST Service
    - Key Functions of the EST Service in ISE
    - Verify Certificate Authority and EST Service not Running/Initializing
  - SXP Engine Service
    - Key Functions of SXP Engine Service in ISE
    - Verification and Troubleshooting for SXP Engine Service in ISE
  - TC-NAC Service
    - Key Functions of the TC-NAC Service in ISE
    - Verify and Troubleshoot TC-NAC Service in ISE
  - PassiveID WMI Service

- Key Functions of the PassiveID WMI service in ISE
- Verify and Troubleshoot PassiveID WMI Service

PassiveID Syslog Service

- Key Functions of the Passive ID Syslog Service

PassiveID API Service

- Key Functions of the Passive ID API Service

PassiveID Agent Service

- Key Functions of the Passive ID Agent Service

PassiveID Endpoint Service

- Key Functions of the PassiveID Endpoint Service

PassiveID SPAN Service

- Key Functions of the PassiveID SPAN Service
- Verification and Troubleshooting for PassiveID Stack (PassiveID SPAN Service, PassiveID Syslog Service, PassiveID Endpoint Service, PassiveID Agent, PassiveID API Service)

DHCP Server (dhcpd)

- Key Functions of the DHCP Server (dhcpd) Service in ISE
- Verify and Troubleshoot DHCP Server (dhcpd)

DNS Server (Named)

- Key Functions of the DNS Server (Named) Service in ISE
- Verify and Troubleshoot for DNS Server (Named)

ISE Messaging Service

- Key Functions of the ISE Messaging Service
- Verify the ISE Messaging Service is not Running or Initializing

ISE API Gateway Database Service

- Key Functions of the ISE API Gateway Database Service
- ISE API Gateway Service
- Key Functions of the ISE API Gateway Service
- Verify and Troubleshoot ISE API Gateway Service and ISE API Gateway Database Service

ISE pxGrid Direct Service

- Key Functions of ISE pxGrid Direct Service
- Verify and Troubleshoot ISEPxgrid Direct Service

Segmentation Policy Service

- Key Functions of the Segmentation Policy Service
- Verify and Troubleshoot Segmentation Policy Service

REST Auth Service

- Key Functions of the REST Auth Service
- Verification and Troubleshooting for Rest Auth

SSE Connector

- Key Functions of the SSE Connector
- Verify and Troubleshoot SSE Connector

Hermes (pxGrid Cloud Agent)

- Key Features and Functions of Hermes (pxGrid Cloud Agent)
- Verifiy and Troubleshoot Hermes (Pxgrid Cloud Agent)

McTrust (Meraki Sync Service)

- Key Features and Functions of McTrust (Meraki Sync Service)
- Verify and Troubleshoot McTrust (Meraki Sync Service)

ISE Node Exporter

- Key Features and Functions of ISE Node Exporter

ISE Prometheus Service

- Key Features and Functions of ISE Prometheus Service

- ISE Grafana Service
  - Key Features and Functions of ISE Grafana Service
  - Verify and Troubleshoot ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter
- ISE MNT LogAnalytics Elasticsearch
  - Key Features and Functions of ISE MNT LogAnalytics Elasticsearch
  - Verify and Troubleshoot ISE M&T LogAnalytics Elasticsearch
- ISE Logstash Service
  - Key Features and Functions of the ISE Logstash Service
  - Verify and Troubleshoot ISE Logstash Service
- ISE Kibana Service
  - Key Features and Functions of the ISE Kibana Service
  - Verify and TroubleshootISE Kibana Service
- ISE Native IPSec Service
  - Key Features and Functions of ISE Native IPSec Service
  - Verify and Troubleshoot Native IPSec Service
- MFC Profiler
  - Key Features and Functions of the MFC Profiler Service in ISE
  - Verifiy and Troubleshoot MFC Profiler Service

Services included in ISE 3.4

- MFA (Duo Sync Service)
  - Key Features and Functions of MFA (Duo Sync Service) in ISE
  - Verify and Troubleshoot MFA (Duo Sync Service)
- Aciconn (ACI Connection Service)
  - Key Features and Functions of Aciconn Service in ISE
  - Verify and Troubleshoot Aciconn
- ISE Prometheus Exporter
  - Key Features and Functions of ISE Prometheus Service in ISE
  - Verify and Troubleshoot ISE Prometheus Exporter
- ISE Prometheus Alert Manager
  - Key Features and Functions of ISE Prometheus Alert Manager Service in ISE
  - Verify and Troubleshoot ISE Prometheus Alert Manager
- Protocols Engine
  - Key Features and Functions of the Protocols Engine Service in ISE
  - Verify and Troubleshoot Protocols Engine

Services Included in ISE 3.5

- Remote Support Authorization Service
  - Key Features and Functions of Remote Support Authorization Service in ISE
  - Verify and Remote Support Authorization Service in ISE
- ISE Prometheous Alert Manager Service
  - Key Features and Functions of ISE PrometheusAlert Manager Service in ISE
  - Verify ISE Prometheous Alert Manager Service in ISE
- ISE DataGrid Service
  - Key Features and Functions of ISE DataGrid Service in ISE
  - Verify ISE DataGrid Service in ISE

Standard Concerns in ISE

- Verification for High Load Average, ResourceUtilization Issues (CPU/MEMORY/DISK), Insufficient Resources
- Verify and Troubleshoot Monitoring Issues

Reference

Introduction

This document describes ISE services, purpose and troubleshooting.

Prerequisites

Radius

Requirements

Cisco recommends that you have knowledge on:

- Cisco Identity Services Engine

Components Used

The document is not restricted to any specific software and hardware versions of Cisco Identity Services Engine.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Identity Services Engine (ISE) is a comprehensive solution designed to provide advanced network security through centralized policy management, authentication, authorization, and accounting (AAA). It enables organizations to manage network access for users, devices, and applications while ensuring security, compliance, and seamless user experiences.

To achieve these goals, Cisco ISE utilizes a range of services, each responsible for specific tasks that enable the system to function efficiently. These services work together to ensure secure network access, robust policy enforcement, detailed logging, seamless integrations with external systems, and efficient device profiling.

Each service in ISE plays a vital role in maintaining the integrity and availability of the solution. Some services handle core functions, such as database management and authentication, while others enable advanced features like device profiling, certificate management, and monitoring.

This article provides an overview of the various services in Cisco ISE, explaining their purpose, importance, and potential troubleshooting steps if they experience issues. Whether you are an administrator or a network security professional, understanding these services helps ensure your ISE deployment runs smoothly and securely.

Understanding and Troubleshooting ISE Services

The services mentioned in the next screenshot are utilized by ISE to support its functionality. Verify the status or services available in ISE by running the show application status ise command via CLI of the ISE node. This is a sample output that displays the status or available services on the 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
```

Services available in ISE.

Now, take a closer look at each service in detail.

Database Listener

The Database Listener service is a critical component that assists in managing the communication between ISE and the database server. It listens for and processes requests related to the database, ensuring the ISE system can read from and write to its underlying database.

Key Points on the Database Listener Service in ISE

1. Communication Interface: It acts as the communication bridge between ISE and the database server, allowing the system to retrieve and store data like user credentials, session information, network policies, and more.
2. External Database Support: ISE can be configured to use an external database (such as Oracle or Microsoft SQL Server) for user authentication and policy storage. The Database Listener Service ensures ISE can connect to and interact with this external database securely and efficiently.
3. Data Handling: The service listens for database queries from the ISE system and translates them into the appropriate actions on the external database. It can handle requests such as inserting, updating, or deleting records, and retrieving information from the database.
4. Database Health Monitoring: In addition to providing the communication channel, it also helps ensure the connection to the external database is stable and operational. If the connection fails, ISE falls back to local storage or enters a degraded mode depending on configuration.

Database Server

The Database Server service is responsible for managing the storage and retrieval of data used by the system. It handles the interaction with the underlying database ISE uses to store configuration, policy information, user data, authentication logs, device profiles, and other necessary information.

Key Points on the Database Server Service in ISE

1. Internal Data Storage: The Database Server Service primarily manages the internal embedded database ISE uses to store operational data locally. This includes data such as Authentication and authorization records, User profiles, Network access policies, Device and endpoint information, and Session information.

2. Embedded Database: In most Cisco ISE deployments, the system uses an embedded PostgreSQL database for local storage. The Database Server Service ensures this database operates smoothly and handles all queries, updates, and management tasks related to the data stored within it.

3. Database Integrity: The service ensures all transactions are processed properly and the integrity of the database is maintained. It handles tasks like locking records, managing database connections, and executing database queries.

Verify and Troubleshoot the Database Listener and Database Server Services are Initializing or not Running

The Database Listener and Database Server are essential services that must run together for all other services to function properly. If these services are not running or are stuck during initialization, these troubleshooting steps help in recovery.

---

1. Restart the ISE services by running the application stop ise and application start ise commands.

2. If this is a VM node, restarting of the node from the VM must help recovery of services.

3. If the node is a physical node, restarting/reloading the node from CIMC must help in recovery of services.

4. If the Database is corrupted, contact Cisco TAC for further troubleshooting.

The Database Listener and Database Server typically go down or fail to start when there is a discrepancy in the database or when the database is unable to initialize properly. In those cases, performing application reset by using the command application reset-config ise must help in recovery and fresh initiation of the database. Running the application reset-config ise command removes configurations and certificates, but IP address and domain name details are retained. It is recommended to contact Cisco TAC for further information and to understand the potential impact before applying this command on any node in the deployment.

Application Server

The Application Server is a key component responsible for running and managing the core functionality and services of the ISE platform. It hosts the business logic, user interfaces, and services that allow ISE to perform its role in network access control, authentication, authorization, accounting, and policy management.

Key Points on the Application Server Service in ISE

1. User Interface (UI): The Application Server Service is responsible for rendering the web-based user interface (UI) for ISE. This allows administrators to configure and manage policies, view logs and reports, and interact with other features of ISE.

2. Service Management: It is responsible for handling the various services that ISE provides; including policy management, administrative tasks, and communication with other ISE nodes in a distributed deployment.

3. Centralized Processing: The Application Server Service plays a central role in ISE architecture, providing the logic that interprets the policies, authentication requests, and data from network devices, directories, and external services.

Verification for Application Server is Initializing or Not Running

The Application Server depends on web applications like Certificates, Resources, Deployment, and Licensing. When any of the web applications fail to initialize, the application server stays immobile in the initializing state. The Application Server takes approximately 15 - 35 minutes from Not running → Initializing → Running state, depending on the configuration data on the node.

---

1. Ensure the Admin certificate of ISE is valid and active in the deployment for all nodes.
2. Ensure all nodes in the deployment are in sync with the Primary Admin node.
3. If the node is a VM, ensure the recommended resources are allocated to the node.

Verify the status of application server by running the show application status ise command from CLI of the ISE node. Most logs related to the application server are available under the Catalina.Out and Localhost.log files.

If the conditions are satisfied and the application server remains immobile in the initializing state, secure the support bundle from the CLI/GUI of ISE. Recover/restart the services by running the application stop ise and application start ise commands.

Profiler Database

The Profiler Database is used to store information on network devices, endpoints, and device profiles discovered by the Profiler service. This is a critical component of ISE that automatically identifies and classifies network devices (such as computers, smartphones, printers, IoT devices and so on) based on network characteristics and behaviors.

Key Points about the Profiler Database Service in ISE

1. Device Profiling: The main function of the Profiler Database Service is to support the profiling process. ISE uses this service to store information it gathers during profiling, such as:

- Device type (for example, smartphone, laptop, printer, IoT devices, and so on)

- Device Operating System(s) (Fsor example, Windows®, macOS®, Cisco IOS®, Android®)
- Device Manufacturer
- Network behaviors or patterns that help classify devices

2. Profiler Information: Stores profiler attributes such as the device hardware and software profiles, which are used to match devices to predefined policies. This information is used to dynamically assign devices to the correct network access policies or VLANs based on their profile.

3. Profiling Process: The profiling process is typically based on:

- Active Profiling: ISE actively queries devices on the network for information.
- Passive Profiling: ISE passively gathers data from network traffic, such as DHCP requests, RADIUS attributes, HTTP headers, and other network protocols to determine the device type.

Verify and Troubleshoot ISE Profiling Services

1. From ISE CLI, run the show application status ise command to verify the profiler database service is running.

2. From the GUI of the Primary Admin node, navigate to Administration > Deployment > Select the node. Click Edit and verify the Session Services and ensure Profiling Services are enabled.

3. Now, navigate to Administration > Deployment > Select the node. Move to Profiler Configuration and verify the required probes are enabled for securing the endpoint data.

4. Navigate to Administration > System > Profiling and verify the profiler settings are configured for CoA.

5. From the Context Visibility > Endpoints, select the endpoints and verify the attributes collected by different probes for the endpoints.

Useful debugs for troubleshooting profiling Issues:

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

ISE Indexing Engine

The Indexing Engine is a service responsible for efficiently searching, indexing, and retrieving data stored in

the ISE database. It enhances the performance and scalability of ISE, particularly when it comes to handling large volumes of data and providing quick access to information needed for authentication, authorization, monitoring, and reporting tasks.

Key Points about the ISE Indexing Engine in ISE

1. Data Indexing: The ISE Indexing Engine creates indexes for various types of data stored in ISE, such as authentication logs, session logs, policy hits, profiling data, and network access records. Indexing helps organize data that ensures searching and querying are more efficient.

2. Log Management and Reporting: This service plays a critical role in log management by improving the performance of reporting and log queries. When searching for specific authentication events, the indexing engine enables quicker retrieval of desired records, which is crucial for security monitoring and compliance reporting.

3. Data Retrieval: The indexing engine is also responsible for ensuring ISE can efficiently retrieve indexed data from its underlying database when needed. This allows ISE to provide fast responses to queries from the user interface, external tools, or APIs.

Verify the ISE Indexing Engine is not Running or Initializing

1. Verify forward and reverse DNS lookups are working or all nodes in the cluster via CLI are using the nslookup <FQDN / IP address of the ISE node> command.
2. Verify the ISE Admin Certificates are valid and active for all nodes in the cluster.
3. Verify NTP is working an in sync with the ISE nodes via CLI by running the show ntp command.

The indexing engine is used by Context Visibility and the Indexing Engine must be up and running for Context Visibility to run properly. Useful logs that help with troubleshooting are ADE.log files. These can be secured from the support bundle or tailed through CLI by running the show logging system ade/ADE.log tail command when the issue arises.

AD Connector

The AD Connector (Active Directory Connector) is a service that allows ISE to integrate with Microsoft Active Directory (AD), enabling ISE to authenticate, authorize, and manage users based on their AD credentials and group memberships. The AD Connector serves as a bridge between ISE and Active Directory, allowing ISE to leverage AD for network access control (NAC) and policy enforcement.

Key Functions of the AD Connector Service in ISE

1. Integration with Active Directory: The AD Connector Service acts as a bridge between ISE and Active Directory. It allows ISE to securely connect to AD, allowing ISE to utilize AD as a centralized identity store for user authentication and policy enforcement.
2. Synchronization: The AD Connector Service supports synchronizing user and group data from Active Directory to ISE. This ensures ISE has updated information on users and groups, which is critical for accurate policy enforcement.
3. Secure Communication: The AD Connector Service establishes secure communication channels between ISE and Active Directory, typically using protocols like LDAP over SSL (LDAPS) to ensure data privacy and integrity during authentication and query processes.
4. Multiple Active Directory Domain Support: The service can support connections to multiple Active Directory domains. This is particularly useful in large or multi-domain environments where ISE must authenticate users from different AD forests or domains.
5. User and Group Lookup: This enables ISE to query AD for user and group information. This can include details like usernames, group memberships, and other user attributes that can be used to enforce network access policies. For example, network access policies can be applied based on a user AD group membership (For example: granting different access levels to users in different groups).

---

1. Verify if NTP is in sync with the nodes and time difference between AD and ISE; must be less than 5 minutes.

2. Verify if the DNS server can resolve FQDNs and domains related to AD.

3. Navigate to Operations > Reports > Reports > Diagnostics > AD Connector Operations and verify the events or reports related to AD.

Useful logs for troubleshooting are ad_agent.log with debug logs for runtime component.

M&T Session Database

M&T Session Database (Monitoring and Troubleshooting Session Database) plays a critical role in storing and managing session-related data for network access events. The M&T Session Database holds information on active sessions. This includes user authentications, device connections, and network access events, which is essential for monitoring, troubleshooting, and analyzing network activity.

Key Functions of M&T Session Database Service in ISE

1. Session Data Storage: The M&T Session Database service is responsible for storing and indexing user and device data sessions on the network. This includes session start and end times, authentication results, user or device identity, and the associated policies (such as role assignments or VLAN assignments.) The data also includes RADIUS accounting information that details the session lifecycle, including initial authentication and any accounting messages that tracks session events.
2. Real-time and Historical Data: The service provides access to real-time session data (active sessions) and historical session data (past sessions.) This enables administrators to not only monitor ongoing user access, but look back at past session logs to investigate issues or validate access events. Real-time session monitoring ensures no unauthorized devices are currently on the network.

3. Enhanced Monitoring: Provides insights into user and device activity, including policies applied to their sessions, helping to detect potential security concerns or unauthorized access.
4. Auditing and Reporting: Facilitates compliance auditing and reporting by storing a history of network of access events and providing data for regulatory reporting.

Verify and Troubleshoot M&T Session Database in ISE

1. Verify if the node is allocated with recommended resources.

2. Secure and run the show tech-support from the ISE CLI for further verification of the issue.

3. Reset the M&T session database by running the application configure ise command oin the ISE CLI and select option 1.



Note: Resetting the M&T database must be completed only after verifying the potential impact in the deployment. Contact Cisco TAC for further verification.

Known defects: Cisco bug ID 32364

M&T Log Processor

The M&T Log Processor (Monitoring and Troubleshooting Log Processor) is a component responsible for collecting, processing, and managing log data generated by various services within ISE. It is a key part of the Monitoring and Troubleshooting (M&T) framework, which helps administrators to monitor and troubleshoot network access events, authentication attempts, policy enforcement, and other activities within the ISE system. The M&T Log Processor specifically handles the processing of log entries, ensuring ISE can store, analyze, and present necessary information for reporting, auditing, and troubleshooting.

Key Functions of the M&T Log Processor Service in ISE

1. Log Collection and Processing: The M&T Log Processor Service collects and processes logs generated by various ISE components, such as authentication requests, authorization decisions, accounting messages, and policy enforcement activities. These logs include detailed information about users, devices, and network access attempts, such as timestamps, user IDs, device types, applied policies, success or failure of access requests, and reasons for failures.
2. Reporting and Compliance: Logs processed by this service are critical for compliance reporting. Many regulations require organizations to retain logs of user access and security events. The M&T Log Processor Service ensures all relevant logs are processed and available for regulatory compliance

audits. It helps in generating detailed reports based on log data, such as user access logs, authentication success/failure rates, or policy enforcement logs.

Verify and Troubleshoot M&T Log Processor Service in ISE

1. Ensure the ISE node is deployed with recommended resources per the Cisco Installation Guide.
2. To verify the issue, run thr show logging system ade/ADE.log tail command via the ISE CLI for relevant exceptions/errors.

Known defects: Cisco bug ID15130

Certificate Authority Service

The Certificate Authority (CA) Service is a critical component that assists in managing digital certificates for securing communications and authenticating devices, users, and network services. Digital certificates are essential in establishing trusted connections and ensuring secure communication between clients (computers, smartphones, network devices) and network infrastructure components (switches, wireless access points, VPN gateways.) The CA Service in Cisco ISE works in tandem with X.509 certificates, which are used for several purposes in network security, including 802.1X authentication, VPN access, secure communication, and SSL/TLS encryption.

Key Functions of Certificate Authority Service in ISE

1. Certificate Management: The Certificate Authority Service is responsible for handling the creation, issuance, management, and renewal of digital certificates within ISE. These certificates are used for various authentication protocols and encryption purposes across the network. It can either act as the internal certificate authority or integrate with an external CA (for example, Microsoft AD CS, Public CAs like VeriSign or DigiCert) to issue certificates.
2. Issuing Certificates: For environments that require EAP-TLS or similar certificate-based authentication methods, ISE can issue certificates for Network Access Devices (NADs), users, or endpoints. ISE can automatically generate and deploy certificates for authenticating devices and users, or it can request certificates from an external CA.
    - Certificate Enrollment: The CA Service supports certificate enrollment for endpoints, such as laptops, phones, and other network devices, which need to authenticate to the network using certificates. ISE uses protocols such as SCEP (Simple Certificate Enrollment Protocol) or ACME (Automated Certificate Management Environment) to facilitate certificate enrollment for devices.
    - Certificate Renewal: The service automates the renewal of expiring certificates for both devices and users. It ensures certificates are always valid and up to date, preventing service interruptions caused by expired certificates.
3. Integration with External Certificate Authorities: While ISE can act as its own CA, it is more common to integrate with an external CA (for example, Microsoft Active Directory Certificate Services). The CA Service can manage the interaction between ISE and the external CA, requesting certificates for users, devices, and network resources as needed.

EST Service

Enrollment over Secure Transport (EST) Service is a protocol used to securely issue digital certificates to network devices and users in a certificate-based authentication environment. EST is a certificate enrollment protocol that allows devices to request certificates from a Certificate Authority (CA) in a secure and automated way. EST Service is useful for device authentication, such as in 802.1X environments, VPN connections, or BYOD (Bring Your Own Device) scenarios, where devices must authenticate to the network using certificates.

Key Functions of the EST Service in ISE

1. Certificate Enrollment: The EST Service is responsible for enabling secure certificate enrollment for devices (such as switches, access points, or endpoints) that require certificates for authentication. The enrollment is completed over secure transport (like HTTPS), ensuring the process is encrypted and protected from unauthorized access.
2. Certificate Revocation and Renewal: Once certificates are enrolled, the EST Service also plays a role in managing certificate revocation or renewal. For example, devices must request a new certificate when the current one expires, and EST can help automate this process.
3. Improved Network Access Control: By enabling devices to authenticate using certificates, the EST Service strengthens security posture of the network in environments using 802.1X authentication.

Verify Certificate Authority and EST Service not Running/Initializing

1. Navigate to Administration > System > Certificates > Certificate Authority > Internal CA settings. Ensure CA, EST and OCSP Responder Status is Sorted and Enabled.
2. Useful debugs that can help in troubleshooting are est, provisioning, ca-service, and ca-service-cert. Refer to ise-psc.log, catalina.out, caservice.log, and error.log files.
3. Verify ISE Root CA and ISE Messaging Certificates are valid in the deployment. If renewal of ISE Root CA is required, navigate to Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Request, select usage as ISE Root CA. Click renew ISE Root CA.

SXP Engine Service

SXP Engine Service is responsible for managing and facilitating communication between ISE and network devices using the Security Group Tag (SGT) and the Security Group Exchange Protocol (SXP). It plays a critical role in supporting TrustSec policies, which are used to enforce network access control based on the Security Group of the device rather than just IP addresses or MAC addresses. The SXP Engine in ISE is primarily used for the exchange of security group information, which helps in enforcing policies based on user or device identity, application, and location. It enables devices to share Security Group Tags (SGTs), which are used to enforce security policies across network devices, like routers and switches.

Key Functions of SXP Engine Service in ISE

1. Integration with TrustSec: SXP is commonly deployed in environments that leverage Cisco TrustSec, a solution that enforces consistent security policies across both wired and wireless networks. The SXP Engine facilitates the communication of SGTs between devices, allowing for dynamic policy enforcement based on the security context of a device or user.
2. Security Group Tags (SGTs): The core of TrustSec's policy enforcement revolves around SGTs. These tags are used to classify network traffic, and the SXP protocol helps share the mapping of these tags to specific users or devices. This allows for granular, policy-driven control over network access and traffic flow.

Verification and Troubleshooting for SXP Engine Service in ISE

1. By default, the SXP Engine Service is disabled in ISE. To enable it, go to ISE GUI > Administration > Deployment, Select the node. Check the Enable SXP Service box, and choose the interface. Then, verify the status of the SXP Engine service from the ISE CLI by running the show application status ise command.
2. If there are network communication issues, verify the interface assigned to the SXP engine has a valid IP address by running the show interface command in the CLI, and ensure the IP subnet is permitted in the network.
3. Check the RADIUS live logs to verify the SXP connection events on ISE.
4. Enable the SXP component on the ISE nodes to debug and capture relevant logs and exceptions related to SXP.

TC-NAC Service

The TC-NAC Service (TrustSec Network Access Control) is a component that facilitates the enforcement of TrustSec policies on network devices, ensuring access control is based on Security Group Tags (SGTs) rather than traditional IP or MAC addresses.

TrustSec, in turn, is a framework developed by Cisco that enables security policy enforcement across the network based on device roles, users, or contexts, rather than using legacy mechanisms like VLANs or IP addresses. It provides more granular and dynamic network access control by grouping devices into different Security Groups and tagging them with SGTs.

Key Functions of the TC-NAC Service in ISE

1. Integration with Third-Party NAC Systems: The TC-NAC Service enables ISE to communicate and interact with third-party Network Access Control solutions. This can be useful for organizations that have existing NAC infrastructure in place, but want to integrate with Cisco ISE to improve functionality, leverage additional security policies, or take advantage of other network security features of Cisco.
2. Providing Seamless Policy Enforcement: When integrated with third-party NAC solutions, ISE can

take over certain aspects of policy enforcement and decision-making. This allows for a more unified policy framework, ensuring policies applied by both Cisco and non-Cisco NAC systems are consistent across the network.
3. Support for Legacy NAC Systems: The TC-NAC Service helps organizations that have legacy NAC systems, to continue using those systems while adopting Cisco ISE for its enhanced security features. ISE can integrate with older NAC solutions and extend their lifecycle, providing access control, security, and compliance enforcement in tandem.
4. Facilitating Third-Party NAC Vendor Communication: This service allows ISE to facilitate communication with third-party NAC solutions that use proprietary protocols or standards. ISE can interact with third-party NAC systems via industry-standard protocols (like RADIUS, TACACS+, or SNMP) or customized APIs, depending on the NAC solution being used.

Verify and Troubleshoot TC-NAC Service in ISE

1. Verify Threat Centric NAC is enabled by navigating to Administration > Deployment > PSN node > Enable Threat Centric NAC.
2. If the issue is with the SourceFire FireAMP adapter, verify if port 443 is allowed in your network.
3. Verify the endpoint session details from Operations > Threat-Centric NAC Live Logs.

Alarms Triggered by Threat Centric NAC:

- Adapter Unreachable (syslog ID: 91002): Indicates the adapter cannot be reached.
- Adapter Connection Failed (syslog ID: 91018): Indicates the adapter is reachable, however, the connection between the adapter and source server is down.
- Adapter Stopped Due to Error (syslog ID: 91006): This alarm is triggered if the adapter is not in the desired state. If this alarm is displayed, check the adapter configuration and server connectivity. Refer to the adapter logs for more details.
- Adapter Error (syslog ID: 91009): Indicates the Qualys adapter cannot establish a connection with or download information from the Qualys site.

Useful debugs to troubleshoot TC-NAC issues:

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

PassiveID WMI Service

The PassiveID WMI Service is a service that allows ISE to perform device profiling using Windows

Management Instrumentation (WMI) as a passive mechanism for identifying and profiling endpoints in the network. It plays a crucial role in device profiling in environments where devices running Windows OS must be accurately identified for network access control and policy enforcement.

Key Functions of the PassiveID WMI service in ISE

1. Device Identity Collection: The PassiveID WMI service allows ISE to passively collect identity information from Windows devices using Windows Management Instrumentation (WMI). It gathers system details such as the hostname of the device, OS version, and other relevant attributes without requiring the device to actively participate.

2. Integration with ISE Policy: The information gathered by the PassiveID WMI service is integrated into the ISE policy framework. It helps in the dynamic application of policies based on device attributes such as type, OS, and compliance with security standards.

Verify and Troubleshoot PassiveID WMI Service

A highly secure and precise source, and most common to receive user information. As a probe, AD works with WMI technology to deliver authenticated user identities. In addition, AD itself, rather than the probe, functions as a source system (a provider), from which other probes retrieve user data as well.

Useful debugs and information required for troubleshooting purposes. Set these attributes to debug level for PassiveID WMI issues:

- PassiveID (passiveid*)
- runtime-logging (prrt-server.log)
- Active Directory (ad)_agent.log) - Trace level
- collector (collector.log) (on PassiveID,MnT nodes and on active pxGrid node if sessions are published)
- pxGrid (pxgrid/) (on secondary MnT and active pxGrid node if the sessions are published)

Information required for troubleshooting PassiveID WMI:

1. Was it working before? Any changes done recently (such as any upgrades, patch installs on ISE/upgrades on DC?)
2. Does the test connection work properly (before the integration, check the test connection?)
3. Details on the username used to Join AD and username used for WMI (whether the admin or non admin account.)
4. Check whether the events (4768, 4770) in DC is logged (check the event viewer log from DC.)
5. Capture logs: Set debug level for passive ID and runtime-logging, then complete configuration for wmi for DC, AD with trace level with timestamp.

PassiveID Syslog Service

The PassiveID Syslog Service is a service that enables the PassiveID profiling feature to collect and process syslog messages from network devices in the environment. These syslog messages contain important information on the endpoints connected to the network, and ISE uses these to profile devices for network access control and policy enforcement.

Key Functions of the Passive ID Syslog Service

1. Passive Authentication: The Passive ID Syslog service allows Cisco ISE to authenticate users and devices passively by collecting syslog messages from network devices (like switches or routers) that indicate user and device activity. This is useful in situations where traditional active methods of authentication, like 802.1X, is not suitable or feasible.

2. Event Logging: The Passive ID Syslog service relies on the syslog protocol to receive logs from network devices that track user access and behavior on the network. The information contained in these logs can include things like device log in attempts, access points, and interface details, which help ISE passively identify the device or user.

PassiveID API Service

The PassiveID API Service is a service that enables integrations with systems that require information about the identity of devices or users that are connected to the network. It is typically used in environments where network administrators want to perform identity-based policies and actions without requiring active network authentication protocols like 802.1X for every device.

Key Functions of the Passive ID API Service

1. Integration with External Systems: The Passive ID API allows ISE to receive identity information from third-party systems or network devices (such as switches, routers, firewalls, or any system that can generate identity-related events.) These external systems can send information like syslog messages, authentication logs, or other relevant data that can help ISE passively identify a user or device.
2. Passive Authentication: The Passive ID API service is used to authenticate users and devices passively by gathering identity data without requiring active authentication (for example, no need for 802.1X, MAB, or web authentication.) It can capture information from network devices, Active Directory logs, or security appliances and use it to identify the user or device.
3. Mapping Identity Information: The Passive ID API can be used to map identity data to specific security policies. This information is used to dynamically assign Security Group Tags (SGTs) or roles to users and devices, which then influences the enforcement of network access controls (like segmentation and firewall policies).

PassiveID Agent Service

The PassiveID Agent Service enables device profiling through the use of PassiveID Agents installed on endpoints (such as computers, laptops, mobile devices and so on). The PassiveID Agent allows ISE to gather profiling information about devices on the network by listening to traffic from endpoints, without requiring active scans or direct interactions with the devices.

Key Functions of the Passive ID Agent Service

1. Passive User and Device Identification: The Passive ID Agent Service is responsible for gathering identity-related information passively, typically from network devices or endpoints, and sending this data to ISE. This service allows ISE to authenticate and identify users and devices based on their activities or characteristics, without needing active authentication from the device (for example, without 802.1X credentials being provided.)
2. Integration with Other Cisco Components: The Passive ID Agent works closely with Cisco network devices, like switches, wireless controllers, and access points to gather identity-related information from network traffic, syslog logs, or other management systems. It can also integrate with Cisco TrustSec and Cisco Identity Services to map this data to specific Security Group Tags (SGTs) or other identity-based policies.
3. Contextual Network Access Control: The Passive ID Agent sends this information to Cisco ISE, which applies the appropriate access control policies based on the identity and context of the user or device. This can include:

- Role-based access control
- Dynamic VLAN assignment
- Network segmentation
- Enforcing security policies based on the user role or device security posture

---

PassiveID Endpoint Service

The PassiveID Endpoint Service is a service that is responsible for the identification and profiling of endpoints (devices) on the network based on PassiveID technology. This service helps ISE collect, process, and classify information on devices connecting to the network, without requiring active interaction with the endpoints themselves. The PassiveID Endpoint Service plays a critical role in profiling, network access control, and security policy enforcement.

Key Functions of the PassiveID Endpoint Service

1. Passive User and Device Identification: The PassiveID Endpoint Service permits ISE to identify and authenticate devices on the network passively, by leveraging information from network activity or system logs. This includes identifying users and devices based on their network behavior or characteristics, such as MAC address, IP address, or log in information from an external identity store like Active Directory (AD).

2. Data Collection from Endpoints: The Endpoint Service collects various types of endpoint-specific data from different sources:

- User log in information from external identity stores like Active Directory or other directories.
- Device characteristics such as IP addresses, MAC addresses, and device type (for example, whether the device is a Windows PC, mobile phone, or IoT device.)
- Endpoint network activity such as DHCP requests, ARP requests, and other network-layer communications.

PassiveID SPAN Service

The PassiveID SPAN Service leverages SPAN (Switched Port Analyzer) port mirroring on network devices to capture and analyze network traffic for endpoint profiling. This service helps ISE passively obtain information on endpoints within the network by analyzing network communication patterns without requiring active probes or agents installed on devices.

Key Functions of the PassiveID SPAN Service

1. Passive Identity Collection from SPAN Traffic: The PassiveID SPAN Service allows ISE to collect identity data based on network traffic that is mirrored or copied through a SPAN port on a switch. A SPAN port is used for network monitoring by mirroring network traffic from other ports or VLANs. By capturing this traffic, ISE can passively gather identity information such as:

- MAC addresses of devices
- IP addresses associated with devices
- DHCP requests or other identity-related information from captured traffic
- Authentication logs from network devices, such as switches or wireless controllers

2. Capture of User and Device Identity Information: The SPAN Service listens to the traffic that passes through the network and identifies key identity information from the network packets without the need to interact directly with devices. This can include data such as:

- User identities when authenticating via protocols like EAP (Extensible Authentication Protocol)
- Device identities based on MAC addresses and IP addresses
- Device roles and behaviors based on observed traffic patterns and events

---

Verification and Troubleshooting for PassiveID Stack (PassiveID SPAN Service, PassiveID Syslog Service, PassiveID Endpoint Service, PassiveID Agent, PassiveID API Service)

1. PassiveID stack is a list of providers and all services and the PassiveID stack is disabled by default. Navigate to ISE GUI > Administration > Deployment > Select the node > Enable Passive Identity Service, click Save. To verify the PassiveID stack service status, log in to the CLI of the ISE node and

run the show application status ise command.
2. If there are issues with the Passive ID Agent, check if the FQDN of the agent is resolvable from the ISE node. To perform this, log in to the ISE CLI and run nslookup < FQDN of Agent configured > command.
3. Ensure the ISE Indexing engine is active and both reverse and forward DNS lookups are being resolved by the DNS or name server configured in ISE.
4. To ensure seamless communication with the syslog providers, ensure UDP port 40514 and TCP port 11468 are open in your network.
5. To configure the SPAN Provider on a node, ensure the ISE Passive Identity Service is enabled. Verify the interface you want to configure on the SPAN provider is available in ISE by running the show interface command from ISE CLI.
6. To check the logs, based on the Passive ID provider, you must review the passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log. The mentioned logs can be secured from the support bundle of ISE node.

DHCP Server (dhcpd)

The DHCP Server (dhcpd) Service provides Dynamic Host Configuration Protocol (DHCP) functionality to network devices. It is primarily used to assign IP addresses to devices (endpoints) trying to connect to the network. In ISE, the DHCP server plays a crucial role in providing IP addresses to endpoints that request them when connecting to the network. The service can also provide additional configuration information, such as DNS servers, default gateway, and other network settings.

Key Functions of the DHCP Server (dhcpd) Service in ISE

1. Dynamic IP Address Allocation: The dhcpd service in ISE functions as a DHCP server, which provides IP address allocation for devices that request an IP address when connecting to the network. This is important in scenarios where devices join the network dynamically, such as in BYOD (Bring Your Own Device) environments or when devices are configured to obtain IP addresses automatically.
2. Profile-Based DHCP: The dhcpd service can allocate IP addresses based on the profile of the device. If ISE has profiled the device (smartphone, laptop, IoT device), it can assign an appropriate IP address or apply other settings based on the type of device or role.
3. Support for DHCP Relay: ISE can function as a DHCP relay agent, forwarding DHCP requests from devices to an external DHCP server if ISE is not handling the actual IP address assignment. In this case, the dhcpd service can forward requests from devices to a central DHCP server, while ISE continues to apply network policies and access controls.

Verify and Troubleshoot DHCP Server (dhcpd)

1. Contact Cisco TAC to verify if the DHCP server package is installed on the ISE.
2. Log in to the root of ISE > rpm -qi dhcp.

DNS Server (Named)

The DNS Server (named) Service allows ISE to function as a DNS (Domain Name System) server or DNS resolver. It is primarily responsible for resolving domain names into IP addresses and vice versa, facilitating the communication between devices in the network.

Key Functions of the DNS Server (Named) Service in ISE

1. DNS Resolution for ISE Communication: The named service in ISE helps to resolve domain names to IP addresses. This is important when ISE must connect to other network devices or external services (such as Radius servers, Active Directory, or external NTP servers) using domain names rather than IP addresses.

- When ISE must reach a Radius server or an external directory service (like Active Directory), it must resolve the domain name of that server to an IP address.
- ISE queries the DNS server configured on the system to resolve these domain names, ensuring smooth communication.

2. DNS Resolution for External Services: The DNS service enables ISE to connect to external services that require domain names. For instance, ISE must resolve the names of external services like:

- Cloud-based services.
- NTP (Network Time Protocol) servers.
- Certificate Authorities (CAs) or LDAP servers.

3. Multi-Domain and Redundant DNS Servers: ISE can be configured to use multiple DNS servers for redundancy. If one DNS server becomes unavailable, ISE can fall back on another DNS server to ensure continuous operation and DNS resolution.

Verify and Troubleshoot for DNS Server (Named)

1. From CLI of the ISE node, verify the reachability to the named server or DNS server of the deployment by running the ping <IP of DNS server / name server> command.
2. Verify the DNS resolvance of ISE FQDNs by running the nslookup <FQDN / IP address of ISE nodes> command via ISE CLI.

ISE Messaging Service

The ISE Messaging Service is a component that facilitates asynchronous communication between various services and components within the ISE system. It plays a crucial role in the overall system architecture of

ISE, enabling different parts of the platform to send and receive messages, manage tasks, and synchronize activities.

Key Functions of the ISE Messaging Service

1. Inter-Process Communication (IPC): The ISE Messaging Service enables inter-process communication (IPC) between various ISE services. It ensures different ISE modules and services, such as authentication, authorization, and policy enforcement, can exchange data and instructions in a coordinated manner.
2. Distributed Environment Support: In larger or distributed ISE deployments (such as in multi-node or high-availability configurations), the Messaging Service helps facilitate communication between the various ISE nodes. This ensures that data, such as authentication requests, user sessions, and policy updates, are correctly synchronized across different nodes within the ISE system.
3. Policy and Configuration Sync: The Messaging Service is involved in synchronizing configurations and policies between ISE nodes. When configuration changes are made to a primary node, the service ensures these changes are propagated to secondary or backup nodes in the system. This is essential in maintaining consistency and ensuring that the network access policies applied across different locations or distributed ISE nodes remain synchronized.

Verify the ISE Messaging Service is not Running or Initializing

1. Verify port TCP 8671 is not blocked in the firewall, this port is used for Inter-node communication between ISE devices.
2. Verify any queue link errors and if any are found, renew the ISE Messaging and ISE Root CA certificates. Queue link errors can occur due to internal certificate corruption issues. To resolve queue link errors, renew the ISE Message and ISE Root CA certificates by referring to the ISE - Queue Link Error documentation.
3. From GUI > Administration > Certificates > Select ISE Messaging Certificate. Click View to validate the status of the certificate.
4. You can use ade.Jog logs to troubleshoot ISE Messaging Services, which is available in the support bundle or can be tailed via CLI by running the show logging system ade/ADE.Jog tail command when the issue arises.
5. If the ADE.Jog log shows rabbitmq: connection refused errors, contact Cisco TAC to remove the lock from the Rabbitmq module from ISE Root.

ISE API Gateway Database Service

The ISE API Gateway Database Service is a component responsible for managing and processing data related to API requests and responses within the ISE system. It acts as an intermediary that connects the ISE API Gateway with the ISE database, ensuring custom applications updates or modifies data within ISE. For example, adjusting access policies or adding/removing users through API calls managed by the service.

Key Functions of the ISE API Gateway Database Service

1. API Access to ISE Data: The ISE API Gateway Database Service acts as a bridge allowing external applications to interact with the ISE database via ISEs RESTful APIs. These APIs can be used to retrieve or modify data stored in the ISE database, such as:

- User authentication logs
- Network access policies
- Device profiling information
- System configuration and settings

2. Enabling External System Integrations: This service plays a crucial role in integrating ISE with external systems like:

- External authentication servers (LDAP, Active Directory, RADIUS)
- Network Management Systems (NMS)
- Security Information and Event Management (SIEM) solutions
- Custom applications or services that must interact with ISE data

By providing API access, the API Gateway Database Service allows these external systems to query ISE data, send updates to ISE, or trigger specific actions within ISE in response to external events.

3. Supporting RESTful API Communication: ISE exposes RESTful APIs designed to work over HTTP/HTTPS. The API Gateway Database Service is responsible for managing the flow of API requests and responses, ensuring requests are authenticated, processed, and appropriate data from the ISE database is returned in response.

ISE API Gateway Service

The ISE API Gateway Service is a critical component that provides RESTful API access to ISE services, data, and functionalities. It acts as a bridge between ISE and external systems, allowing these systems to interact programmatically with ISE network access control, policy enforcement, authentication, and other services. The API Gateway enables third-party applications, network management systems, and custom applications to interact with Cisco ISE without manual intervention or direct access to the ISE user interface.

Key Functions of the ISE API Gateway Service

1. Enabling API Access to ISE: The ISE API Gateway Service enables external systems to securely access and interact with Cisco ISE data and policies using RESTful APIs. This provides programmatic access to ISE functionalities, such as authentication, policy enforcement, session management, and more.
2. Providing Programmatic Control: The API Gateway Service allows for programmatic control over ISE functions. Administrators and developers can use APIs to:

- Retrieve or modify network policies
- Query or manage user sessions and authentication logs
- Create and manage network access control rules
- Access or update device profiles
- This control can be leveraged for automation or custom workflow orchestration, such as dynamically adjusting network access policies based on real-time data or integrating ISE into a broader security automation platform.

3. Monitoring and Reporting: The API Gateway Service allows external systems to collect data from operational ISE logs, session history, and policy enforcement details. This is important for:

- Compliance reporting
- Security monitoring
- Incident response

API calls can be used to pull logs, audit information, and events; allowing security teams to monitor ISE activities from a centralized dashboard or reporting tool.

Verify and Troubleshoot ISE API Gateway Service and ISE API Gateway Database Service

1. Verify if the Admin Certificate of the ISE node is active and valid. Navigate to Administration > Certificates > Select the node > Select Admin Certificate. Click View to verify the status of the Admin Certificate of the ISE node.
2. Set ise-api-gateway, api-gateway, apiservice components to debug and the logs can be tailed by running these commands:

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

ISE pxGrid Direct Service

The ISE pxGrid Direct Service is a critical component that supports pxGrid (Platform Exchange Grid) functionality in ISE. pxGrid is a Cisco technology that facilitates secure, standardized, and scalable data sharing and integration between Cisco network security solutions and third-party applications, services, and devices. The ISE pxGrid Direct Service enables direct communication between ISE and other pxGrid-compatible systems without requiring intermediary devices or services.

Key Functions of ISE pxGrid Direct Service

1. Direct Integration with Third-Party Systems: The ISE pxGrid Direct Service allows ISE to integrate directly with third-party network security systems, such as firewalls, routers, NAC solutions, SIEM platforms, and other security appliances. It allows these systems to exchange information regarding

network access events, security incidents, and contextual network data.
2. Context Sharing: One of the primary functions of pxGrid is the sharing of contextual information (such as device identities, user roles, security posture, and network access information.) With pxGrid Direct Service, ISE can directly share context with other devices or applications without relying on traditional methods such as RADIUS or TACACS+.
3. Simplified Communication: By using pxGrid, ISE can communicate and exchange information with third-party solutions using a standardized protocol. This simplifies the integration process as systems do not need custom integrations for each individual third-party solution.
4. Enhanced Security and Compliance: The pxGrid Direct Service improves security posture and compliance by ensuring all systems in the network ecosystem have access to real-time, contextual data on users, devices, and security policies. This provides a coordinated enforcement of network security policies across the entire environment.

Verify and Troubleshoot ISEPxgrid Direct Service

1. Contact Cisco TAC to verify if edda*.lock* is present in the /tmp folder. If yes, Cisco TAC can remove the lock and restart the Pxgrid Direct service from root.
2. Set the PxGrid Direct component to debug in the ISE node for troubleshooting. The logs can be secured via ISE support bundle or ISE CLI by running these commands:

- show logging application pxgriddirect-service.log
- show logging application pxgriddirect-connector.log
- These logs provide information on the endpoint data fetched and received by Cisco ISE along with the connectivity status of Pxgrid Connector.

Segmentation Policy Service

The Segmentation Policy Service is a key component responsible for enforcing network segmentation policies based on user identity, device posture, or other information. It helps control the access of users/devices to specific network segments, ensuring only authorized users or compliant devices can access certain parts of the network. Network segmentation is essential for reducing surface attacks of the network, preventing lateral movement of threats, and ensuring regulatory compliance. The Segmentation Policy Service in ISE is used to enforce these network segmentation rules dynamically and provides flexibly across the network.

Key Functions of the Segmentation Policy Service

1. Defining Network Segments: The Segmentation Policy Service in ISE allows administrators to define various network segments (subnets or VLANs) based on the characteristics of users or devices. For example:

- Devices with different security postures can be assigned to different segments (trusted devices in one VLAN and untrusted devices in another.)

- Users from different departments or roles can be assigned to different network segments to enforce least privilege and restrict access to sensitive resources.

2. Dynamic Segmentation: This service enables dynamic network segmentation, which allows network segments or VLANs to change based on real-time conditions. For example:

- A user can be assigned to a specific VLAN based on their role or device health status.
- A device that is deemed non-compliant or is running an outdated operating system can be moved to a quarantine or guest VLAN until it is remediated.

3. Policy-Based Enforcement: The Segmentation Policy Service uses policies to decide which segment a device or user must be placed into. There are various factors these policies take into account, such as:

- User Identity: Based on the user role or attributes.
- Device Posture: The health of compliance status of the device (is the device running the latest antivirus software).
- Location: The physical location of the user or device on the network (office, guest area, remote access).
- TIme of Access: Time of day, day or the week when the request for access is made.

4. Enforcement of Security Policies: The Segmentation Policy ensure security policies are consistently enforced across network devices (such as switches, routers, firewalls, and so on) by leveraging industry standards like RADIUS and VLAN assignment. This allows Cisco ISE to communicate with network infrastructure devices to enforce required segmentation policies.

Verify and Troubleshoot Segmentation Policy Service

1. Verify if the segmentation is properly configured by navigating to Work Centres > TrustSec > Overview > Dashboard.
2. Then go to, Work Centres > TrustSec > Reports and select TrustSec Reports to verify the segmentation policy service status and reports.

REST Auth Service

The REST Auth Service provides authentication capabilities using RESTful APIs. It enables external applications and systems to authenticate users or devices by interacting with ISE over HTTP(S) using standard REST protocols. This service allows for seamless integration of Cisco ISE authentication functionality with third-party applications or systems that must authenticate users or devices but cannot use the traditional methods (like RADIUS or TACACS+).

Key Functions of the REST Auth Service

1. RESTful Authentication: The REST Auth Service enables authentication requests over the REST API protocol. This allows external systems (applications, third-party network devices, or services) to authenticate users or devices using ISE as the authentication server, but through RESTful web service calls rather than traditional authentication protocols like RADIUS or TACACS+.
2. Integration with External Applications: This service is designed for external applications that must authenticate users or devices but do not use traditional authentication methods (like RADIUS or TACACS+). Instead, they can interact with ISE via REST APIs, which is simpler to integrate ISE authentication into web-based or cloud-native applications.
3. Flexible and Scalable Authentication: The REST Auth Service provides a scalable method of authentication that is not limited to network devices or on-premise solutions. It can be used by cloud services, mobile apps, and other web-based platforms that must authenticate users/devices by querying ISE for credentials and policies.
4. Easy to Apply: The REST API offers a standardized interface, which is easier to apply and integrate with modern software and applications compared to traditional methods. It provides JSON formatted responses and uses HTTP methods like GET, POST, PUT, and DELETE, which is more accessible for web developers and systems integrating ISE for authentication.

Verification and Troubleshooting for Rest Auth

1. To troubleshoot Open API-related issues, set the apiservice component to debug.
2. To troubleshoot ERS API related issues, set the ers component to debug.
3. If the API service GUI page: https://{iseip}:{port}/api/swagger-ui/index.html or https://{iseip}:9060/ers/sdk is accessible, it concludes that API service is working as expected.

Refer to the API Documentation for more information on Cisco APIs.

SSE Connector

The SSE Connector (Secure Software-Defined Edge Connector) integrates ISE with the Cisco Secure Software-Defined Access (SD-Access) solution. The SSE Connector allows ISE to securely communicate with the Cisco DNA Center, enabling automated network policies, segmentation, and edge security management in an SD-Access environment.

Key Functions of the SSE Connector

1. Integration with Third-Party Security Systems: The SSE Connector facilitates the integration of Cisco ISE with third-party security systems like firewalls, Intrusion Prevention Systems (IPS), Network Access Control (NAC) solutions, and Security Information and Event Management (SIEM) systems. It allows these external systems to send/receive data from ISE in a secure manner, which can be used for more dynamic policy enforcement.
2. Real-Time Threat Intelligence: By connecting ISE with other security systems, the SSE Connector enables the exchange of real-time threat intelligence. This information can include suspicious activity, compromised endpoints, or malicious behaviors detected by other security systems, allowing ISE to

dynamically adjust access policies based on current threat levels or device status.
3. Automated Remediation: The integration enabled by the SSE Connector can support automated remediation workflows. For example, if a system is flagged as compromised by an external security appliance, ISE can automatically enforce policies that block network access or redirect the endpoint to a remediation network segment for further investigation.

Verify and Troubleshoot SSE Connector

1. The SSE connector is enabled only when the PassiveID service is enabled in ISE.
2. The sse-connector (connector.log) component in debug provides more information on SSE Connector related messages.

Hermes (pxGrid Cloud Agent)

Hermes (pxGrid Cloud Agent) facilitates the integration between ISE and the pxGrid (Platform Exchange Grid) ecosystem in a cloud environment. Hermes is the cloud-based agent used to enable communication between ISE and cloud-based services or platforms. It supports the pxGrid framework in sharing contextual information across different network and security systems.

Key Features and Functions of Hermes (pxGrid Cloud Agent)

1. Cloud-to-On-Premises Integration: Hermes (pxGrid Cloud Agent) is designed for seamless integrations between cloud-based services and on-premises ISE infrastructure. It extends the power of pxGrid beyond traditional on-prem network environments, enabling secure data exchange and policy enforcement across cloud-based applications and services.
2. pxGrid Ecosystem Support: pxGrid is a Cisco platform for securely sharing information across network security solutions. Hermes acts as the cloud agent for pxGrid, enabling secure, real-time communication between ISE and various cloud-based services. This integration allows consistent network security policies across both on-prem and cloud environments for easy management and to enforce security.
3. Cloud-Based Endpoint Visibility: One core advantage of Hermes is the visibility into cloud-based endpoints, similar to how ISE provides visibility with on-prem endpoints. It can gather data on devices and users in the cloud, such as compliance posture, security status, and identity information. This allows ISE to enforce network access policies on cloud endpoints like on-premises devices.
4. Seamless Extension of ISE to Cloud Environments: One key benefit of Hermes is it provides a seamless bridge between the ISE on-premises environment and the growing number of cloud-native applications. This is easier to extend ISE security policies, authentication methods, and access controls to cloud services without requiring a complete overhaul of existing infrastructure.

Verifiy and Troubleshoot Hermes (Pxgrid Cloud Agent)

1. By default, Hermes service is disabled, connecting ISE with the Cisco PxGrid as the cloud service is

enabled with Hermes. If the Hermes service is disabled in ISE, verify if the Pxgrid Cloud option is enabled from ISE GUI > Administration > Deployment, Select ISE node. Click Edit, and Enable Pxgrid Cloud.

2. Useful debugs for troubleshooting issues related to the Pxgrid cloud are hermes.log and the pxcloud.log. These debugs are available only on the Pxgrid node where the Pxgrid Cloud is enabled.

McTrust (Meraki Sync Service)

McTrust (Meraki Sync Service) enables integration between Cisco ISE and Cisco Meraki systems for syncing and managing network devices and access policies. The McTrust service acts as a connector that synchronizes user and device information between Meraki's cloud-managed network infrastructure and ISE on-premises identity and policy management systems.

Key Features and Functions of McTrust (Meraki Sync Service)

1. Seamless Integration with Meraki Devices: McTrust enables ISE to synchronize and integrate with Meraki's cloud-managed devices. This includes devices such as Meraki access points, switches, and security appliances that are part of Meraki's portfolio. It allows ISE to communicate directly with Meraki's infrastructure, making it easier to apply network access control policies to Meraki-managed devices.
2. Automated Device Synchronization: The Meraki Sync Service automatically synchronizes ISE policies with Meraki network devices. Any changes on the network access control policies in ISE are automatically reflected in Meraki devices, without requiring manual intervention. This allows administrators easy management network access across both Meraki and ISE platforms.
3. Policy Enforcement for Meraki-Managed Devices: McTrust allows ISE to enforce network access policies on Meraki devices based on authentication and device posture. It dynamically assigns policies to Meraki network elements, such as adjusting VLAN assignments, applying Access Control Lists (ACLs), or restricting access to certain network resources, depending on the security posture of the device or user requesting access.
4. Meraki Dashboard Integration: McTrust integrates ISE directly with the Meraki Dashboard, providing a unified management interface. With this integration, administrators can view and manage network policies and access control rules for both Meraki devices and ISE-managed resources, all within the Meraki cloud-managed interface.

Verify and Troubleshoot McTrust (Meraki Sync Service)

1. Log into ISE GUI > Work Centers > TrustSec > Integrations > Sync Status. Verify any issues/errors found.
2. Ensure all admin certificates with ISE nodes are active & valid.
3. Useful troubleshooting for debugs with the Meraki Sync Service is meraki-connector.log.

ISE Node Exporter

The ISE Node Exporter is a component used for monitoring and collecting performance metrics with the ISE system, from the ISE nodes (whether they are administration nodes, monitoring nodes, or policy service nodes.)

Key Features and Functions of ISE Node Exporter

1. Metrics Export: The ISE Node Exporter provides a variety of performance-related metrics, such as CPU usage, Memory usage, Disk utilization, Network statistics, System load, and Other operating system-level metrics. These metrics are used for monitoring the health and performance of the ISE node and can be visualized in a monitoring dashboard like Grafana.
2. System Health Monitoring: By exporting the performance data to Prometheus, the ISE Node Exporter allows for continuous monitoring of the health and operational status of the ISE node. Administrators can create alerts based on predefined thresholds to notify of performance degradation or system issues.
3. Prometheus Integration: The ISE Node Exporter is typically used in conjunction with Prometheus, an open-source monitoring and alerting toolkit designed for reliability and scalability. The Node Exporter exposes system-level metrics that can be scraped by Prometheus to collect and store time-series data.

ISE Prometheus Service

The ISE Prometheus Service integrates Prometheus with ISE to enable monitoring and collects performance metrics from ISE. Prometheus is an open-source monitoring and alerting toolkit used to collect, store, and analyze time-series data, and the ISE Prometheus Service allows ISE to expose its internal metrics to Prometheus for monitoring purposes.

Key Features and Functions of ISE Prometheus Service

1. Metrics Collection for Monitoring: The ISE Prometheus Service is designed to export various operational and performance metrics related to ISE. These metrics typically include, but are not limited to CPU utilization and system load, Memory usage, Disk usage and I/O performance, Network statistics, Authentication request statistics, Policy enforcement statistic, System health and uptime data
2. Prometheus Integration: Prometheus allows ISE to expose data in a format that is compatible with Prometheus, which scrapes data at regular intervals. Prometheus stores data in a time-series database, which tracks trends and historical performance of the ISE system.
3. Visualization and Reporting with Grafana: The Prometheus Service in ISE integrates seamlessly with Grafana, a popular open-source visualization tool. After exporting the metrics to Prometheus, administrators can use Grafana dashboards to visualize the data in real-time. This enables easy identification of performance bottlenecks, system trends, and potential issues in the ISE deployment.

ISE Grafana Service

ISE Grafana provides system performance metrics and is an open-source platform for monitoring and data visualization. It integrates with Prometheus to display real-time and historical data collected from ISE, allowing admins to create interactive dashboards that provide insights into the health, performance, and usage of the ISE system.

Key Features and Functions of ISE Grafana Service

1. Customizable Dashboards: Grafana is highly customizable, allowing admins to create and modify dashboards based on their monitoring needs. Custom queries can be created to extract specific data points from Prometheus, and those queries can be visualized in various formats like graphs, tables, heatmaps, and more.
2. Centralized Monitoring for Distributed ISE Deployments: For distributed ISE deployments where multiple ISE nodes are deployed across different locations, Grafana provides a centralized view of all system metrics collected from each node. This allows admins to monitor the performance of the entire ISE deployment from a single location.
3. Historical Data and Trend Analysis: With the data stored in Prometheus, Grafana enables historical analysis of system metrics, allowing admins to track trends over time. For example, admins can monitor how CPU usage has changed over the past month or how authentication success rates have fluctuated. This historical data is valuable for capacity planning, trend analysis, and identifying long-term issues.

Verify and Troubleshoot ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter

- ISE Grafana Service, ISE Prometheus Service, and ISE Node Exporter service work together and are called Grafana Stack Services. There are no specific debugs to enable troubleshooting for these services. However, these commands help in troubleshooting.

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



Note: When Monitoring is enabled, ISE Node Exporter, ISE Prometheus Service, and ISE Grafana Service must be running as any disruption of these services cause issues during data collection.

ISE MNT LogAnalytics Elasticsearch

The ISE MNT LogAnalytics Elasticsearch is a component that integrates Elasticsearch with ISE Monitoring and Troubleshooting (MNT) capabilities. It is used for log aggregation, search, and analytics related to ISE

logs and events. Elasticsearch is a widely-used, distributed search and analytics engine, and when integrated with ISE, it enhances the system to store, analyze, and visualize log data generated by ISE components.

Key Features and Functions of ISE MNT LogAnalytics Elasticsearch

1. Log Storage and Indexing: The Elasticsearch service in ISE is responsible for storing and indexing the log data generated by ISE. Elasticsearch is a distributed search and analytics engine. It allows ISE logs to be stored that enables fast searching, querying, and retrieving specific events, errors, or system activities.
2. Integration with Log Analytics: ISE MNT LogAnalytics Elasticsearch works in conjunction with Log Analytics to provide a comprehensive logging solution. It enables ISE to collect log data related to authentication, policy enforcement, system operations, and other activities. This data is stored in Elasticsearch, which provides detailed analysis and insights into ISE behavior.
3. Centralized Logging: By integrating with Elasticsearch, ISE provides a centralized logging solution, which is critical for environments that require distributed log collection. This allows admins to view and analyze logs from multiple ISE nodes in a single, unified interface, for easy troubleshooting and monitoring of ISE performance.
4. Log Analysis and Troubleshooting: The ISE MNT LogAnalytics Elasticsearch service helps admins analyze system behavior and troubleshoot issues for easy access to logging data. If there is a sudden spike in authentication failures or an unexpected system outage, Elasticsearch allows for quick querying of log data to identify the root cause.

Verify and Troubleshoot ISE M&T LogAnalytics Elasticsearch

1. Disabling and re-enabling of log analytics service in ISE must help. Navigate to Operations > System 360 > Settings > Log analytics (disable and enable by using the toggle option.)
2. Restart the M&T LogAnalytics from ISE Root resolves this issue. Contact Cisco TAC to complete this action.

Known defects: Cisco bug ID ·66198

ISE Logstash Service

The ISE Logstash Service integrates Logstash, an open-source data processing pipeline with ISE to collect, transform, and forward logs. It processes ISE logs into a structured format and sends them to centralized logging systems for analysis, storage, and monitoring.

Key Features and Functions of the ISE Logstash Service

1. Log Collection and Forwarding: ISE Logstash Service collects log data from various ISE components (such as authentication logs, system logs, policy enforcement logs and so on) and forwards to a central

location (typically Elasticsearch or another log management system) for storage and analysis.
2. Log Parsing: Logstash can parse collected logs into structured formats. It processes raw log data and extracts meaningful information, transforming log entries into a format easier to query and analyze. This can involve filtering, parsing, and enriching data before forwarding to Elasticsearch or other systems.

Verify and Troubleshoot ISE Logstash Service

1. No specific debugs to enable. However, running the show logging application ise-logstash/logstash.log command provides insight on the status of the service.
2. Disabling and re-enabling the log analytics service in ISE can help. Navigate to Operations > System 360 > Settings > Log Analytics (disable and reenable by using the toggle option).

Known defects related to Logstash:

- Cisco bug ID ·74832
- Cisco bug ID ·58596

ISE Kibana Service

ISE Kibana Service is an open-source data visualization tool with ISE logging and monitoring. Kibana works in tandem with Elasticsearch, which stores and indexes log data and is a powerful platform for visualizing, searching, and analyzing ISE logs and performance metrics.

Key Features and Functions of the ISE Kibana Service

1. Data Visualization: ISE Kibana allows admins to create visual representations of llog data collected from ISE. This can include:

- Charts, graphs, and tables for trends in authentication, policy enforcement, user activity, and system health.
- Pie charts, line graphs, and bar charts to track specific metrics such as the number of failed log in, session duration, or errors over time.

Verify and Troubleshoot ISE Kibana Service

1. If the ISE Kibana Service is not running, disable and reenable the log analytics in ISE. Then, navigate to Operations > System 360 > Settings, Log Analytics (disable and reenable by using toggle option.)
2. In many scenarios, there can be a duplicate entry in /etc/hosts folder, which can be causing an issue.

Contact TAC to remove the duplicate entry.

Known defects related to the Kibana issue:

- Cisco bug ID ·78050
- Cisco bug ID ·59848



Note: When Log Analytics is enabled, ISE MNT LogAnalytics Elasticsearch, ISE Logstash Service, and the ISE Kibana Service must be running as any disruption of these services create issues during data collection.

ISE Native IPSec Service

The ISE Native IPSec Service refers to the built-in support for IPSec (Internet Protocol Security), which provides secure communication between ISE nodes or between ISE and other network devices. IPSec is a suite of protocols used to secure network communications by authenticating and encrypting each IP packet in a communication session. The Native IPSec Service is part of the broader security and network access management framework. It provides capabilities to handle and manage IPsec VPN connections, ensuring the data transmitted between the ISE system and remote endpoints is secure. This can involve interactions with client devices, network access devices (such as routers or firewalls), or other ISE nodes, where IPsec encryption and tunneling are necessary for securing sensitive information.

Key Features and Functions of ISE Native IPSec Service

1. Secure Communication via IPsec: The main function of the ISE Native IPSec Service is to maintain and secure communication channels using IPSec. This involves using encryption and authentication mechanisms to ensure data transmits between ISE and other devices to protect from interception, tampering, and unauthorized access.
2. IPSec VPN Connectivity: The ISE Native IPSec Service helps facilitate VPN connections that use the IPSec protocol to provide a secure, encrypted tunnel for data transmission. This is useful for remote workers, branch offices, or other locations to securely access ISE environments over untrusted networks like traditional internet access.
3. Support for Remote Access VPN: The Native IPSec Service can be involved in remote access VPN configurations, where users or devices located offsite (such as remote employees or branch offices) securely connect to the ISE system via IPsec tunnels. This service ensures all remote access traffic is encrypted and authenticated before reaching the ISE environment.
4. IPsec VPN Client Compatibility: ISE Native IPSec Service ensures compatibility with IPsec VPN clients. It supports common client configurations, enabling devices to securely connect to the network without exposing sensitive data to risks.

Verify and Troubleshoot Native IPSec Service

1. There are no specific debugs to enable for the Native IPSec Service. Verify the logs running the show

logging application strongswan/charon.log tail command via ISE CLI.
2. If any issue is observed for tunnel, verify the status of the tunnel establishment via GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec.

MFC Profiler

The MFC Profiler is a specialized component used for profiling network devices and endpoints. Profiling is a key part of network access control, as it allows ISE to identify devices on the network, classify them, and apply appropriate network policies based on the type of device and behavior.

Key Features and Functions of the MFC Profiler Service in ISE

1. Traffic Profiling: The MFC Profiler service in ISE collects and profiles traffic data. It monitors how endpoints behave on the network, including the types of applications used, the services accessed, and the traffic patterns exhibited by devices. This data helps build a profile for each endpoint.
2. Endpoint Profiling: The MFC Profiler service allows ISE to identify and categorize endpoints based on their behavior. It detects if an endpoint is a printer, computer, or mobile device based on traffic patterns. This can help enforce specific policies for different types of devices, improving security, and operational efficiency.

Verifiy and Troubleshoot MFC Profiler Service

1. Navigate to ISE GUI > Administration > Profiling > MFC Profiling and AI Rules. Verify if the service is enabled.
2. If the service is enabled, but showing as disabled/not running via show application status ise command in ISE CLI. Disable and reenable MFC profiling service in ISE by referring to the previous step.
3. Useful troubleshooting steps for debugging, refer to the MFC Profiler component in the debug. The logs can be verified from the support bundle or tail the logs by running the show logging application ise-pi-profiler.log tail command via ISE CLI.

Known defect for MFC profiler showing up as not running instead of a disabled state:

- Cisco bug ID ·72853

Services included in ISE 3.4

MFA (Duo Sync Service)

In Cisco Identity Services Engine (ISE) 3.4, the Duo Sync Service facilitates seamless integration of Duo Multi-Factor Authentication (MFA) without requiring an external Duo Authentication Proxy. This native integration enhances security for VPN and TACACS+ authentication workflows.

Key Features and Functions of MFA (Duo Sync Service) in ISE

1. Native Duo Integration (No Duo Proxy Required): Cisco ISE 3.4 supports direct integration with Duo, without deploying and managing a separate Duo Authentication Proxy. This simplifies deployment and reduces infrastructure complexity.
2. Identity Sync with Duo: ISE 3.4 includes a Duo Sync Service that enables automated user synchronization from Active Directory to Duo and is not required to manually add users to Duo—synchronization as it is handled via ISE.

Verify and Troubleshoot MFA (Duo Sync Service)

1. By default, the MFA Duo Sync service is disabled. To enable this service, navigate to Administration > Identity Management > Settings > External Identity Source Settings > Toggle MFA.
2. If the service is enabled, but showing as disabled/not running via the show application status ise command in ISE CLI. Disable and reenable the MFA Duo Sync Service in ISE by referring to the prior step.
3. Useful troubleshooting steps for debugs, run the ise-duo command component in debug. The logs can be verified from the support bundle or tail the logs by running the show logging application ise-duo.log tail command via ISE CLI.

Aciconn (ACI Connection Service)

The ACIconn (ACI Connector) Service is responsible for integrating Cisco ISE with Cisco Application Centric Infrastructure (ACI). This integration allows ISE to dynamically share endpoint identity and posture information with Cisco ACI for software-defined segmentation and policy enforcement.

Key Features and Functions of Aciconn Service in ISE

1. Context Sharing with ACI: ACIconn shares user identity, authentication status, posture, and session details with Cisco APIC. It enables context-aware micro segmentation and policy decisions based on ISE data.
2. Dynamic Endpoint-to-EPG Mapping: Automatically maps users/devices authenticated in ISE to Endpoint Groups (EPGs) in Cisco ACI. Enables identity-based segmentation in your data center.
3. Bi-directional Communication: ISE can send updates to ACI and ACI can query ISE for endpoint statuses, which enables real-time access control and segmentation changes.

Verify and Troubleshoot Aciconn

1. By default Aciconn service is disabled. To enable this service, navigate to Workcenters > TrustSec > Settings -> ACI Settings > Enable ACI Integration and fill in the required details to establish the connection.
2. If the service is enabled but showing as disabled/not running via the show application status ise command in ISE CLI. Disable and reenable ACI Integration Service in ISE by referring to to the prior step.
3. Useful troubleshooting steps for debugs, check the ACI Connector component in debug. The logs can be verified from the support bundle or tail the logs by running the show logging application aciconn.log tail & show logging application workloads.log tail command via ISE CLI.

ISE Prometheus Exporter

The ISE Prometheus Exporter is a background service that exports the Cisco ISE metrics in a format compatible with Prometheus, a popular open-source monitoring and alerting system. This allows third-party monitoring tools like Prometheus and Grafana to ingest ISE metrics for dashboards, alerts, and performance analysis.

Key Features and Functions of ISE Prometheus Service in ISE

1. Standardized Metrics Export: Exports Cisco ISE performance, usage, and health metrics in Prometheus, compatible format and enables consistent and structured monitoring data.
2. Third-Party Monitoring Integration: Seamlessly integrates with monitoring tools like Prometheus, Grafana, and others.
3. Supports Alerting and Reporting: Metrics can be used to define alerts in Prometheus or integrated alerting platforms. Helps identify trends or anomalies over time.

Verify and Troubleshoot ISE Prometheus Exporter

1. ISE Prometheus Exporter is enabled by default in ISE. If the service is not running, run the application stop ise and application start ise command to restart services.
2. Useful troubleshooting steps for debugs, check the Prometheus component in debug. The logs can be verified from the support bundle or tail the logs by running the show logging application prometheus.log tail command via ISE CLI.

3.Verify if there are any instances of high resource utilization on the node, as this impacts the performance of ISE Prometheus.

ISE Prometheus Alert Manager

ISE Prometheus Alert Manager in ISE, manages the alerting based on the metrics exported by the Prometheus Exporter Service. It processes the collected telemetry data and triggers alarms or notifications when certain thresholds or conditions are met.

Key Features and Functions of ISE Prometheus Alert Manager Service in ISE

1. Alert Processing: Monitors ISE metrics for anomalies or threshold breaches like high CPU, memory, or authentication failures.
2. Works with Prometheus Exporter: Complements the metrics exporter by acting on the data, enabling proactive health management.
3. Notification Integration: Forwards alerts to external tools or dashboards like email, SNMP traps, or other monitoring systems.

Verify and Troubleshoot ISE Prometheus Alert Manager

1. ISE Prometheus Exporter is enabled by default in ISE. If the service is not running, run the application stop ise and application start ise command to restart services.
2. Useful troubleshooting steps for debugs, check the alertmanager component in debug. The logs can be verified from the support bundle or tail the logs by running the show logging application alertmanager.log tail command via ISE CLI.
3. Verify if there are any instances of high resource utilization on the node, as this impacts the performance of the ISE Prometheus.

Protocols Engine

Protocols Engine is the ISE service/module that manages and processes network protocol interactions such as RADIUS, TACACS+, Diameter, and other authentication and accounting protocols supported by ISE. Without the protocols engine running as expected, ISE cannot process authentication requests or enforce network access policies. It ensures secure and reliable communication between network devices and the ISE server.

Key Features and Functions of the Protocols Engine Service in ISE

1. Radius Processing: Handles authentication, authorization, and accounting (AAA) requests from network devices.
2. TACACS+ Handling: Manages TACACS+, authentication, and command authorization for device administration.
3. Protocol Parsing and Validation: Parses incoming protocol packets and validates correctness.

Verify and Troubleshoot Protocols Engine

1. The ISE protocols engine is enabled by default in ISE. If the service is not running, run the application stop ise and application start ise command to restart services.

2. Useful troubleshooting steps for debugs, check the ProtocolsEngine-AAA, ProtocolsEngine-config, ProtocolsEngine-GRPC, ProtocolsEngine-logging components in debug. The logs can be verified from the support bundle or tail the logs by running the show logging application protocols-engine.log tail command via ISE CLI.

Services Included in ISE 3.5

Remote Support Authorization Service

The Remote Support Authorization Service is the ISE Service that securely manages authorization for Cisco Technical Assistance Center (TAC) remote support sessions. It validates whether remote support access is permitted based on the configured support policies and ensures only authorized remote troubleshooting sessions can be established. This service helps maintain secure administrative access while allowing Cisco TAC engineers to assist in troubleshooting when remote support is enabled.

Key Features and Functions of Remote Support Authorization Service in ISE

1. Remote Support Authorization: Validates and authorizes Cisco TAC remote support sessions.
2. Secure Access Control: Ensures remote access is granted only when remote support is explicitly enabled and authorized.
3. Support Session Management: Coordinates authorization requests between the ISE node and Cisco remote support infrastructure.

Verify and Remote Support Authorization Service in ISE

The Remote Support Authorization Service is enabled by default when remote support functionality is available. If the service is not running, run the application stop ise and application start ise commands to restart services.

---

1. Useful troubleshooting steps for debugs, include RemoteSupportAuthorization-config, RemoteSupportAuthorization-service, and RemoteSupportAuthorization-logging components in debug mode. The logs can be verified from the support bundle or viewed running the CLI show logging application remote-support-authorization.log tail command.

ISE Prometheous Alert Manager Service

The ISE Prometheus Alertmanager Service manages alerts generated from Prometheus and metrics are collected within Cisco ISE. It receives alerts from the Prometheus monitoring service, groups and suppresses duplicate alerts, and forwards notifications to the configured destinations. This service enables administrators to monitor the operational health of ISE and responds proactively to infrastructure or application issues.

Key Features and Functions of ISE Prometheus Alert Manager Service in ISE

1. Alert Processing: Receives alerts generated from Prometheus metrics.
2. Alert Grouping and Deduplication: Groups similar alerts and suppresses duplicate notifications to reduce alert noise.
3. Notification Management: Routes alerts to configured notification channels based on alert policies.

Verify ISE Prometheous Alert Manager Service in ISE

The ISE Prometheus Alert Manager Service is enabled by default as part of the monitoring framework. If the service is not running, run the application stop ise and application start ise to restart services.

Useful troubleshooting steps for debugs, include Alertmanager-config, Alertmanager-service, and Alertmanager-logging components in debug mode. The logs can be verified from the support bundle or viewed running the CLI show logging application alertmanager.log tail command.

ISE DataGrid Service

The ISE Data Grid Service provides distributed in-memory data storage and synchronization across Cisco ISE nodes. It enables multiple ISE services to securely share runtime information such as session data, endpoint information, caches, and operational state between nodes. The Data Grid Service improves scalability, performance, and high availability by allowing services to access shared data without relying solely on the primary database.

Key Features and Functions of ISE DataGrid Service in ISE

1. Distributed Data Storage: Maintains shared in-memory data across all ISE nodes.
2. Session and Cache Synchronization: Synchronizes runtime information, endpoint data, and service caches between nodes.
3. High Availability Support: Enables distributed services to continue operating efficiently by providing resilient data sharing across the deployment.

Verify ISE DataGrid Service in ISE

1. The ISE Data Grid Service is enabled by default. If the service is not running, run the application stop ise and application start ise commands to restart services.
2. Useful troubleshooting steps for debugs include, DataGrid-cluster, DataGrid-cache, DataGrid-config, and DataGrid-logging components in debug mode. The logs can be verified from the support bundle or viewed running the CLI show logging application datagrid.log tail command.

Standard Concerns in ISE

Apart from the issues with ISE services, these are some concerns found in the ISE nodes along with basic troubleshooting steps:

Verification for High Load Average, Resource Utilization Issues (CPU/MEMORY/DISK), Insufficient Resources

1. Verify the Cisco recommended resources are allocated to the node by running the show inventory command via ISE CLI.

2. From the CLI of the ISE node, run the tech top command to verify resource utilization of ISE.

3. Verify disk utilization by running the show disk command via ISE CLI.

4. Purge the inactive endpoints, clear the local disk of node, and perform upgrade clean-ups.

If the issue persists, Contact Cisco TAC, and provide the secured support bundle, Heap dump and Thread dump from the node experiencing the issue.

---

1. To secure the heap dump, log in to the CLI ISE node, run the application configure ise command. Select option 22.
2. To secure the thread dump, log in to the CLI ISE node, run the application configure ise command. Select option 23. The thread dump is included in the support bundle or can be tailed via ISE CLI running the show logging application appserver/cataline.out command.\

Verify and Troubleshoot Monitoring Issues

Monitoring and Troubleshooting (MnT) function of ISE is one of the major blocks of ISE architecture,

which provides monitoring, reporting and alerting capabilities. ISE displays monitoring information in many places, including:

- Cisco ISE Homepage
- Context Visibility Views
- RADIUS Live Logs and Live Sessions
- Global Search
- Threat-Centric NAC Live Logs
- TACACS Live Logs

General issues observed in the Monitoring and Troubleshooting Category:

1. Radius/ TACACS Live logs not available
2. Live sessions not available
3. Health Summary not available
4. Performance (high CPU/Memory) issues seen on the (MnT nodes)

Debugs to be enabled on the MnT nodes to narrow down the issue:

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

In addition to the components in debug, this information can help for troubleshooting:

1. Are live sessions also affected or only live logs?
2. Are Radius or TACACS logs affected or both?
3. Do you see high CPU utilization or high swap space usage on MnT nodes?
4. How many buffer files do you see on the MnT nodes? Buffer files can be found under: /opt/CSCOcpm/mnt/data/collector
5. Is the memory and CPU reservations enabled? if not, enable it.
6. Was the MnT/config/session DB reset performed recently or in the past?
7. Are the syslogs being sent from the PSN’s to MnT nodes?

If you are using Syslog services for MnT, this information is required for troubleshooting:

1. Are you using secure syslog targets, if not, disable it, as it is known to cause deadlocks in threads causing collectors to stop functioning.
2. Are you using secure syslog targets, ensure cert mapping is properly set under Administration > Logging > Remote Logging Targets > Secure Syslog Collector 1 and 2
3. Verify if logging categories are appropriately (recommended to remove unused/unwanted logging categories - this reduces the load on MnT nodes) set and logging targets are correctly configured.

4. Check the awrrep*.html files from the support bundle to understand and receive a hint of what component is sending more frequent syslogs. For instance, if TACACS tables are seen with insert or update queries, TAC can check the collector logs to correlate and understand what syslogs are being sent more frequently.

If the issue is related to the performance on the MnT node, TAC requires this information:

1. Tech top output from the ISE CLI of the MnT node.
2. If the CPU is high, do you see high memory or high swap space utilization?
3. Support bundle with the heap dump and thread dump secured.

Reference

- Cisco Identity Services Engine Administrator Guide, Release 3.3
- Cisco Identity Services Engine Administrator Guide, Release 3.4
- Troubleshoot and Enable Debugs on ISE