Comprendre les services, l'objectif et le dépannage ISE

Table des matières

Introduction

Ce document décrit les services ISE, leur objectif et le dépannage.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur Cisco Identity Services Engine.

Composants utilisés

Le document n'est pas limité à des versions logicielles et matérielles spécifiques de 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cisco Identity Services Engine (ISE) est une solution complète conçue pour fournir une sécurité réseau avancée grâce à la gestion centralisée des politiques, à l'authentification, à l'autorisation et à la comptabilité (AAA). Elle permet aux entreprises de gérer l'accès au réseau pour les utilisateurs, les périphériques et les applications tout en garantissant la sécurité, la conformité et une expérience utilisateur transparente.

Pour atteindre ces objectifs, Cisco ISE utilise une gamme de services, chacun étant responsable de tâches spécifiques qui permettent au système de fonctionner efficacement. Ces services fonctionnent ensemble pour garantir un accès réseau sécurisé, une application robuste des politiques, une journalisation détaillée, des intégrations transparentes aux systèmes externes et un profilage efficace des périphériques.

Chaque service d'ISE joue un rôle essentiel dans le maintien de l'intégrité et de la disponibilité de la solution. Certains services gèrent des fonctions de base, telles que la gestion et l'authentification des bases de données, tandis que d'autres offrent des fonctionnalités avancées, telles que le profilage des périphériques, la gestion des certificats et la surveillance.

Cet article présente les différents services de Cisco ISE et explique leur objectif, leur importance et les étapes de dépannage potentielles en cas de problème. Que vous soyez un administrateur ou un professionnel de la sécurité réseau, la compréhension de ces services vous permet de garantir un déploiement ISE fluide et sécurisé.

Présentation et dépannage des services ISE

Les services mentionnés dans la capture d'écran sont utilisés par ISE pour prendre en charge ses fonctionnalités. Vérifiez l'état ou les services disponibles dans ISE en utilisant la commande show application status ise via l'interface de ligne de commande du noeud ISE. Voici un exemple de résultat qui montre l'état ou les services disponibles sur l'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 disponibles dans ISE.

Maintenant, examinez chaque service de plus près en détail.

Écouteur de base de données

Le service Écouteur de base de données est un composant essentiel qui permet de gérer la communication entre ISE et le serveur de base de données. Il écoute et traite les demandes liées à la base de données, ce qui garantit que le système ISE peut lire et écrire dans sa base de données sous-jacente.

Points clés sur le service d'écoute de base de données dans ISE

1. Interface de communication : Il sert de pont de communication entre ISE et le serveur de base de données, permettant au système de récupérer et de stocker des données telles que les informations d'identification de l'utilisateur, les informations de session, les stratégies réseau, etc.

2. Prise en charge des bases de données externes : ISE peut être configuré pour utiliser une base de données externe (telle qu'Oracle ou Microsoft SQL Server) pour l'authentification des utilisateurs et le stockage des politiques. Le service d'écoute de base de données garantit qu'ISE peut se connecter et interagir avec cette base de données externe de manière sécurisée et efficace.

3. Gestion des données : Le service écoute les requêtes de base de données du système ISE, puis les traduit en actions appropriées sur la base de données externe. Il peut traiter des demandes telles que l'insertion, la mise à jour ou la suppression d'enregistrements, ainsi que la récupération d'informations à partir de la base de données.

4. Surveillance du fonctionnement de la base de données : En plus de fournir le canal de communication, il permet également de s'assurer que la connexion à la base de données externe est stable et opérationnelle. Si la connexion échoue, ISE revient au stockage local ou passe en mode dégradé en fonction de la configuration.

Serveur de base de données

Le service Serveur de base de données est responsable de la gestion du stockage et de la récupération des données utilisées par le système. Il gère l'interaction avec la base de données sous-jacente qu'ISE utilise pour stocker la configuration, les informations de stratégie, les données utilisateur, les journaux d'authentification, les profils de périphérique et d'autres informations nécessaires.

Points clés sur le service de serveur de base de données dans ISE

1. Stockage interne des données : Le service de serveur de base de données gère principalement la base de données interne intégrée qu'ISE utilise pour stocker localement les données opérationnelles. Cela inclut des données telles que les enregistrements d'authentification et d'autorisation, les profils utilisateur, les politiques d'accès réseau, les informations sur les périphériques et les terminaux, les informations sur les sessions.

2. Base de données intégrée : Dans la plupart des déploiements Cisco ISE, le système utilise une

base de données PostgreSQL intégrée pour le stockage local. Le service Serveur de base de données garantit le bon fonctionnement de cette base de données et gère toutes les requêtes, mises à jour et tâches de gestion liées aux données qu'elle contient.

3. Intégrité de la base de données : Le service veille à ce que toutes les transactions soient traitées correctement et à ce que l'intégrité de la base de données soit maintenue. Il gère des tâches telles que le verrouillage d'enregistrements, la gestion des connexions aux bases de données et l'exécution de requêtes.

Vérifier et dépanner que les services Écouteur de base de données et Serveur de base de données sont en cours d'initialisation ou non

L'écouteur de base de données et le serveur de base de données sont des services essentiels qui doivent être exécutés ensemble pour que tous les autres services fonctionnent correctement. Si ces services ne sont pas en cours d'exécution ou sont bloqués pendant l'initialisation, ces étapes de dépannage aident à la récupération.

1. Redémarrez les services ISE à l'aide des commandes application stop ise et application start ise.

2. S'il s'agit d'un noeud de VM, le redémarrage du noeud à partir de la VM doit aider à la récupération des services.

3. Si le noeud est un noeud physique, le redémarrage/rechargement du noeud à partir de CIMC doit aider à la récupération des services.

4. Si la base de données est endommagée, contactez le TAC Cisco pour obtenir des informations complémentaires sur le dépannage.

Le processus d'écoute de la base de données et le serveur de base de données s'arrêtent ou ne démarrent généralement pas en cas de divergence dans la base de données ou lorsque celle-ci ne peut pas s'initialiser correctement. Dans ces cas, l'exécution de la réinitialisation d'application à l'aide de la commande application reset-config ise doit aider à la récupération et au nouveau lancement de la base de données. L'exécution de la commande application reset-config ise supprime les configurations et les certificats, mais les détails de l'adresse IP et du nom de domaine sont conservés. Il est recommandé de contacter le centre d'assistance technique de Cisco pour obtenir plus d'informations et comprendre l'impact potentiel avant d'appliquer cette commande à n'importe quel noeud du déploiement.

Serveur d'applications

Le serveur d'applications est un composant clé responsable de l'exécution et de la gestion des fonctionnalités et des services de base de la plate-forme ISE. Il héberge la logique métier, les interfaces utilisateur et les services qui permettent à ISE de jouer son rôle dans le contrôle d'accès au réseau, l'authentification, l'autorisation, la comptabilité et la gestion des politiques.

Points clés sur le service de serveur d'applications dans ISE

1. Interface utilisateur (UI) : Le service de serveur d'applications est responsable du rendu de l'interface utilisateur Web pour ISE. Cela permet aux administrateurs de configurer et de gérer des stratégies, d'afficher des journaux et des rapports, et d'interagir avec d'autres fonctionnalités d'ISE.

2. Gestion des services : Il est chargé de gérer les différents services fournis par ISE, notamment la gestion des politiques, les tâches administratives et la communication avec d'autres noeuds ISE dans un déploiement distribué.

3. Traitement centralisé : Le service de serveur d'applications joue un rôle central dans l'architecture ISE, en fournissant la logique qui tient compte des stratégies, des demandes d'authentification et des données provenant des périphériques réseau, des répertoires et des services externes.

Vérification de l'initialisation ou de l'inexécution du serveur d'applications

Le serveur d'applications dépend de quelques applications Web telles que les certificats, les ressources, le déploiement et les licences. Lorsqu'une application Web n'a pas pu s'initialiser, le serveur d'applications reste bloqué dans l'état d'initialisation. Le serveur d'applications met environ 15 à 35 minutes pour passer de l'état **Non exécuté** → **Initialisation** → **En cours d'exécution** selon les données de configuration sur le noeud.

1. Assurez-vous que le certificat d'administration d'ISE est valide et actif dans le déploiement pour tous les noeuds.
2. Assurez-vous que tous les noeuds du déploiement sont synchronisés avec le noeud Administrateur principal.
3. Si le noeud est une machine virtuelle, assurez-vous que les ressources recommandées sont allouées au noeud.

Vérifiez l'état du serveur d'applications à l'aide de la commande **show application status ise** de l'interface de ligne de commande du noeud ISE. La plupart des journaux associés au serveur d'applications sont disponibles sous

Fichiers Catalina.Out et Localhost.log.

Si les conditions mentionnées sont remplies et que le serveur d'applications reste bloqué à l'état d'initialisation, sécurisez l'ensemble de support à partir de l'interface CLI/GUI d'ISE. Récupérez / redémarrez les services à l'aide des commandes application stop ise et application start ise.

Base de données Profiler

La base de données du profileur est une base de données spécialisée utilisée pour stocker des informations sur les périphériques réseau, les terminaux et les profils de périphériques détectés par le service du profileur. Le profileur est un composant essentiel d'ISE qui identifie et classe automatiquement les périphériques réseau (ordinateurs, smartphones, imprimantes, périphériques IoT, etc.) en fonction des caractéristiques et des comportements du réseau.

Points clés sur le service de base de données Profiler dans ISE

1. Profilage des périphériques : La fonction principale du service de base de données du profileur est de prendre en charge le processus de profilage. ISE utilise ce service pour stocker les informations collectées lors du profilage, telles que :

- Type de périphérique (par exemple : smartphone, ordinateur portable, imprimante, périphérique IoT)
- Système d'exploitation du périphérique (par exemple : Windows®, macOS®, Cisco IOS®, Android®)
- Fabricant de périphériques
- Comportements ou modèles de réseau permettant de classer les périphériques

2. Informations sur le profileur : Il stocke les attributs de profileur, tels que les profils matériels et logiciels des périphériques, qui sont utilisés pour faire correspondre les périphériques à des politiques prédéfinies. Ces informations sont également utilisées pour attribuer dynamiquement des périphériques aux politiques d'accès réseau ou aux VLAN appropriés en fonction de leur profil.

3. Processus de profilage : Le processus de profilage est généralement basé sur :

- Profilage actif : ISE interroge activement les périphériques du réseau pour obtenir des informations.
- Profilage passif : ISE collecte passivement les données du trafic réseau, telles que les requêtes DHCP, les attributs RADIUS, les en-têtes HTTP et d'autres protocoles réseau, afin de déterminer le type de périphérique.

Vérification et dépannage des services de profilage ISE

1. À partir de l'interface de ligne de commande ISE, exécutez la commande show application status ise pour vérifier que le service de base de données du profileur est en cours d'exécution.

2. Dans l'interface utilisateur graphique du noeud d'administration principal, accédez à Administration > Déploiement > sélectionnez le noeud. Cliquez sur Edit et vérifiez que les services de session et les services de profilage sont activés.

3. À présent, accédez à Administration > Déploiement > Sélectionnez le noeud. Passez à la configuration Profiler et vérifiez si les sondes requises sont activées pour sécuriser les données des points d'extrémité.

4. Accédez à Administration > System > Profiling et vérifiez les paramètres du profileur configurés pour CoA.

5. Dans Visibilité du contexte > Points de terminaison > Sélectionnez les points de terminaison et vérifiez les attributs collectés par différentes sondes pour les points de terminaison.

Débogages utiles pour le dépannage des problèmes de profilage :

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

Moteur d'indexation ISE

Le moteur d'indexation est un service chargé de rechercher, d'indexer et d'extraire efficacement les données stockées dans la base de données ISE. Elle améliore les performances et l'évolutivité d'ISE, en particulier lorsqu'il s'agit de gérer de grands volumes de données et de fournir un accès rapide aux informations nécessaires aux tâches d'authentification, d'autorisation, de surveillance et de création de rapports.

Points clés sur le moteur d'indexation ISE dans ISE

1. Indexation des données : Le moteur d'indexation ISE crée des index pour différents types de données stockées dans ISE, tels que les journaux d'authentification, les journaux de session, les résultats de stratégie, les données de profilage et les enregistrements d'accès au réseau. L'indexation aide à organiser ces données de manière à rendre la recherche et l'interrogation plus efficaces.

2. Gestion des journaux et création de rapports : Ce service joue un rôle essentiel dans la gestion des journaux en améliorant les performances des rapports et des requêtes de journaux. Par exemple, lors de la recherche d'événements d'authentification spécifiques, le moteur d'indexation permet une récupération plus rapide des enregistrements souhaités, ce qui est essentiel pour la surveillance de la sécurité et la création de rapports de conformité.

3. Récupération des données : Le moteur d'indexation est également chargé de s'assurer qu'ISE peut récupérer efficacement des données indexées à partir de sa base de données sous-jacente si nécessaire. Cela permet à ISE de fournir des réponses rapides aux requêtes provenant de l'interface utilisateur, d'outils externes ou d'API.

Vérifiez que le moteur d'indexation ISE n'est pas en cours d'exécution ou d'initialisation

1. Vérifiez que les recherches DNS directes et inversées fonctionnent pour tous les noeuds du cluster via l'interface de ligne de commande en utilisant la commande **nslookup <FQDN / IP address of the ISE node** > .
2. Vérifiez que les certificats d'administration ISE sont valides et actifs pour tous les noeuds du cluster.
3. Vérifiez que NTP fonctionne et est synchronisé avec les noeuds ISE via l'interface de ligne de commande en utilisant la commande **show ntp**.

Le moteur d'indexation est utilisé par la visibilité du contexte et doit être opérationnel pour que la visibilité du contexte fonctionne. Les journaux utiles qui peuvent aider au dépannage du moteur d'indexation sont les fichiers **ADE.log** qui peuvent être sécurisés à partir du bundle de support ou adaptés via l'interface de ligne de commande en utilisant la commande **show logging system ade/ADE.log tail** au cours du problème.

Connecteur AD

Le connecteur AD (Active Directory Connector) est un service qui permet à ISE de s'intégrer à Microsoft Active Directory (AD), permettant à ISE d'authentifier, d'autoriser et de gérer les utilisateurs en fonction de leurs informations d'identification AD et de leur appartenance à un groupe. Le connecteur AD sert de pont entre ISE et Active Directory, permettant à ISE d'exploiter AD pour le contrôle d'accès au réseau (NAC) et l'application des politiques.

Fonctions clés du service de connecteur AD dans ISE

1. Intégration à Active Directory : Le service de connecteur AD agit comme un pont entre ISE et Active Directory. Elle permet à ISE de se connecter en toute sécurité à AD, ce qui lui permet d'utiliser AD comme magasin d'identités centralisé pour l'authentification des utilisateurs et l'application des politiques.

2. Synchronisation : Le service Connecteur AD prend en charge la synchronisation des données d'utilisateur et de groupe d'Active Directory vers ISE. Cela garantit que ISE dispose d'informations à jour sur les utilisateurs et les groupes, ce qui est essentiel pour l'application précise des politiques.

3. Communication sécurisée : Le service de connecteur AD établit des canaux de communication sécurisés entre ISE et Active Directory, généralement à l'aide de protocoles tels que LDAP sur SSL (LDAPS) pour garantir la confidentialité et l'intégrité des données lors des processus d'authentification et de requête.

4. Prise en charge de plusieurs domaines Active Directory : Le service peut prendre en charge les connexions à plusieurs domaines Active Directory. Cela est particulièrement utile dans les environnements de grande taille ou multidomaines, où ISE doit authentifier les utilisateurs de différents domaines ou forêts AD.

5. Recherche d'utilisateurs et de groupes : Elle permet à ISE d'interroger AD pour obtenir des informations sur les utilisateurs et les groupes. Il peut s'agir de détails tels que les noms d'utilisateur, les appartenances à des groupes et d'autres attributs d'utilisateur pouvant être utilisés pour appliquer des stratégies d'accès au réseau. Par exemple, les stratégies d'accès réseau peuvent être appliquées en fonction de l'appartenance à un groupe AD d'un utilisateur (par exemple : l'octroi de différents niveaux d'accès aux utilisateurs de différents groupes).

1. Vérifiez si le protocole NTP est synchronisé avec les noeuds et que la différence de temps entre AD et ISE doit être inférieure à 5 minutes.

2. Vérifiez si le serveur DNS peut résoudre les noms de domaine complets et les domaines associés à Active Directory.

3. Accédez à **Operations** > **Reports** > **Reports** > **Diagnostics** > **AD connector Operations**, vérifiez les événements ou les rapports liés à AD.

Les journaux utiles pour le dépannage sont **ad_agent.log** avec des journaux de débogage pour le composant **runtime**.

Base de données de session M&T

La base de données de session M&T (Monitoring and Troubleshooting Session Database) joue un rôle essentiel dans le stockage et la gestion des données de session pour les événements d'accès au réseau. La base de données de sessions M&T contient des informations sur les sessions actives, notamment les authentifications utilisateur, les connexions de périphériques et les événements d'accès au réseau, qui sont essentielles pour la surveillance, le dépannage et l'analyse de l'activité du réseau.

Fonctions clés du service de base de données de session M&T dans ISE

1. Stockage des données de session : Le service de base de données de session M&T est chargé de stocker et d'indexer les données relatives aux sessions utilisateur et périphérique sur le réseau. Cela inclut les heures de début et de fin de session, les résultats d'authentification, l'identité de l'utilisateur ou du périphérique et les stratégies associées (telles que les attributions de rôles ou les attributions de VLAN). Les données incluent également des informations de gestion de compte RADIUS qui détaillent le cycle de vie de la session, y compris l'authentification initiale et tous les messages de gestion de compte qui suivent les événements de session.

2. Données historiques et en temps réel : Le service fournit un accès aux données de session en temps réel (sessions actives) et aux données de session historiques (sessions passées). Cela permet aux administrateurs non seulement de surveiller l'accès utilisateur en cours, mais également de consulter les journaux de session précédents pour examiner les problèmes ou valider les événements d'accès. La surveillance des sessions en temps réel permet de s'assurer qu'aucun périphérique non autorisé ne se trouve actuellement sur le réseau.

3. Surveillance renforcée : Fournit des informations sur l'activité des utilisateurs et des périphériques, y compris les stratégies appliquées à leurs sessions, afin de détecter les problèmes de sécurité potentiels ou les accès non autorisés.

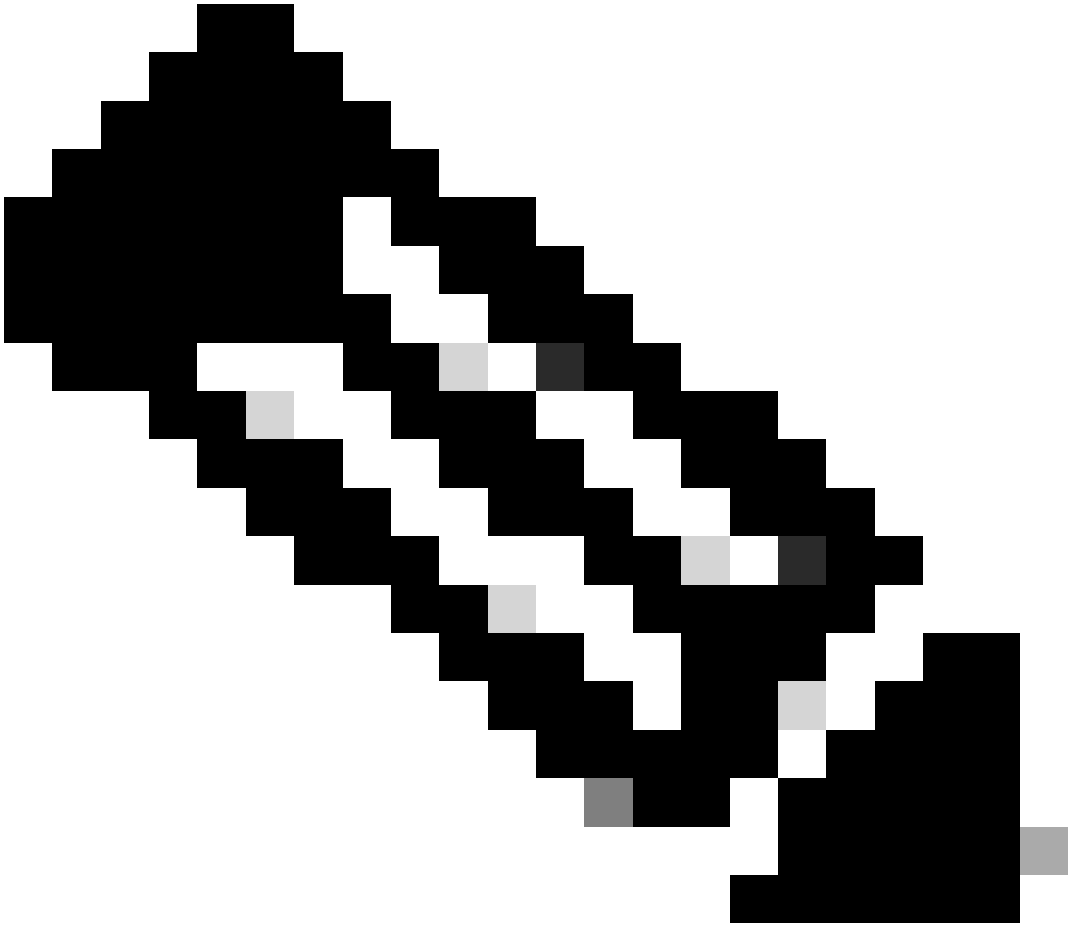
4. Audit et rapports : Facilite l'audit de conformité et la création de rapports en stockant un historique des événements d'accès au réseau et en fournissant des données pour la création de rapports réglementaires.

Vérification et dépannage de la base de données de session M&T dans ISE

1. Vérifiez si le noeud est alloué avec les ressources recommandées.

2. Sécurisez **show tech-support** depuis l'interface de ligne de commande ISE pour une vérification plus approfondie du problème.

3. Réinitialisez la base de données de session M&T en exécutant la commande **application configure ise** dans via l'interface de ligne de commande ISE et sélectionnez l'option **1**.



Remarque : La réinitialisation de la base de données M&T ne doit être effectuée qu'après vérification de l'impact potentiel du déploiement. Contactez le TAC Cisco pour une vérification plus approfondie.

Défauts connus

ID de bogue Cisco ·32364

Processeur de journaux M&T

M&T Log Processor (Monitoring and Troubleshooting Log Processor) est un composant chargé de la collecte, du traitement et de la gestion des données de journal générées par divers services au sein d'ISE. Il s'agit d'un élément clé de l'infrastructure de surveillance et de dépannage (M&T), qui aide les administrateurs à surveiller et à dépanner les événements d'accès au réseau, les tentatives d'authentification, l'application des politiques et d'autres activités au sein du système ISE. Le processeur de journalisation M&T gère spécifiquement le traitement des entrées de journal, garantissant qu'ISE peut stocker, analyser et présenter les informations nécessaires à la

création de rapports, à l'audit et au dépannage.

Principales fonctions du service de processeur de journalisation M&T dans ISE

1. Collecte et traitement des journaux : Le service Log Processor de M&T collecte et traite les journaux générés par divers composants ISE, tels que les demandes d'authentification, les décisions d'autorisation, les messages de comptabilité et les activités d'application des stratégies. Ces journaux incluent des informations détaillées sur les utilisateurs, les périphériques et les tentatives d'accès au réseau, telles que les horodatages, les ID utilisateur, les types de périphériques, les stratégies appliquées, la réussite ou l'échec des demandes d'accès et les raisons des échecs.

2. Déclaration et conformité : Les journaux traités par ce service sont essentiels pour la création de rapports de conformité. De nombreuses réglementations exigent des entreprises qu'elles conservent des journaux des accès utilisateur et des événements de sécurité. Le service Log Processor de M&T garantit que tous les journaux pertinents sont traités et disponibles pour les audits de conformité à la réglementation. Il permet de générer des rapports détaillés basés sur les données des journaux, tels que les journaux d'accès utilisateur, les taux de réussite/d'échec de l'authentification ou les journaux d'application des stratégies.

Vérification et dépannage du service Log Processor M&T dans ISE

1. Assurez-vous que le noeud ISE est déployé avec les ressources recommandées conformément au Guide d'installation de Cisco.

2. Pour vérifier le problème, exécutez la commande **show logging system ade/ADE.log tail** via l'interface de ligne de commande ISE pour les exceptions / erreurs pertinentes.

Défauts connus

ID de bogue Cisco ·15130

Service d'autorité de certification

Le service d'autorité de certification (CA) est un composant essentiel qui permet de gérer les certificats numériques pour sécuriser les communications et authentifier les périphériques, les utilisateurs et les services réseau. Les certificats numériques sont essentiels pour établir des connexions fiables et assurer une communication sécurisée entre les clients (ordinateurs, smartphones, périphériques réseau) et les composants de l'infrastructure réseau (commutateurs, points d'accès sans fil, passerelles VPN). Le service CA de Cisco ISE fonctionne en tandem avec les certificats X.509, qui sont utilisés à plusieurs fins dans la sécurité du réseau, y compris l'authentification 802.1X, l'accès VPN, la communication sécurisée et le cryptage SSL/TLS.

Fonctions clés du service d'autorité de certification dans ISE

1. Gestion des certificats : Le service d'autorité de certification est responsable de la création, de l'émission, de la gestion et du renouvellement des certificats numériques au sein d'ISE. Ces

certificats sont utilisés pour divers protocoles d’authentification et à des fins de chiffrement sur le réseau. Il peut agir en tant qu'autorité de certification interne ou s'intégrer à une autorité de certification externe (par exemple : Microsoft AD CS, les autorités de certification publiques comme VeriSign ou DigiCert) pour émettre des certificats.

2. Délivrance des certificats : Pour les environnements nécessitant EAP-TLS ou des méthodes d'authentification similaires basées sur des certificats, ISE peut émettre des certificats pour les périphériques d'accès réseau (NAD), les utilisateurs ou les terminaux. ISE peut générer et déployer automatiquement des certificats pour l'authentification des périphériques et des utilisateurs, ou demander des certificats à une autorité de certification externe.

3. Inscription au certificat : Le service AC prend en charge l'inscription de certificats pour les terminaux, tels que les ordinateurs portables, les téléphones et autres périphériques réseau, qui doivent s'authentifier sur le réseau à l'aide de certificats. ISE utilise des protocoles tels que SCEP (Simple Certificate Enrollment Protocol) ou ACME (Automated Certificate Management Environment) pour faciliter l'inscription de certificats pour les périphériques.

4. Renouvellement du certificat : Le service automatise le renouvellement des certificats expirant pour les périphériques et les utilisateurs. Il garantit que les certificats sont toujours valides et à jour, évitant ainsi les interruptions de service provoquées par des certificats expirés.

5. Intégration avec les autorités de certification externes : Bien qu'ISE puisse agir comme sa propre autorité de certification, il est plus courant de l'intégrer avec une autorité de certification externe (par exemple : Services de certificats Microsoft Active Directory). Le service AC peut gérer l'interaction entre ISE et l'AC externe, en demandant des certificats pour les utilisateurs, les périphériques et les ressources réseau, le cas échéant.

Service EST

Le service d'inscription sur transport sécurisé (EST) est un protocole utilisé pour délivrer des certificats numériques aux périphériques réseau et aux utilisateurs dans un environnement d'authentification basé sur des certificats. EST est un protocole d'inscription de certificat qui permet aux périphériques de demander des certificats à une autorité de certification (CA) de manière sécurisée et automatisée. Le service EST est particulièrement utile pour l'authentification des périphériques, comme dans les environnements 802.1X, les connexions VPN ou les scénarios BYOD (Bring Your Own Device), où les périphériques doivent s'authentifier sur le réseau à l'aide de certificats.

Fonctions clés du service EST dans ISE

1.Inscription au certificat : Le service EST est chargé d'activer l'inscription sécurisée des certificats pour les périphériques (tels que les commutateurs, les points d'accès ou les terminaux) qui nécessitent des certificats à des fins d'authentification. L'inscription est effectuée sur un transport sécurisé (généralement HTTPS), garantissant que le processus est chiffré et protégé contre tout accès non autorisé.

2. Révocation et renouvellement des certificats : Une fois les certificats inscrits, le service EST

joue également un rôle dans la gestion de la révocation ou du renouvellement des certificats. Par exemple, les périphériques doivent demander un nouveau certificat lorsque le certificat actuel arrive à expiration, et EST peut vous aider à automatiser ce processus.

3. Amélioration du contrôle d'accès au réseau : En permettant aux périphériques de s'authentifier à l'aide de certificats, le service EST renforce la position de sécurité du réseau, en particulier dans les environnements utilisant l'authentification 802.1X.

Vérifier que l'autorité de certification et le service EST ne sont pas en cours d'exécution/initialisation

1. Accédez à **Administration > System > Certificates > Certificate Authority > Internal CA settings.** Assurez-vous que l'état du répondeur CA, EST et OCSP est trié et activé.
2. Les débogages utiles qui peuvent aider au dépannage sont set , provisioning , ca-service , et ca-service-cert. Référez-vous aux fichiers **toise-psc.log , catalina.out , caservice.log** , et **error.log**.
3. Vérifiez que les certificats d'autorité de certification racine et de messagerie ISE sont valides dans le déploiement. Si le renouvellement de l'autorité de certification racine ISE est requis, accédez à **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Request,** sélectionnez usage as **ISE Root CA.** Cliquez sur renouveler l'**autorité de certification racine ISE**.

Service de moteur SXP

Le service du moteur SXP est chargé de gérer et de faciliter la communication entre ISE et les périphériques réseau à l'aide des balises SGT (Security Group Tag) et SXP (Security Group Exchange Protocol). Il joue un rôle essentiel dans la prise en charge des stratégies TrustSec, qui sont utilisées pour appliquer un contrôle d'accès réseau basé sur le groupe de sécurité du périphérique plutôt que sur les adresses IP ou MAC. Le moteur SXP dans ISE est principalement utilisé pour l'échange d'informations sur le groupe de sécurité, ce qui permet d'appliquer des stratégies basées sur l'identité, l'application et l'emplacement de l'utilisateur ou du périphérique. Elle permet aux périphériques de partager des balises de groupe de sécurité (SGT), qui sont utilisées pour appliquer des politiques de sécurité sur les périphériques réseau, tels que les routeurs et les commutateurs.

Fonctions clés du service de moteur SXP dans ISE

1.Intégration avec TrustSec : SXP est généralement déployé dans des environnements qui exploitent Cisco TrustSec, une solution qui applique des politiques de sécurité cohérentes sur les réseaux filaires et sans fil. Le moteur SXP facilite la communication des balises SGT entre les périphériques, permettant l'application dynamique des politiques en fonction du contexte de sécurité d'un périphérique ou d'un utilisateur.

2. Balises de groupe de sécurité (SGT) : L'application des politiques de TrustSec repose essentiellement sur les balises de groupe de sécurité. Ces balises sont utilisées pour classer le trafic réseau et le protocole SXP permet de partager le mappage de ces balises avec des utilisateurs ou des périphériques spécifiques. Cela permet un contrôle granulaire, basé sur des politiques, de l'accès au réseau et du flux de trafic.

Vérification et dépannage du service de moteur SXP dans ISE

1. Par défaut, le service SXP Engine est désactivé dans ISE. Pour l'activer, accédez à **ISE GUI > Administration > Deployment, sélectionnez le noeud. Cochez la case Enable SXP Service** et choisissez l'interface. Vérifiez ensuite l'état du service du moteur SXP à partir de l'interface de ligne de commande ISE en utilisant la commande **show application status ise.**

2.En cas de problèmes de communication réseau, vérifiez que l'interface attribuée au moteur SXP a une adresse IP valide à l'aide de la commande show interface dans l'interface de ligne de commande, et assurez-vous que le sous-réseau IP est autorisé dans le réseau.

3.Consultez les journaux RADIUS en direct pour vérifier les événements de connexion SXP sur ISE.

4. Activez le composant SXP sur les noeuds ISE pour déboguer et capturer les journaux et les exceptions pertinents liés à SXP.

Service TC-NAC

Le service TC-NAC (TrustSec Network Access Control) est un composant qui facilite l'application des stratégies TrustSec sur les périphériques réseau, en s'assurant que le contrôle d'accès est basé sur les balises de groupe de sécurité (SGT) plutôt que sur les adresses IP ou MAC traditionnelles.

TrustSec, quant à lui, est un cadre développé par Cisco qui permet l'application de politiques de sécurité sur le réseau en fonction des rôles des périphériques, des utilisateurs ou des contextes, plutôt qu'en utilisant des mécanismes hérités tels que les VLAN ou les adresses IP. Il offre un contrôle d'accès au réseau plus granulaire et plus dynamique en regroupant les périphériques dans différents groupes de sécurité et en les marquant avec des balises SGT.

Fonctions clés du service TC-NAC dans ISE

1. Intégration avec les systèmes NAC tiers : Le service TC-NAC permet à ISE de communiquer et d'interagir avec des solutions de contrôle d'accès réseau tierces. Cela peut s'avérer utile pour les entreprises qui disposent déjà d'une infrastructure NAC, mais qui souhaitent l'intégrer à Cisco ISE afin d'améliorer les fonctionnalités, d'exploiter des politiques de sécurité supplémentaires ou de tirer parti d'autres fonctionnalités de sécurité réseau de Cisco.

2. Assurer une application transparente des politiques : Lorsqu'elle est intégrée à des solutions NAC tierces, ISE peut prendre en charge certains aspects de l'application des politiques et de la prise de décision. Cela permet un cadre de politiques plus unifié, garantissant que les politiques appliquées par les systèmes NAC Cisco et non Cisco sont cohérentes sur l'ensemble du réseau.

3. Prise en charge des anciens systèmes NAC : Le service TC-NAC aide les entreprises qui disposent de systèmes NAC existants, leur permettant de continuer à utiliser ces systèmes tout en adoptant Cisco ISE pour ses fonctionnalités de sécurité améliorées. ISE peut s'intégrer aux solutions NAC plus anciennes et étendre leur cycle de vie, en assurant le contrôle d'accès, la

sécurité et la mise en conformité en tandem.

4. Facilitation de la communication avec les fournisseurs NAC tiers : Ce service permet à ISE de faciliter la communication avec les solutions NAC tierces qui utilisent des protocoles ou des normes propriétaires. ISE peut interagir avec les systèmes NAC tiers via des protocoles standard (tels que RADIUS, TACACS+ ou SNMP) ou des API personnalisées, en fonction de la solution NAC spécifique utilisée.

Vérification et dépannage du service TC-NAC dans ISE

1. Vérifiez que le contrôle d'accès réseau axé sur les menaces est activé en sélectionnant **Administration > Deployment > PSN node > Enable Threat Centric NAC**.

2. Si le problème provient de la carte SourceFireAMP, vérifiez que le **port 443** est autorisé sur votre réseau.

3. Vérifiez les détails de la session du terminal dans **Operations** > **Threat-Centric NAC Live Logs.**

Alarmes déclenchées par le NAC axé sur les menaces :

- Carte inaccessible (ID syslog : 91002): Indique que la carte n'est pas accessible.
- Échec de la connexion de la carte (ID syslog : 91018): Indique que la carte est accessible mais que la connexion entre la carte et le serveur source est interrompue.
- Carte arrêtée en raison d'une erreur (ID syslog : 91006): Cette alarme est déclenchée si la carte n'est pas dans l'état souhaité. Si cette alarme est affichée, vérifiez la configuration de la carte et la connectivité du serveur. Consultez les journaux de l'adaptateur pour plus de détails.
- Erreur de carte (ID syslog : 91009): Indique que la carte Qualys ne parvient pas à établir une connexion avec le site Qualys ou à télécharger des informations à partir de celui-ci.

Débogages utiles pour dépanner les problèmes de TC-NAC :

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

Service WMI PassiveID

Le service WMI PassiveID est un service qui permet à ISE d'effectuer le profilage de périphérique à l'aide de WMI (Windows Management Instrumentation) en tant que mécanisme passif d'identification et de profilage des points d'extrémité dans le réseau. Il joue un rôle crucial dans le profilage des périphériques, en particulier dans les environnements où les périphériques exécutant le système d'exploitation Windows doivent être identifiés avec précision pour le contrôle d'accès au réseau et l'application des politiques.

Fonctions clés du service WMI PassiveID dans ISE

1. Collecte des identités des périphériques : Le service WMI PassiveID permet à ISE de collecter passivement des informations d'identité à partir de périphériques Windows à l'aide de WMI (Windows Management Instrumentation). Il rassemble des détails système tels que le nom d'hôte du périphérique, la version du système d'exploitation et d'autres attributs pertinents sans que le périphérique doive participer activement.

2. Intégration avec la politique ISE : Les informations collectées par le service WMI PassiveID sont intégrées dans le cadre de stratégie ISE. Il facilite l'application dynamique des politiques basées sur les attributs des périphériques tels que le type, le système d'exploitation et la conformité aux normes de sécurité.

Vérification et dépannage du service WMI PassiveID

Une source hautement sécurisée et précise, ainsi que la plus courante, à partir de laquelle recevoir des informations sur les utilisateurs. En tant que sonde, AD fonctionne avec la technologie WMI pour fournir des identités utilisateur authentifiées.En outre, AD lui-même, plutôt que la sonde, fonctionne comme un système source (un fournisseur) à partir duquel d'autres sondes récupèrent également des données utilisateur.

Débogages utiles et informations requises à des fins de dépannage. Définissez ces attributs au niveau de débogage pour les problèmes WMI PassiveID :

- PassiveID (passiveid*)
- runtime-logging (prrt-server.log)
- Active Directory (ad)_agent.log) - Niveau de suivi
- collecteur (collector.log) (sur les noeuds PassiveID, MnT et sur le noeud pxGrid actif si les sessions sont publiées)
- pxGrid (pxgrid/) (sur MnT secondaire et noeud pxGrid actif si les sessions sont publiées)

Informations requises pour le dépannage de PassiveID WMI :

1. Si ça marchait avant ? Toute modification effectuée récemment. (Comme la mise à niveau, l'installation du correctif sur ISE / la mise à niveau sur DC)
2. La connexion test fonctionne-t-elle correctement (avant l'intégration, vérifiez la connexion test) ?
3. Détails sur le nom d'utilisateur utilisé pour joindre AD et le nom d'utilisateur utilisé pour WMI (compte administrateur ou non administrateur)
4. Vérifiez si les événements (4768, 4770) dans DC sont consignés. (Journal de l'Observateur d'événements du DC)
5. Journaux de capture : Définissez le niveau de débogage pour l'ID passif et la journalisation du runtime, puis exécutez config wmi pour ce DC, AD - niveau de trace avec horodatage.

Service Syslog PassiveID

Le service Syslog PassiveID est un service qui active la fonctionnalité de profilage PassiveID pour

collecter et traiter les messages Syslog des périphériques réseau dans l'environnement. Ces messages syslog contiennent des informations importantes sur les terminaux connectés au réseau, et ISE les utilise pour profiler ces périphériques pour le contrôle d'accès au réseau et l'application des politiques.

Fonctions clés du service Syslog d'ID passif

1. Authentification passive : Le service Passive ID Syslog permet à Cisco ISE d'authentifier passivement les utilisateurs et les périphériques en collectant des messages syslog à partir des périphériques réseau (tels que les commutateurs ou les routeurs) qui indiquent l'activité des utilisateurs et des périphériques. Cela est utile dans les situations où les méthodes d'authentification actives traditionnelles, telles que 802.1X, ne sont pas adaptées ou faisables.

2. Journalisation des événements : Le service Syslog d'ID passif s'appuie sur le protocole Syslog pour recevoir des journaux des périphériques réseau qui suivent l'accès et le comportement des utilisateurs sur le réseau. Les informations contenues dans ces journaux peuvent inclure des informations telles que les tentatives de connexion des périphériques, les points d'accès et les détails de l'interface, qui aident ISE à identifier passivement le périphérique ou l'utilisateur.

Service API PassiveID

Le service d'API PassiveID est un service qui permet l'intégration avec les systèmes qui nécessitent des informations sur l'identité des périphériques ou des utilisateurs connectés au réseau. Il est généralement utilisé dans les environnements où les administrateurs réseau souhaitent appliquer des politiques et des actions basées sur l'identité sans avoir à recourir à des protocoles d'authentification réseau actifs tels que 802.1X pour chaque périphérique.

Fonctions clés du service d'API d'ID passif

1. Intégration aux systèmes externes : L'API d'identification passive permet à ISE de recevoir des informations d'identité de systèmes ou de périphériques réseau tiers (tels que des commutateurs, des routeurs, des pare-feu ou tout système pouvant générer des événements liés à l'identité). Ces systèmes externes peuvent envoyer des informations telles que des messages syslog, des journaux d'authentification ou d'autres données pertinentes qui peuvent aider ISE à identifier passivement un utilisateur ou un périphérique.

2. Authentification passive : Le service d'API d'ID passif est utilisé pour authentifier passivement les utilisateurs et les périphériques en collectant des données d'identité sans nécessiter d'authentification active (par exemple : pas besoin d'authentification 802.1X, MAB ou Web). Par exemple, il peut capturer des informations à partir de périphériques réseau, de journaux Active Directory ou d'appareils de sécurité et les utiliser pour identifier l'utilisateur ou le périphérique.

3. Mappage des informations d'identité : L'API d'ID passif peut être utilisée pour mapper des données d'identité à des stratégies de sécurité spécifiques. Ces informations sont utilisées pour attribuer dynamiquement des balises de groupe de sécurité (SGT) ou des rôles aux utilisateurs et aux périphériques, ce qui influence ensuite l'application des contrôles d'accès au réseau (comme la segmentation et les politiques de pare-feu).

Service d'agent PassiveID

Le service d'agent PassiveID est un service qui permet le profilage des périphériques grâce à l'utilisation d'agents PassiveID installés sur des points d'extrémité (tels que des ordinateurs, des ordinateurs portables, des périphériques mobiles, etc.). L'agent PassiveID permet à ISE de collecter des informations de profilage sur les périphériques du réseau en écoutant le trafic des terminaux, sans nécessiter d'analyses actives ni d'interactions directes avec les périphériques.

Fonctions clés du service d'agent d'ID passif

1. Identification passive des utilisateurs et des périphériques : Le service Passive ID Agent est chargé de collecter passivement des informations relatives aux identités, généralement à partir de périphériques réseau ou de points d'extrémité, et d'envoyer ces données à ISE. Ce service permet à ISE d'authentifier et d'identifier les utilisateurs et les périphériques en fonction de leurs activités ou de leurs caractéristiques, sans avoir besoin d'une authentification active à partir du périphérique (par exemple : sans informations d'identification 802.1X).

2. Intégration avec d'autres composants Cisco : Passive ID Agent travaille en étroite collaboration avec les périphériques réseau Cisco, tels que les commutateurs, les contrôleurs sans fil et les points d'accès, pour collecter des informations relatives à l'identité à partir du trafic réseau, des journaux Syslog ou d'autres systèmes de gestion. Il peut également s'intégrer à Cisco TrustSec et à Cisco Identity Services pour mapper ces données à des balises de groupe de sécurité (SGT) spécifiques ou à d'autres politiques basées sur l'identité.

3. Contrôle d’accès réseau contextuel : Passive ID Agent envoie ces informations à Cisco ISE, qui applique ensuite les stratégies de contrôle d'accès appropriées en fonction de l'identité et du contexte de l'utilisateur ou du périphérique. Cela peut inclure :

- Contrôle d'accès basé sur les rôles.
- Attribution de VLAN dynamique.
- Segmentation du réseau.
- Application des stratégies de sécurité en fonction du rôle de l'utilisateur ou de la position de sécurité du périphérique.

Service de point de terminaison PassiveID

Le service de point de terminaison PassiveID est un service qui est responsable de l'identification et du profilage des points de terminaison (périphériques) sur le réseau basé sur la technologie PassiveID. Ce service aide ISE à collecter, traiter et classer les informations relatives aux périphériques se connectant au réseau, sans nécessiter d'interaction active avec les terminaux eux-mêmes. Le service PassiveID Endpoint joue un rôle essentiel dans le profilage, le contrôle d'accès au réseau et l'application des stratégies de sécurité.

Fonctions clés du service de point de terminaison PassiveID

1. Identification passive des utilisateurs et des périphériques : Le service PassiveID Endpoint permet à Cisco ISE d'identifier et d'authentifier les périphériques sur le réseau de manière

passive, en exploitant les informations provenant de l'activité du réseau ou des journaux système. Cela inclut l'identification des utilisateurs et des périphériques en fonction de leur comportement ou de leurs caractéristiques réseau, telles que l'adresse MAC, l'adresse IP ou les informations de connexion à partir d'un magasin d'identités externe tel qu'Active Directory (AD).

2. Collecte de données à partir des terminaux : Le service de point de terminaison collecte différents types de données spécifiques aux points de terminaison provenant de différentes sources :

- Informations de connexion utilisateur provenant de magasins d'identités externes tels qu'Active Directory ou d'autres répertoires.
- Caractéristiques des périphériques telles que les adresses IP, les adresses MAC et le type de périphérique (par exemple : si le périphérique est un PC Windows, un téléphone portable ou un périphérique IoT).
- Activité du réseau du point d'extrémité, telle que les requêtes DHCP, les requêtes ARP et d'autres communications de couche réseau.

Service SPAN PassiveID

Le service SPAN PassiveID est un service qui exploite la mise en miroir des ports SPAN (Switched Port Analyzer) sur les périphériques réseau pour capturer et analyser le trafic réseau à des fins de profilage des points d'extrémité. Ce service aide ISE à collecter passivement des informations sur les terminaux (périphériques) du réseau en analysant leurs modèles de communication réseau sans nécessiter d'analyseurs ou d'agents actifs installés sur les périphériques eux-mêmes.

Fonctions clés du service PassiveID SPAN

1. Collecte passive des identités à partir du trafic SPAN : Le service PassiveID SPAN permet à ISE de collecter des données d'identité en fonction du trafic réseau mis en miroir ou copié via un port SPAN sur un commutateur. Un port SPAN est généralement utilisé pour la surveillance du réseau en mettant en miroir le trafic réseau provenant d’autres ports ou VLAN. En capturant ce trafic, ISE peut collecter passivement des informations d'identité telles que :

- Adresses MAC des périphériques.
- Adresses IP associées aux périphériques.
- Requêtes DHCP ou autres informations relatives à l'identité à partir du trafic capturé.
- Journaux d'authentification des périphériques réseau, tels que les commutateurs ou les contrôleurs sans fil.

2. Capture des informations d'identité des utilisateurs et des périphériques : Le service SPAN écoute essentiellement le trafic qui traverse le réseau et identifie les informations d'identité clés à partir des paquets du réseau sans avoir à interagir directement avec les périphériques. Il peut s'agir de données telles que :

- Identités des utilisateurs lorsqu'ils s'authentifient via des protocoles tels que EAP (Extensible Authentication Protocol).

- Identités des périphériques basées sur les adresses MAC et IP.
- Rôles et comportements des périphériques en fonction des modèles et des événements de trafic observés.

Vérification et dépannage de la pile PassiveID (service PassiveID SPAN, service PassiveID Syslog, service PassiveID Endpoint, PassiveID Agent, service PassiveID API)

1. La pile PassiveID est une liste de fournisseurs et tous les services de la pile PassiveID sont désactivés par défaut. Accédez à ISE GUI > Administration > Deployment > Sélectionnez le noeud, Enable Passive Identity Service, cliquez sur Save. Pour vérifier l'état du service de pile PassiveID, connectez-vous à l'interface de ligne de commande du noeud ISE et exécutez la commande show application status ise.

2. En cas de problème avec l'agent d'ID passif, vérifiez si le nom de domaine complet de l'agent peut être résolu à partir du noeud ISE. Pour ce faire, connectez-vous à l'interface de ligne de commande ISE et exécutez la commande nslookup < FQDN of Agent configured >.

3. Assurez-vous que le moteur d'indexation ISE est actif et que les recherches DNS inverse et directe sont toutes deux résolues par le serveur DNS ou de noms configuré dans ISE.

4. Pour garantir une communication transparente avec les fournisseurs syslog, vérifiez que les ports UDP 40514 et TCP 1468 sont ouverts sur votre réseau.

5. Pour configurer le fournisseur SPAN sur un noeud, assurez-vous que le service d'identité passive ISE est activé. Vérifiez que l'interface que vous voulez configurer sur le fournisseur SPAN est disponible dans ISE en utilisant la commande show interface de l'interface de ligne de commande ISE.

Pour vérifier les journaux, en fonction du fournisseur d'ID passif, vous devez consulter passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log. Les journaux mentionnés peuvent être sécurisés à partir du bundle de support du noeud ISE.

Serveur DHCP (dhcpd)

Le service DHCP Server (dhcpd) est un service qui fournit la fonctionnalité DHCP (Dynamic Host Configuration Protocol) aux périphériques réseau. Il est principalement utilisé pour attribuer des adresses IP aux périphériques (terminaux) qui tentent de se connecter au réseau. Dans ISE, le serveur DHCP joue un rôle crucial en fournissant des adresses IP aux points d'extrémité qui les demandent lorsqu'ils se connectent au réseau. Le service peut également fournir des informations de configuration supplémentaires, telles que les serveurs DNS, la passerelle par défaut et d'autres paramètres réseau.

Principales fonctions du service de serveur DHCP (dhcpd) dans ISE

1. Attribution dynamique des adresses IP : Le service dhcpd dans ISE fonctionne comme un serveur DHCP, qui fournit l'allocation d'adresses IP pour les périphériques qui demandent une adresse IP lorsqu'ils se connectent au réseau. Ceci est important dans les scénarios où les

périphériques se connectent au réseau de manière dynamique, par exemple dans les environnements BYOD (Bring Your Own Device) ou lorsque les périphériques sont configurés pour obtenir leurs adresses IP automatiquement.

2. DHCP basé sur le profil : Le service dhcpd peut allouer des adresses IP en fonction du profil du périphérique. Si ISE a profilé le périphérique (par exemple : en déterminant qu'il s'agit d'un smartphone, d'un ordinateur portable, d'un périphérique IoT), il peut attribuer une adresse IP appropriée ou appliquer d'autres paramètres en fonction du type de périphérique ou du rôle.

3. Prise en charge du relais DHCP : ISE peut fonctionner en tant qu'agent de relais DHCP et transférer les requêtes DHCP des périphériques vers un serveur DHCP externe si ISE ne gère pas l'attribution d'adresse IP réelle. Dans ce cas, le service dhcpd peut transférer les requêtes des périphériques vers un serveur DHCP central, tandis qu'ISE continue d'appliquer les stratégies réseau et les contrôles d'accès.

Vérification et dépannage du serveur DHCP (dhcpd)

1. Contactez le TAC Cisco pour vérifier si le package de serveur DHCP est installé sur l'ISE.

2. Connectez-vous à la racine de **ISE > rpm -qi dhcp**.

Serveur DNS (nommé)

Le service Serveur DNS (nommé) est un service qui permet à ISE de fonctionner en tant que serveur DNS (Domain Name System) ou résolveur DNS. Il est principalement responsable de la résolution des noms de domaine en adresses IP et vice versa, facilitant ainsi la communication entre les périphériques du réseau.

Fonctions clés du service de serveur DNS (nommé) dans ISE

1. Résolution DNS pour la communication ISE : Le service nommé dans ISE aide à résoudre les noms de domaine en adresses IP. Ceci est particulièrement important lorsque ISE doit se connecter à d'autres périphériques réseau ou services externes (tels que des serveurs Radius, Active Directory ou des serveurs NTP externes) à l'aide de noms de domaine plutôt que d'adresses IP.

- Par exemple, lorsqu'ISE doit atteindre un serveur Radius ou un service d'annuaire externe (comme Active Directory), il doit convertir le nom de domaine de ce serveur en adresse IP.
- ISE interroge le serveur DNS configuré sur le système pour résoudre ces noms de domaine, garantissant ainsi une communication fluide.

2. Résolution DNS pour les services externes : Le service DNS permet à ISE de se connecter à des services externes qui nécessitent des noms de domaine. Par exemple, ISE doit résoudre les noms des services externes tels que :

- Services basés sur le cloud.
- Serveurs NTP (Network Time Protocol).
- Autorités de certification (CA) ou serveurs LDAP.

3. Serveurs DNS multidomaines et redondants : ISE peut être configuré pour utiliser plusieurs serveurs DNS pour la redondance. Si un serveur DNS devient indisponible, ISE peut se rabattre sur un autre serveur DNS pour assurer un fonctionnement continu et une résolution DNS.

Vérification et dépannage du serveur DNS (nommé)

1. À partir de l'interface de ligne de commande du noeud ISE, vérifiez l'accessibilité au serveur de noms ou au serveur DNS du déploiement à l'aide de la commande **ping <IP of DNS server / name server>**.

2. Vérifiez la résolution DNS des FQDN ISE à l'aide de la commande **nslookup <FQDN / IP address of ISE nodes>** via l'interface de ligne de commande ISE.

Service de messagerie ISE

Le service de messagerie ISE est un composant qui facilite la communication asynchrone entre divers services et composants au sein du système ISE. Il joue un rôle crucial dans l'architecture système globale d'ISE, permettant à différentes parties de la plate-forme d'envoyer et de recevoir des messages, de gérer des tâches et de synchroniser des activités.

Fonctions clés du service de messagerie ISE

1. Communication interprocessus (IPC) : Le service de messagerie ISE joue un rôle clé dans l'activation de la communication interprocessus (IPC) entre divers services ISE. Elle garantit que différents modules et services ISE, tels que l'authentification, l'autorisation et l'application des politiques, peuvent échanger des données et des instructions de manière coordonnée.

2. Prise en charge de l'environnement distribué : Dans les déploiements ISE plus importants ou distribués (comme dans les configurations à plusieurs noeuds ou à haute disponibilité), le service de messagerie facilite la communication entre les différents noeuds ISE. Cela garantit que les données, telles que les demandes d'authentification, les sessions utilisateur et les mises à jour de stratégie, sont correctement synchronisées entre les différents noeuds du système ISE.

3. Synchronisation de la stratégie et de la configuration : Le service de messagerie est impliqué dans la synchronisation des configurations et des politiques entre les noeuds ISE. Lorsque des modifications de configuration sont apportées à un noeud principal, le service s'assure que ces modifications sont propagées aux noeuds secondaires ou de sauvegarde du système. Cela est essentiel pour maintenir la cohérence et garantir que les politiques d'accès réseau appliquées sur différents sites ou noeuds ISE distribués restent synchronisées.

Vérifiez que le service de messagerie ISE n'est pas en cours d'exécution ou d'initialisation

1. Vérifiez que le port TCP 8671 n'est pas bloqué dans le pare-feu, car ce port est utilisé pour la communication entre les noeuds entre les périphériques ISE.

2. Vérifiez l'erreur de liaison de file d'attente et, le cas échéant, renouvelez les certificats de messagerie et d'autorité de certification racine ISE, car des erreurs de liaison de file d'attente se produiraient généralement en raison de problèmes d'altération de certificat interne. Pour résoudre les erreurs de liaison de file d'attente, renouvelez la messagerie ISE et le

certificat d'autorité de certification racine ISE en vous reportant à l'article : Erreur de liaison de file d'attente ISE

3. Dans GUI -> Administration -> Certificats -> Sélectionnez ISE Messaging Certificate. Cliquez sur View pour vérifier l'état du certificat.

Les journaux utiles pour dépanner le service de messagerie ISE sont ade.log qui est disponible dans le bundle de support ou peut être adapté via l'interface de ligne de commande en utilisant la commande show logging system ade/ADE.log tail pendant le problème.

4. Si le journal ADE.log affiche rabbitmq : erreurs de refus de connexion, contactez le TAC Cisco pour supprimer le verrou du module Rabbitmq de la racine ISE.

Service de base de données ISE API Gateway

Le service de base de données ISE API Gateway est un composant chargé de gérer et de traiter les données relatives aux demandes et aux réponses d'API au sein du système ISE. Il agit comme un intermédiaire qui connecte la passerelle d'API ISE à la base de données ISE, garantissant que les applications personnalisées peuvent également mettre à jour ou modifier les données au sein d'ISE. (par exemple, ajuster les stratégies d'accès ou ajouter/supprimer des utilisateurs) via des appels d'API gérés par le service.

Fonctions clés du service de base de données de passerelle d'API ISE

1. Accès API aux données ISE : Le service de base de données ISE API Gateway agit comme un pont, permettant aux applications externes d'interagir avec la base de données ISE via les API ISE RESTful. Ces API peuvent être utilisées pour récupérer ou modifier des données stockées dans la base de données ISE, telles que :

- Journaux d'authentification utilisateur.
- Stratégies d'accès réseau.
- Informations de profilage de périphérique.
- Configuration et paramètres du système.

2. Activation des intégrations de systèmes externes : Ce service joue un rôle crucial dans l'intégration d'ISE à des systèmes externes tels que :

- Serveurs d'authentification externes (LDAP, Active Directory, RADIUS).
- Systèmes de gestion de réseau (NMS).
- Solutions SIEM (Security Information and Event Management).
- Applications ou services personnalisés qui doivent interagir avec les données ISE.

En fournissant un accès API, le service de base de données de passerelle API permet à ces systèmes externes d'interroger les données ISE, d'envoyer des mises à jour à ISE ou de déclencher des actions spécifiques au sein d'ISE en réponse à des événements externes.

3. Prise en charge de la communication RESTful API : ISE expose les API RESTful conçues pour fonctionner sur HTTP/HTTPS. Le service de base de données de la passerelle API est chargé de gérer le flux des demandes et des réponses API, de s'assurer que les demandes sont

authentifiées, traitées et que les données appropriées de la base de données ISE sont renvoyées en réponse.

Service de passerelle API ISE

Le service ISE API Gateway est un composant essentiel qui fournit un accès RESTful API aux services, aux données et aux fonctionnalités ISE. Il agit comme un pont entre ISE et les systèmes externes, permettant à ces systèmes d'interagir par programme avec le contrôle d'accès au réseau ISE, l'application des politiques, l'authentification et d'autres services. La passerelle API permet aux applications tierces, aux systèmes de gestion de réseau et aux applications personnalisées d'interagir avec Cisco ISE sans intervention manuelle ni accès direct à l'interface utilisateur ISE.

Fonctions clés du service de passerelle d'API ISE

1. Activation de l'accès API à ISE : Le service de passerelle d'API ISE permet aux systèmes externes d'accéder et d'interagir en toute sécurité avec les données et les politiques Cisco ISE à l'aide des API RESTful. Cela fournit un accès par programme aux fonctionnalités ISE, telles que l'authentification, l'application des politiques, la gestion des sessions, etc.

2. Fournir un contrôle programmatique : Le service de passerelle API permet un contrôle par programmation des fonctions ISE. Les administrateurs et les développeurs peuvent utiliser des API pour :

- Récupérez ou modifiez les stratégies réseau.
- Interroger ou gérer les sessions utilisateur et les journaux d'authentification.
- Créez et gérez des règles de contrôle d'accès au réseau.
- Accéder aux profils de périphérique ou les mettre à jour.

Ce contrôle peut être utilisé pour l'automatisation ou l'orchestration personnalisée des workflows, par exemple pour l'ajustement dynamique des politiques d'accès au réseau en fonction des données en temps réel ou pour l'intégration d'ISE dans une plate-forme d'automatisation de la sécurité plus large.

3. Surveillance et établissement de rapports : Le service de passerelle API permet aux systèmes externes de collecter des données à partir des journaux ISE opérationnels, de l'historique des sessions et des détails d'application des politiques. Ceci est important pour :

- Rapports de conformité.
- Surveillance de la sécurité.
- Réponse aux incidents.

Les appels d'API peuvent être utilisés pour extraire des journaux, des informations d'audit et des événements, ce qui permet aux équipes de sécurité de surveiller les activités ISE à partir d'un tableau de bord ou d'un outil de reporting centralisé.

Vérification et dépannage du service de passerelle d'API ISE et du service de base de données de

passerelle d'API ISE

1. Vérifiez si le certificat d'administration du noeud ISE est actif et valide. Accédez à Administration > Certificates > Select the node > Select Admin Certificate. Cliquez sur View (Afficher) pour vérifier l'état du certificat d'administration du noeud ISE.

2. Configurez les composants ise-api-gateway, api-gateway et apiservice pour le débogage et les journaux peuvent être adaptés à l'aide des commandes suivantes :

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

Service direct ISE pxGrid

Le service direct pxGrid ISE est un composant essentiel qui prend en charge la fonctionnalité pxGrid (Platform Exchange Grid) dans ISE. pxGrid est une technologie Cisco qui facilite le partage et l'intégration de données sécurisées, standardisées et évolutives entre les solutions de sécurité réseau Cisco et les applications, services et périphériques tiers. Le service direct ISE pxGrid permet une communication directe entre ISE et d'autres systèmes compatibles pxGrid sans nécessiter de périphériques ou de services intermédiaires.

Fonctions clés du service direct ISE pxGrid

1. Intégration directe aux systèmes tiers : Le service direct ISE pxGrid permet à ISE de s'intégrer directement à des systèmes de sécurité réseau tiers, tels que des pare-feu, des routeurs, des solutions NAC, des plates-formes SIEM et d'autres dispositifs de sécurité. Il permet à ces systèmes d'échanger des informations sur les événements d'accès au réseau, les incidents de sécurité et les données réseau contextuelles.

2. Partage de contexte : L'une des principales fonctions de pxGrid est le partage d'informations contextuelles (telles que les identités des périphériques, les rôles des utilisateurs, la position de sécurité et les informations d'accès au réseau). Avec le service direct pxGrid, ISE peut partager directement ce contexte avec d'autres périphériques ou applications sans recourir à des méthodes traditionnelles telles que RADIUS ou TACACS+.

3. Communication simplifiée : Grâce à pxGrid, ISE peut communiquer et échanger des informations avec des solutions tierces à l'aide d'un protocole normalisé. Cela simplifie le processus d'intégration, car les systèmes n'ont pas besoin d'avoir des intégrations personnalisées pour chaque solution tierce.

4. Sécurité et conformité améliorées : Le service direct pxGrid améliore également la sécurité et la conformité en garantissant que tous les systèmes de l'écosystème réseau ont accès aux mêmes données contextuelles en temps réel sur les utilisateurs, les périphériques et les politiques de sécurité. Cela garantit une application plus coordonnée des politiques de sécurité du réseau dans l'ensemble de l'environnement.

Vérification et dépannage du service direct ISEPxgrid

1. Contactez le TAC Cisco pour vérifier si **edda*.lock*** est présent dans le dossier /tmp. Si oui, le TAC Cisco supprime le verrou et redémarre le service Pxgrid Direct à partir de la racine.

2. Configurez le composant **PxGrid Direct** pour le débogage dans le noeud ISE pour le dépannage. Les journaux peuvent être sécurisés via l'offre groupée de support ISE ou l'interface de ligne de commande ISE à l'aide des commandes suivantes :

show logging application pxgriddirect-service.log

show logging application pxgriddirect-connector.log

Les journaux mentionnés fournissent des informations sur les données de terminaux récupérées et reçues par Cisco ISE, ainsi que sur l'état de connectivité du connecteur Pxgrid.

Service Politique de segmentation

Le Service de politiques de segmentation est un composant clé chargé d'appliquer les politiques de segmentation du réseau en fonction de l'identité de l'utilisateur, de la position du périphérique ou d'autres informations contextuelles. Elle permet de contrôler l'accès des utilisateurs et des périphériques à des segments de réseau spécifiques, garantissant que seuls les utilisateurs autorisés ou les périphériques conformes peuvent accéder à certaines parties du réseau. La segmentation du réseau est essentielle pour réduire la surface d'attaque du réseau, empêcher le déplacement latéral des menaces et garantir la conformité aux réglementations. Le service de politique de segmentation d'ISE est utilisé pour appliquer ces règles de segmentation du réseau de manière dynamique et flexible sur l'ensemble du réseau.

Fonctions clés du service de stratégie de segmentation

1. Définition des segments de réseau : Le service de politique de segmentation d'ISE permet aux administrateurs de définir divers segments de réseau (sous-réseaux ou VLAN) en fonction des caractéristiques des utilisateurs ou des périphériques. Exemple :

- Les périphériques présentant des positions de sécurité différentes peuvent être affectés à des segments différents (par exemple : les périphériques sécurisés d'un VLAN et les périphériques non sécurisés d'un autre).
- Des utilisateurs de différents services ou rôles peuvent être affectés à différents segments de réseau pour appliquer les privilèges les plus faibles et limiter l'accès aux ressources sensibles.

2. Segmentation dynamique : Ce service permet la segmentation dynamique du réseau, ce qui signifie que les segments de réseau ou les VLAN peuvent changer en fonction des conditions en temps réel. Exemple :

- Un utilisateur peut être affecté à un VLAN spécifique en fonction de son rôle ou de l'état de santé de son périphérique.
- Un périphérique jugé non conforme ou exécutant un système d'exploitation obsolète peut être déplacé vers un VLAN de quarantaine ou invité jusqu'à ce qu'il soit corrigé.

3. Application des politiques : Le service de stratégie de segmentation utilise des stratégies pour prendre des décisions sur le segment dans lequel un périphérique ou un utilisateur doit être placé. Ces politiques peuvent tenir compte de divers facteurs, notamment :

- Identité utilisateur : En fonction du rôle ou des attributs de l'utilisateur.
- Posture du périphérique : L'état de santé ou de conformité du périphérique (par exemple : exécute-t-il le dernier logiciel antivirus ?).
- Emplacement: L'emplacement physique de l'utilisateur ou du périphérique sur le réseau (par exemple : bureau, zone réservée aux invités, accès à distance).
- Heure d'accès : L'heure ou le jour de la semaine où la demande d'accès est effectuée.

4. Application des politiques de sécurité : Le service de politique de segmentation garantit que les politiques de sécurité sont appliquées de manière cohérente sur les périphériques réseau (tels que les commutateurs, les routeurs, les pare-feu) en exploitant les normes industrielles telles que RADIUS et l'attribution de VLAN. Cela permet à Cisco ISE de communiquer avec les périphériques de l'infrastructure réseau pour appliquer les politiques de segmentation requises.

Vérification et dépannage du service de stratégie de segmentation

1. Vérifiez que la segmentation est correctement configurée en accédant à Work Centers > TrustSec > Overview > Dashboard.

2. Work Centers > TrustSec > Reports, sélectionnez Rapports TrustSec pour vérifier l'état et les rapports du service de stratégie de segmentation.

Service d'authentification REST

Le service d'authentification REST est un service qui fournit des fonctionnalités d'authentification à l'aide des API RESTful. Il permet aux applications et systèmes externes d'authentifier les utilisateurs ou les périphériques en interagissant avec ISE sur HTTP(S) à l'aide des protocoles REST standard. Ce service permet une intégration transparente de la fonctionnalité d'authentification Cisco ISE avec des applications ou des systèmes tiers qui doivent authentifier les utilisateurs ou les périphériques, mais ne peuvent pas utiliser les méthodes traditionnelles (telles que RADIUS ou TACACS+).

Fonctions clés du service d'authentification REST

1. Authentification RESTful : Le service d'authentification REST active les demandes d'authentification sur le protocole REST API. Cela permet des systèmes externes (Par exemple : applications, périphériques réseau tiers ou services) pour authentifier les utilisateurs ou les périphériques utilisant ISE comme serveur d'authentification, mais par le biais d'appels de service Web RESTful plutôt que par le biais de protocoles d'authentification traditionnels tels que RADIUS ou TACACS+.

2. Intégration aux applications externes : Ce service est conçu pour les applications externes qui doivent authentifier des utilisateurs ou des périphériques, mais qui n'utilisent pas les méthodes d'authentification traditionnelles (telles que RADIUS ou TACACS+). Au lieu de cela, ils peuvent

interagir avec ISE via des API REST, ce qui simplifie l'intégration de l'authentification ISE dans des applications Web ou cloud.

3. Authentification flexible et évolutive : Le service d'authentification REST fournit une méthode d'authentification évolutive qui n'est pas limitée aux périphériques réseau ou aux solutions sur site. Il peut être utilisé par les services cloud, les applications mobiles et d'autres plates-formes Web qui ont besoin d'authentifier des utilisateurs ou des périphériques en interrogeant ISE pour obtenir des informations d'identification et des politiques.

4. Facile à appliquer : L'API REST offre une interface standardisée, plus facile à appliquer et à intégrer avec les logiciels et applications modernes par rapport aux méthodes traditionnelles. Il fournit des réponses au format JSON et utilise des méthodes HTTP telles que GET, POST, PUT et DELETE, ce qui le rend plus accessible pour les développeurs Web et les systèmes intégrant ISE pour l'authentification.

Vérification et dépannage de Rest Auth

1. Pour résoudre les problèmes liés à l'API ouverte, configurez un composant apiserservice sur debug.

2. Pour résoudre les problèmes liés à l'API ERS, configurez le composant ers sur debug.

Si la page GUI du service API : https://{iseip}:{port}/api/swagger-ui/index.html ou https://{iseip}:9060/ers/sdk est accessible, il conclut que le service API fonctionne comme prévu.

Référez-vous à Documentation API pour plus d'informations sur l'API.

Connecteur SSE

Le connecteur SSE (Secure Software-Defined Edge Connector) est un service qui intègre ISE à la solution Cisco Secure Software-Defined Access (SD-Access). Le connecteur SSE permet à ISE de communiquer en toute sécurité avec Cisco DNA Center, ce qui permet d'automatiser les politiques réseau, la segmentation et la gestion de la sécurité de périphérie dans un environnement SD-Access.

Principales fonctions du connecteur SSE

1. Intégration aux systèmes de sécurité tiers : Le connecteur SSE facilite l'intégration de Cisco ISE avec des systèmes de sécurité tiers tels que des pare-feu, des systèmes de prévention des intrusions (IPS), des solutions de contrôle d'accès au réseau (NAC) et des systèmes de gestion des informations et des événements de sécurité (SIEM). Il permet à ces systèmes externes d'envoyer ou de recevoir des données d'ISE de manière sécurisée, ce qui peut être utilisé pour une application plus dynamique des politiques.

2. Informations en temps réel sur les menaces : En connectant ISE à d'autres systèmes de sécurité, le connecteur SSE permet l'échange d'informations en temps réel sur les menaces. Ces informations peuvent inclure des activités suspectes, des terminaux compromis ou des comportements malveillants détectés par d'autres systèmes de sécurité, ce qui permet à ISE

d'ajuster dynamiquement les stratégies d'accès en fonction des niveaux de menace ou de l'état des périphériques actuels.

3. Correction automatisée : L'intégration activée par le connecteur SSE peut prendre en charge les workflows de résolution automatisés. Par exemple, si un système est signalé comme compromis par un dispositif de sécurité externe, ISE peut automatiquement appliquer des politiques qui bloquent l'accès au réseau ou rediriger le point d'extrémité vers un segment de réseau de conversion pour une étude plus approfondie.

Vérification et dépannage du connecteur SSE

1. Le connecteur SSE est activé uniquement lorsque le service PassiveID est activé dans ISE.

2. Le composant sse-connector (connector.log) dans debug fournit plus d'informations sur les messages associés au connecteur SSE.

Hermes (agent cloud pxGrid)

Hermes (pxGrid Cloud Agent) est un composant qui facilite l'intégration entre ISE et l'écosystème pxGrid (Platform Exchange Grid) dans un environnement cloud. Hermes est l'agent basé sur le cloud utilisé pour permettre la communication entre ISE et les services ou plates-formes basés sur le cloud, prenant en charge le cadre pxGrid pour le partage d'informations contextuelles sur différents systèmes de réseau et de sécurité.

Principales caractéristiques et fonctions de Hermes (pxGrid Cloud Agent)

1. Intégration du cloud sur site : Hermes (pxGrid Cloud Agent) est conçu pour faciliter l'intégration transparente entre les services cloud et l'infrastructure ISE sur site. Il étend la puissance de pxGrid au-delà des environnements réseau sur site traditionnels, permettant l'échange sécurisé de données et l'application de politiques sur les applications et les services cloud.

2. Prise en charge de l'écosystème pxGrid : pxGrid est une plate-forme Cisco permettant de partager en toute sécurité le contexte et les informations entre les solutions de sécurité réseau. Hermes agit en tant qu'agent cloud pour pxGrid, permettant une communication sécurisée en temps réel entre ISE et divers services cloud. Cette intégration permet aux politiques de sécurité du réseau d'être cohérentes à la fois sur site et dans les environnements cloud, ce qui facilite la gestion et l'application de la sécurité.

3. Visibilité des terminaux sur le cloud : L'un des principaux avantages de Hermes est qu'il offre une visibilité sur les terminaux basés sur le cloud, de la même manière qu'ISE offre une visibilité sur les terminaux sur site. Il peut collecter des données sur les appareils et les utilisateurs dans le cloud, telles que leur état de conformité, leur état de sécurité et leurs informations d'identité. Cela permet à ISE d'appliquer des politiques d'accès réseau sur les terminaux cloud, tout comme pour les périphériques sur site.

4. Extension transparente d'ISE aux environnements cloud : L'un des principaux avantages de Hermes est qu'il fournit un pont transparent entre l'environnement ISE sur site et le nombre

croissant d'applications natives dans le cloud. Il est ainsi plus facile d'étendre les politiques de sécurité ISE, les méthodes d'authentification et les contrôles d'accès aux services cloud sans avoir à revoir complètement l'infrastructure existante.

Vérification et dépannage de Hermes (Pxgrid Cloud Agent)

1. Par défaut, le service Hermes est désactivé, la connexion d'ISE au cloud Cisco PxGrid active le service Hermes. Par conséquent, si le service Hermes est désactivé dans ISE, vérifiez si l'option Cloud Pxgrid est activée dans **ISE GUI > Administration > Deployment, sélectionnez ISE node**. Modifier , **activer Pxgrid Cloud.**

2. Les débogages utiles pour le dépannage des problèmes liés au nuage Pxgrid sont **hermes.log** et **pxcloud.log**. Ces débogages sont disponibles uniquement sur le noeud Pxgrid où le nuage Pxgrid est activé.

McTrust (Service de synchronisation Meraki)

McTrust (Meraki Sync Service) est un service qui permet l'intégration entre les systèmes Cisco ISE et Cisco Meraki, en particulier pour la synchronisation et la gestion des périphériques réseau et des politiques d'accès. Le service McTrust agit comme un connecteur qui synchronise les informations relatives aux utilisateurs et aux périphériques entre l'infrastructure réseau gérée dans le cloud de Meraki et les systèmes de gestion des politiques et des identités ISE sur site.

Principales caractéristiques et fonctions de McTrust (service Meraki Sync)

1. Intégration transparente aux périphériques Meraki : McTrust permet à ISE de se synchroniser et de s'intégrer avec les appareils gérés dans le cloud de Meraki. Cela inclut les périphériques tels que les points d'accès, les commutateurs et les appareils de sécurité Meraki qui font partie de la gamme Meraki. Elle permet à ISE de communiquer directement avec l'infrastructure de Meraki, ce qui facilite l'application des politiques de contrôle d'accès au réseau aux périphériques gérés par Meraki.

2. Synchronisation automatique des périphériques : Le service Meraki Sync synchronise automatiquement les politiques ISE avec les périphériques réseau Meraki. Cela signifie que toutes les modifications apportées aux politiques de contrôle d'accès au réseau dans ISE sont automatiquement répercutées sur les périphériques Meraki, sans nécessiter d'intervention manuelle. Les administrateurs peuvent ainsi gérer plus facilement l'accès au réseau sur les plates-formes Meraki et ISE.

3. Application des politiques relatives aux périphériques gérés par Meraki : McTrust permet à ISE d'appliquer des politiques d'accès réseau sur les appareils Meraki en fonction de l'authentification et de la position des appareils. Il peut attribuer dynamiquement des politiques aux éléments du réseau Meraki, par exemple pour ajuster les attributions de VLAN, appliquer des listes de contrôle d'accès (ACL) ou restreindre l'accès à certaines ressources du réseau, selon la position de sécurité du périphérique ou de l'utilisateur demandant l'accès.

4. Intégration du tableau de bord Meraki : McTrust intègre directement ISE au tableau de bord Meraki, offrant ainsi une interface de gestion unifiée. Grâce à cette intégration, les administrateurs peuvent visualiser et gérer les politiques réseau et les règles de contrôle d'accès pour les

périphériques Meraki et les ressources gérées par ISE, le tout depuis l'interface gérée dans le cloud de Meraki.

Vérification et dépannage de McTrust (service de synchronisation Meraki)

1. Connectez-vous à l'interface utilisateur graphique ISE -> Work Centers -> TrustSec -> Integrations -> Sync status. Vérifiez les problèmes/erreurs observés.

2. Assurez-vous que tous les certificats d'administration des noeuds ISE sont actifs et valides.

Le débogage utile pour le dépannage du service de synchronisation Meraki est meraki-connector.log.

Exportateur de noeuds ISE

Le service ISE Node Exporter est un composant utilisé pour surveiller et collecter les mesures de performances du système ISE, en particulier des noeuds ISE (qu'il s'agisse de noeuds d'administration, de noeuds de surveillance ou de noeuds de service de stratégie).

Principales caractéristiques et fonctions d'ISE Node Exporter

1.Exportation des mesures : ISE Node Exporter fournit divers indicateurs liés aux performances, tels que l'utilisation du processeur, l'utilisation de la mémoire, l'utilisation des disques, les statistiques réseau, la charge du système et d'autres indicateurs de niveau système d'exploitation. Ces mesures sont ensuite utilisées pour surveiller l'état et les performances du noeud ISE et peuvent être visualisées dans un tableau de bord de surveillance tel que Grafana.

2. Surveillance de l'état du système : En exportant les données de performances vers Prometheus, l'exportateur de noeuds ISE permet une surveillance continue de l'état et de l'état opérationnel du noeud ISE. Les administrateurs peuvent créer des alertes basées sur des seuils prédéfinis pour les avertir de la dégradation des performances ou de problèmes système.

3. Intégration de Prometheus : ISE Node Exporter est généralement utilisé en association avec Prometheus, une boîte à outils open source de surveillance et d'alerte conçue pour la fiabilité et l'évolutivité. L'exportateur de noeuds expose des mesures au niveau du système qui peuvent être récupérées par Prometheus pour collecter et stocker des données de séries chronologiques.

Service Prometheus ISE

Le service ISE Prometheus est un service qui intègre Prometheus à ISE pour permettre la surveillance et la collecte de mesures de performances à partir du système ISE. Prometheus est une boîte à outils open source de surveillance et d'alerte utilisée pour collecter, stocker et analyser des données chronologiques. Le service ISE Prometheus permet à ISE d'exposer ses métriques internes à Prometheus à des fins de surveillance.

Principales caractéristiques et fonctions du service Prometheus ISE

1. Collecte de mesures pour la surveillance : Le service Prometheus ISE est conçu pour exporter divers indicateurs de fonctionnement et de performances liés au système ISE. Ces mesures incluent généralement, sans s'y limiter, l'utilisation du processeur et la charge système, l'utilisation de la mémoire, l'utilisation du disque et les performances d'E/S, les statistiques réseau, les statistiques de demande d'authentification, les statistiques d'application des politiques, l'état du système et les données de temps de fonctionnement

2. Intégration de Prometheus : Le service Prometheus permet à ISE d'exposer les données dans un format compatible avec Prometheus, qui les supprime à intervalles réguliers. Prometheus stocke ensuite les données dans une base de données chronologique, ce qui permet de suivre les tendances et les performances historiques du système ISE.

3. Visualisation et signalement avec Grafana : Le service Prometheus d'ISE s'intègre parfaitement à Grafana, un outil de visualisation open source très répandu. Après avoir exporté les mesures vers Prometheus, les administrateurs peuvent utiliser les tableaux de bord Grafana pour visualiser les données en temps réel. Cela permet d'identifier facilement les goulets d'étranglement des performances, les tendances du système et les problèmes potentiels dans le déploiement ISE.

Service ISE Grafana

Le service ISE Grafana est un service qui permet de visualiser les mesures de performances du système à l'aide de Grafana, une plate-forme open source de surveillance et de visualisation des données. Il s'intègre à Prometheus pour afficher des données historiques et en temps réel collectées à partir d'ISE, ce qui permet aux administrateurs de créer des tableaux de bord interactifs qui fournissent des informations sur l'état, les performances et l'utilisation du système ISE.

Principales caractéristiques et fonctions du service ISE Grafana

1. Tableaux de bord personnalisables : Grafana est hautement personnalisable, ce qui permet aux administrateurs de créer et de modifier des tableaux de bord en fonction de leurs besoins de surveillance spécifiques. Des requêtes personnalisées peuvent être créées pour extraire des points de données spécifiques de Prometheus, et ces requêtes peuvent être visualisées dans divers formats tels que des graphiques, des tableaux, des heatmaps, etc.

2. Surveillance centralisée pour les déploiements ISE distribués : Pour les déploiements ISE distribués, où plusieurs noeuds ISE sont déployés sur différents sites, Grafana fournit une vue centralisée de toutes les mesures système collectées à partir de chaque noeud. Cela permet aux administrateurs de surveiller les performances de l'ensemble du déploiement ISE à partir d'un seul emplacement.

3. Données historiques et analyse des tendances : Grâce aux données stockées dans Prometheus, Grafana permet une analyse historique des mesures système, permettant aux administrateurs de suivre les tendances dans le temps. Par exemple, ils peuvent surveiller l'évolution de l'utilisation du processeur au cours du dernier mois ou la fluctuation des taux de réussite de l'authentification. Ces données historiques sont précieuses pour la planification des capacités, l'analyse des tendances et l'identification des problèmes à long terme.

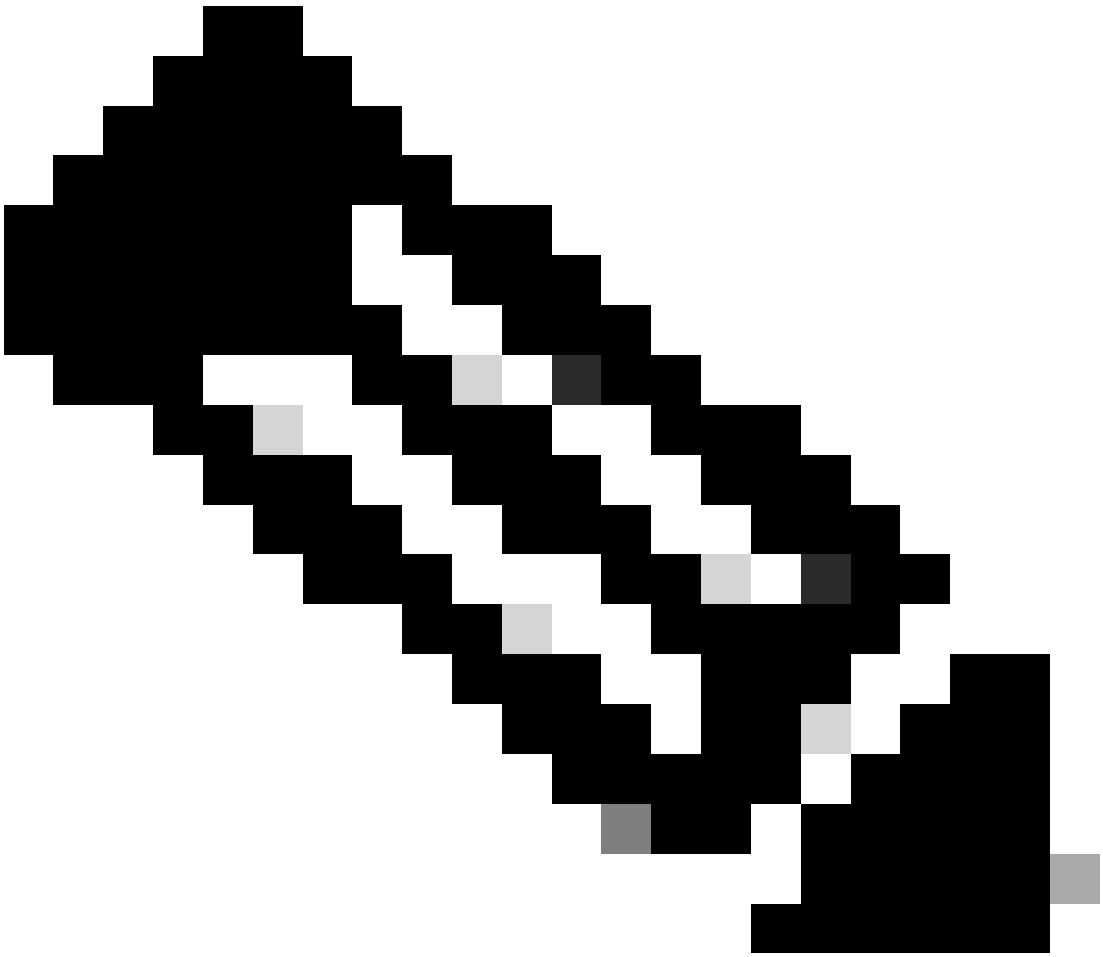
Vérification et dépannage du service ISE Grafana, du service ISE Prometheus, de l'exportateur de noeuds ISE

1. Le service ISE Grafana, le service ISE Prometheus et le service ISE Node Exporter fonctionnent ensemble et sont appelés les services Grafana Stack. Il n'existe aucun débogage spécifique à activer pour le dépannage de ces services. Cependant, ces commandes aident à résoudre les problèmes.

show logging application ise-prometheus/prometheus.log

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

show logging application ise-grafana/grafana.log



Remarque : Lorsque la surveillance est activée, ISE Node Exporter, ISE Prometheus Service et ISE Grafana Service doivent être en cours d'exécution et toute interruption de ces services peut entraîner des problèmes lors de la collecte des données.

ISE MNT LogAnalytics Elasticsearch

Le composant Elasticsearch d'ISE MNT LogAnalytics est un composant qui intègre Elasticsearch aux fonctionnalités de surveillance et de dépannage (MNT) d'ISE. Il est utilisé pour l'agrégation, la recherche et l'analyse des journaux et des événements ISE. Elasticsearch est un moteur de recherche et d'analyse distribué largement utilisé. Intégré à ISE, il améliore la capacité du système à stocker, analyser et visualiser les données de journal générées par les composants ISE.

Principales caractéristiques et fonctions de l'analyse des journaux ISE MNT

1. Stockage et indexation des journaux : Le service Elasticsearch d'ISE est chargé de stocker et d'indexer les données de journal générées par ISE. Elasticsearch est un moteur de recherche et d'analyse distribué qui permet de stocker les journaux ISE de manière à accélérer la recherche, l'interrogation et la récupération d'événements, d'erreurs ou d'activités système spécifiques.

2. Intégration avec Log Analytics : ISE MNT LogAnalytics Elasticsearch fonctionne avec Log Analytics pour fournir une solution de journalisation complète. Elle permet à ISE de collecter des données de journal liées à l'authentification, à l'application des politiques, aux opérations système et à d'autres activités. Ces données sont stockées dans Elasticsearch, ce qui facilite l'exécution d'analyses détaillées et l'obtention d'informations sur le comportement d'ISE.

3. Journalisation centralisée : En s'intégrant à Elasticsearch, ISE fournit une solution de journalisation centralisée, essentielle pour les environnements nécessitant une collecte de journaux distribuée. Cela permet aux administrateurs d'afficher et d'analyser les journaux de plusieurs noeuds ISE dans une seule interface unifiée, ce qui facilite le dépannage et la surveillance des performances ISE.

4. Analyse et dépannage des journaux : Le service de recherche élastique ISE MNT LogAnalytics aide les administrateurs à analyser le comportement du système et à résoudre les problèmes en rendant les données de journal facilement accessibles. Par exemple, en cas de pic soudain d'échecs d'authentification ou de panne système inattendue, la fonction Elasticsearch permet d'interroger rapidement les données du journal afin d'identifier la cause première.

Vérifier et dépanner le logAnalytics d'ISE M&T Elasticsearch

1. La désactivation et la réactivation du service d'analyse des journaux dans ISE doivent être utiles. Accédez à Operations > System 360 > Settings > Log analytics (disable and enable by using toggle option).

2. Le redémarrage de M&T LogAnalytics depuis la racine ISE résout le problème. Contactez le TAC Cisco pour effectuer cette action.

Défauts connus

ID de bogue Cisco ·66198

Service ISE Logstash

ISE Logstash Service est un composant qui intègre Logstash, un pipeline de traitement de données open source, avec ISE pour la collecte, la transformation et le transfert de journaux.

Logstash agit comme un collecteur et un redirecteur de journaux, permettant le traitement des journaux ISE et leur envoi à d'autres systèmes pour analyse, stockage et surveillance. Logstash est un puissant outil open source qui collecte, analyse et transmet des journaux ou d'autres données provenant de différentes sources vers un emplacement central pour le stockage, l'analyse et la visualisation. Dans le contexte d'ISE, le service ISE Logstash est utilisé pour traiter et transférer les journaux dans un format structuré vers un système de journalisation centralisé, où ils peuvent être analysés, surveillés et visualisés.

Principales caractéristiques et fonctions du service ISE Logstash

1. Collecte et transfert des journaux : La fonction principale du service de journalisation ISE est de collecter des données de journal à partir de divers composants ISE (tels que les journaux d'authentification, les journaux système, les journaux d'application des politiques, etc.) et de les transférer vers un emplacement central (généralement Elasticsearch ou un autre système de gestion des journaux) pour le stockage et l'analyse.

2. Analyse du journal : Logstash peut analyser les journaux collectés dans des formats structurés. Il traite les données de journal brutes et en extrait des informations significatives, transformant les entrées de journal dans un format plus facile à interroger et à analyser. Cela peut impliquer le filtrage, l'analyse et l'enrichissement des données avant de les transmettre à Elasticsearch ou à d'autres systèmes.

Vérifier et dépanner le service de vidange ISE

1. Aucun débogage spécifique à activer. Cependant, **show logging application ise-logstash/logstash.log** fournit des informations sur l'état du service.

2. La désactivation et la réactivation du service d'analyse des journaux dans ISE doivent être utiles. Accédez à **Operations > System 360 > Settings > Log analytics** (disable and enable by using toggle option).

Défauts connus liés au service Logstash

ID de bogue Cisco ·74832

ID de bogue Cisco ·58596

Service ISE Kibana

ISE Kibana Service est un composant qui intègre Kibana, un outil de visualisation de données open source, à l'infrastructure de journalisation et de surveillance ISE. Kibana travaille en tandem avec Elasticsearch (qui stocke et indexe les données des journaux) pour fournir une puissante plate-forme de visualisation, de recherche et d'analyse des journaux ISE et des mesures de performances.

Principales caractéristiques et fonctions du service ISE Kibana

1. Visualisation des données : Le service ISE Kibana permet aux administrateurs de créer des

représentations visuelles des données de journal collectées auprès d'ISE. Cela peut inclure :

- Graphiques, graphiques et tableaux indiquant les tendances en matière d'authentification, d'application des stratégies, d'activité des utilisateurs et d'intégrité du système.
- Graphiques à secteurs, graphiques linéaires et graphiques à barres pour suivre des mesures spécifiques telles que le nombre d'échecs de connexion, la durée de la session ou les erreurs au fil du temps.

Vérification et dépannage du service ISE Kibana

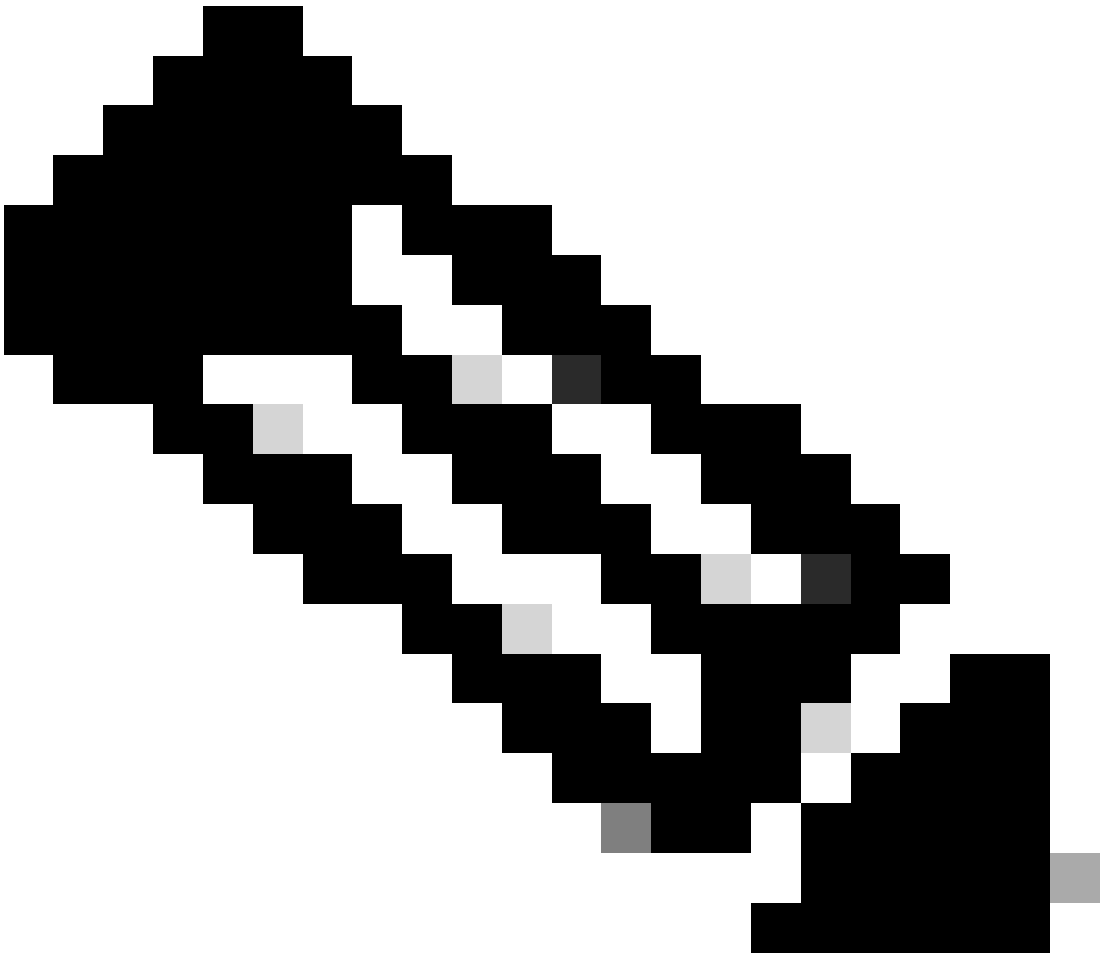
1. Si le service de kibana ISE n'est pas en cours d'exécution, désactivez et réactivez l'analyse des journaux dans ISE, accédez à Operations > System 360 > Settings, Log analytics (disable and enable by using toggle option).

2. Dans de nombreux scénarios, il peut y avoir une entrée dupliquée dans le dossier /etc/hosts qui doit causer un problème. Contactez le TAC pour supprimer l'entrée en double.

Défauts connus liés au problème de Kibana

ID de bogue Cisco ·78050

ID de bogue Cisco ·59848



Remarque : Lorsque Log Analytics est activé, ISE MNT LogAnalytics Elasticsearch, ISE Logstash Service, ISE Kibana Service doivent être en cours d'exécution et l'interruption de l'un de ces services crée des problèmes lors de la collecte des données.

Service IPSec natif ISE

Le service IPSec natif ISE fait référence à la prise en charge intégrée d'IPSec (Internet Protocol Security), qui assure une communication sécurisée entre les noeuds ISE ou entre ISE et d'autres périphériques réseau. IPSec est une suite de protocoles utilisés pour sécuriser les communications réseau en authentifiant et en chiffrant chaque paquet IP au cours d'une session de communication.Le service IPSec natif fait partie du cadre plus large de sécurité et de gestion de l'accès au réseau. Il offre des fonctionnalités de gestion et de gestion des connexions VPN IPsec, garantissant que les données transmises entre le système ISE et les terminaux distants sont sécurisées. Cela peut impliquer des interactions avec des périphériques clients, des périphériques d'accès réseau (tels que des routeurs ou des pare-feu) ou même d'autres noeuds ISE, où le cryptage et la tunnellisation IPsec sont nécessaires pour sécuriser les informations sensibles.

Principales caractéristiques et fonctions du service IPSec natif ISE

1. Communication sécurisée via IPsec : La fonction principale du service IPSec natif ISE est d'établir et de maintenir des canaux de communication sécurisés à l'aide d'IPsec. Cela implique l'utilisation de mécanismes de chiffrement et d'authentification pour garantir que les données transmises entre ISE et d'autres périphériques sont protégées contre l'interception, la falsification et l'accès non autorisé.

2. Connectivité VPN IPsec : Le service IPSec natif ISE facilite les connexions VPN qui utilisent le protocole IPsec pour fournir un tunnel sécurisé et chiffré pour la transmission des données. Cela est particulièrement utile pour les travailleurs distants, les filiales ou d'autres sites ayant besoin d'accéder en toute sécurité à l'environnement ISE sur des réseaux non fiables (tels qu'Internet).

3. Prise en charge du VPN d’accès à distance : Le service IPSec natif peut être impliqué dans des configurations VPN d'accès à distance, où des utilisateurs ou des périphériques situés hors site (tels que des employés distants ou des filiales) se connectent en toute sécurité au système ISE via des tunnels IPsec. Ce service garantit que tout le trafic d'accès à distance est chiffré et authentifié avant d'atteindre l'environnement ISE.

4.Compatibilité du client VPN IPsec : Le service IPSec natif ISE assure la compatibilité avec les clients VPN IPsec. Il prend en charge les configurations client courantes, ce qui permet aux périphériques de se connecter au réseau en toute sécurité sans exposer les données sensibles à des risques.

Vérification et dépannage du service IPSec natif

1. Aucun débogage spécifique à activer pour le service IPSec natif. Vérifiez les journaux à l'aide de la commande show logging application strongswan/charon.log tail via l'interface de ligne de commande ISE.

2. Si un problème est observé pour le tunnel, vérifiez l'état de l'établissement du tunnel via GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec.

MFC Profiler

Le profileur MFC est un composant spécialisé utilisé pour profiler les périphériques réseau et les terminaux. Le profilage est un élément clé du contrôle d'accès au réseau, car il permet à ISE d'identifier les périphériques sur le réseau, de les classer et d'appliquer les politiques réseau appropriées en fonction du type de périphérique et du comportement.

Principales caractéristiques et fonctions du service MFC Profiler dans ISE

1. Profilage du trafic : Le service MFC Profiler d'ISE est responsable de la collecte et du profilage des données de trafic. Il surveille le comportement des terminaux sur le réseau, y compris les types d'applications utilisées, les services auxquels on accède et les modèles de trafic présentés par les périphériques. Ces données permettent de créer un profil pour chaque terminal.

2. Profilage des terminaux : Le service MFC Profiler permet à ISE d'identifier et de classer les terminaux en fonction de leur comportement. Par exemple, il détecte si un terminal est une imprimante, un ordinateur ou un périphérique mobile en fonction des modèles de trafic. Cela permet d'appliquer des politiques plus spécifiques pour différents types de périphériques, améliorant ainsi la sécurité et l'efficacité opérationnelle.

Vérification et dépannage du service de profileur MFC

1. Accédez à Interface utilisateur graphique ISE -> Administration -> Profilage -> Profilage MFC et aux règles AI, vérifiez si le service est activé.

2. Si le service est activé mais s'affiche comme désactivé / non exécuté via la commande show application status ise dans l'interface de ligne de commande ISE. Désactivez et réactivez le service de profilage MFC dans ISE en vous référant à l'étape 1.

Débogages utiles pour le dépannage : Composant du profileur MFC dans le débogage. Les journaux peuvent être vérifiés à partir du bundle de support ou de la queue des journaux en utilisant la commande show logging application ise-pi-profiler.log tail via l'interface de ligne de commande ISE.

Défaut connu du profileur MFC qui s'affiche comme non opérationnel au lieu de l'état désactivé :

ID de bogue Cisco ·72853

Points clés

1. Pour récupérer les services, redémarrez les services à l'aide des commandes application stop ise et application start ise via l'interface de ligne de commande ISE.

2. En cas de problème, assurez-vous qu'un bundle de support est capturé à partir de l'interface utilisateur graphique ISE/de l'interface de ligne de commande ISE pour une vérification plus approfondie du problème. Lien de référence pour la création d'un bundle d'assistance ISE via GUI et CLI : Collect Support Bundle on the Identity Services Engine

3. Si les problèmes sont liés aux ressources, à la moyenne de charge, à l'utilisation du disque, etc., il est obligatoire de collecter le vidage de thread et le vidage de segment de mémoire pour analyse.

4. Avant d'effectuer le rechargement du noeud, contactez le centre d'assistance technique Cisco et fournissez des journaux sécurisés pour une analyse plus approfondie.

Préoccupations standard dans ISE

Outre les problèmes liés aux services ISE, voici quelques-unes des préoccupations rencontrées dans les noeuds ISE, ainsi que les étapes de dépannage de base requises.

Vérification de la charge moyenne élevée, problèmes d'utilisation des ressources (CPU / MÉMOIRE / DISQUE),

ressources insuffisantes

1. Vérifiez que les ressources recommandées par Cisco sont allouées au noeud à l'aide de la commande show inventory via l'interface de ligne de commande ISE.

2. À partir de l'interface de ligne de commande du noeud ISE, exécutez la commande tech top pour vérifier l'utilisation des ressources d'ISE.

3. Vérifiez l'utilisation du disque en utilisant la commande show disk via l'interface de ligne de commande ISE.

4. Purgez les points d'extrémité inactifs, videz le disque local du noeud et effectuez des nettoyages de mise à niveau.

Si le problème persiste, contactez le TAC Cisco et fournissez le bundle d'assistance sécurisé, le vidage de tas et le vidage de thread à partir du noeud qui rencontre le problème.

Pour sécuriser le vidage de tas, connectez-vous à l'interface de ligne de commande du noeud ISE, exécutez la commande **application configure ise**. Sélectionner l'option 22.

Pour sécuriser le thread dump, connectez-vous à l'interface de ligne de commande du noeud ISE, exécutez la commande **application configure ise**, sélectionnez l'**option 23.** Le thread dump est inclus dans le bundle de support ou peut être adapté via l'interface de ligne de commande ISE à l'aide de la commande **show logging application appserver/catalina.out**.

Vérification et dépannage des problèmes de surveillance

La fonction de surveillance et de dépannage (MnT) d'ISE est l'un des principaux blocs de l'architecture ISE qui fournit des fonctionnalités de surveillance, de création de rapports et d'alerte.

ISE affiche des informations de surveillance à de nombreux endroits, notamment :

- Page d'accueil Cisco ISE
- Vues de visibilité contextuelle
- Journaux et sessions en direct RADIUS
- Recherche globale
- Journaux NAC en direct axés sur les menaces
- Journaux TACACS en direct

Problèmes généraux observés dans la catégorie Surveillance et dépannage :

1. Journaux Radius/TACACS Live non disponibles
2. Sessions en direct non disponibles
3. Résumé de l'état non disponible
4. Problèmes de performances (CPU/mémoire élevée) observés sur les noeuds MnT)

Les débogages à activer sur les noeuds MnT pour réduire le problème :

1. Cisco-mnt
2. Collecteur
3. Cpm-mnt

4. journalisation de l'exécution

Outre les composants mentionnés dans debug, ces informations peuvent vous aider à dépanner :

1. Les sessions en direct sont-elles également affectées ou uniquement les journaux en direct ?
2. Les journaux Radius ou TACACS sont-ils affectés ou les deux ?
3. Voyez-vous une utilisation élevée du CPU ou de l'espace d'échange sur les noeuds MnT ?
4. Combien de fichiers de mémoire tampon voyez-vous sur les noeuds MnT ? Les fichiers de mémoire tampon se trouvent sous : /opt/CSCOcpm/mnt/data/collector.
5. Les réservations de mémoire et de CPU sont-elles activées, sinon activez-les.
6. La réinitialisation de la base de données MnT/config/session a-t-elle été effectuée récemment ?
7. Voyez-vous des syslogs envoyés de PSN à des noeuds MnT ?

Si vous utilisez les services Syslog pour MnT, ces informations sont requises à des fins de dépannage :

1. Utilisez-vous une cible Syslog sécurisée, sinon désactivez-la car elle est connue pour provoquer des interblocages dans les threads, ce qui entraîne l'arrêt du fonctionnement du collecteur ?
2. Utilisez-vous une cible Syslog sécurisée, assurez-vous que le mappage de certificat est correctement défini sous Administration->Journalisation->Cibles de journalisation distantes->Collecteur Syslog sécurisé 1 et 2
3. Vérifiez si les catégories de journalisation sont correctement définies (recommandé pour supprimer les catégories de journalisation non utilisées/indésirables, ce qui réduit la charge sur les noeuds MnT) et si les cibles de journalisation sont correctement configurées.
4. Consultez les fichiers awrrep*.html du bundle de support pour comprendre et obtenir un indice de quel composant envoie des syslogs plus fréquents. Par exemple, si des tables TACACS sont vues avec des requêtes d'insertion ou de mise à jour, nous pouvons vérifier les journaux du collecteur pour les corréler afin de comprendre quels syslogs sont envoyés plus fréquemment

Si le problème est lié aux performances sur le noeud MnT, nous avons besoin des informations suivantes :

1. tech top output de l'interface de ligne de commande ISE du noeud MnT.

2. Si le processeur est élevé, voyez-vous également une utilisation élevée de la mémoire ou de l’espace d’échange ?

3. Bundle de soutien avec vidage de tas et vidage de fil sécurisé.

Référence

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.3
- Dépannage et activation des débogages sur ISE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.