Comment dépanner les alarmes non disponibles de l'état d'intégrité ISE

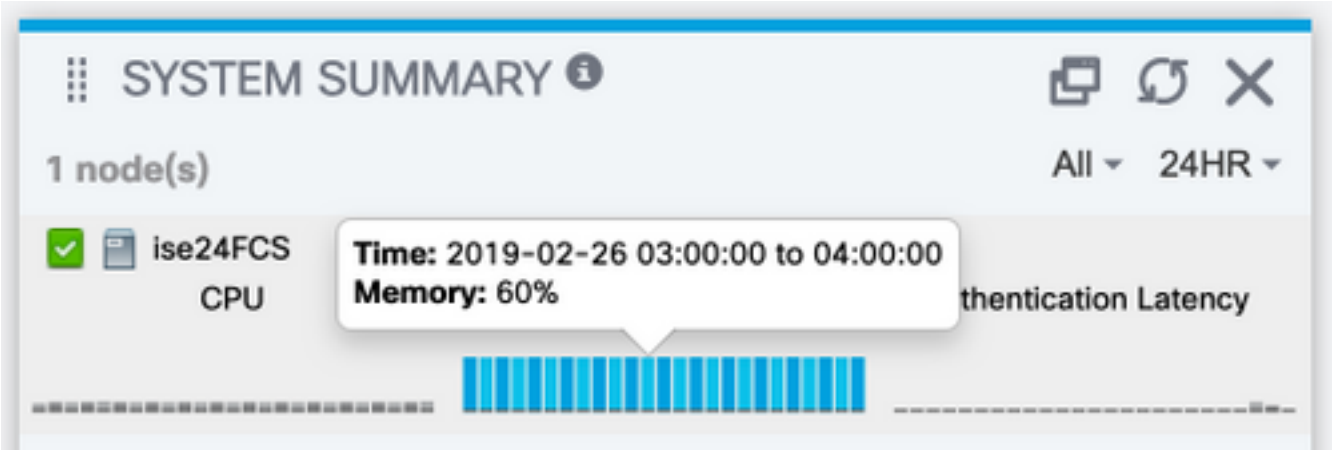
Contenu

Introduction

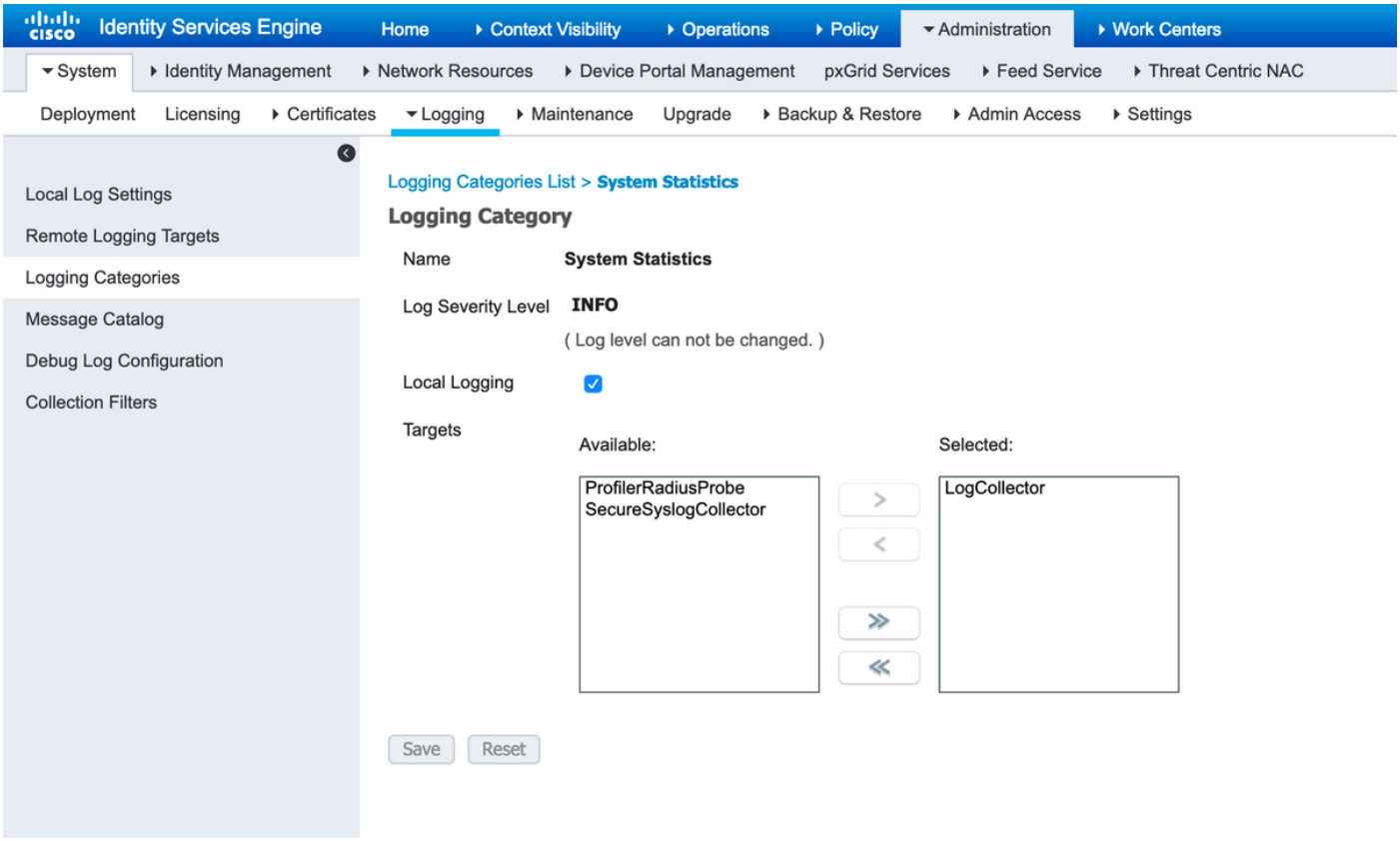
L'interface graphique de l'administrateur principal comprend un tableau de bord récapitulatif du système qui affiche les statistiques de latence du processeur, de la mémoire et de l'authentification par heure au cours des 24 dernières heures.

Ces données sont pilotées par des messages syslog générés par chaque noeud du déploiement et transmis aux noeuds de surveillance toutes les 5 minutes.

Les noeuds de surveillance collectent ces chiffres d'utilisation moyenne des ressources de 5 minutes, qui sont ensuite calculés en moyenne sur une heure pour être affichés dans le tableau de bord System Summary.



La configuration qui régit cette opération (et qui vous permettra également d'envoyer ces données à la collection Syslog externe) se trouve sous Administration > Logging > Logging Categories > System Statistics



Lorsque la case à cocher Journalisation locale est activée, cela indique que chaque noeud va consigner le Syslog localement dans son fichier localStore/iseLocalStore.log et envoyer une copie aux noeuds de surveillance et à toute autre cible de journalisation distante sélectionnée dans cette configuration. LogCollector est le nom par défaut du noeud Surveillance principale. Si votre déploiement comporte 2 noeuds de surveillance, vous pouvez également vous attendre à voir LogCollector2 répertorié comme cible sélectionnée ici. Pour vérifier la liste des cibles, Administration > Logging > Remote Logging Targets.

Vérification et dépannage :

Vous vous attendez à ce que chaque noeud du déploiement envoie ces messages toutes les 5 minutes et les enregistre localement.

Sur le noeud, vous pouvez exécuter :

show logging application localStore/iseLocalStore.log | i « 70000 AVIS »

Vérifier si le noeud génère effectivement ces syslogs.

Avec Collector at DEBUG sur le noeud de surveillance, vous devriez également voir ces messages être collectés via :

show logging application collector.log | i « 70000 AVIS »

sur les noeuds Surveillance.

Si la cible de journalisation n'est pas configurée pour une communication sécurisée, une capture de paquets doit également indiquer si le noeud envoie des données aux noeuds de surveillance. La communication par défaut se trouve sur le port UDP 20514.

Données à collecter :

Activez les débogages du collecteur sous Administration > Logging > Debug Log Configuration > Monitoring noeuds.

Captures de paquets sur le noeud de surveillance et le noeud pour lequel des alarmes d'état de santé non disponibles sont générées.