Como solucionar problemas de alarmes não disponíveis de status de integridade do ISE

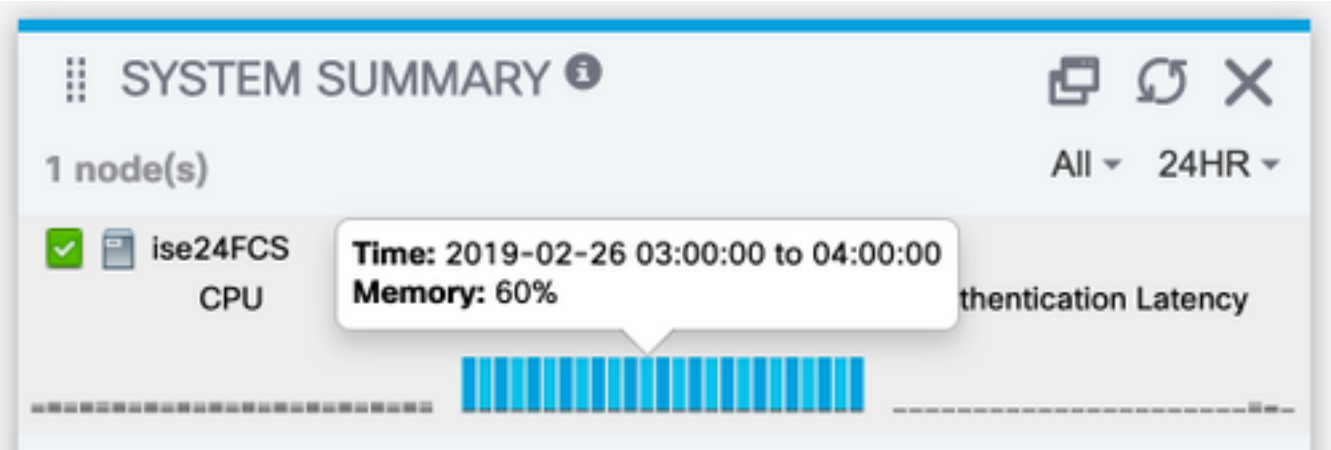
Contents

Introduction

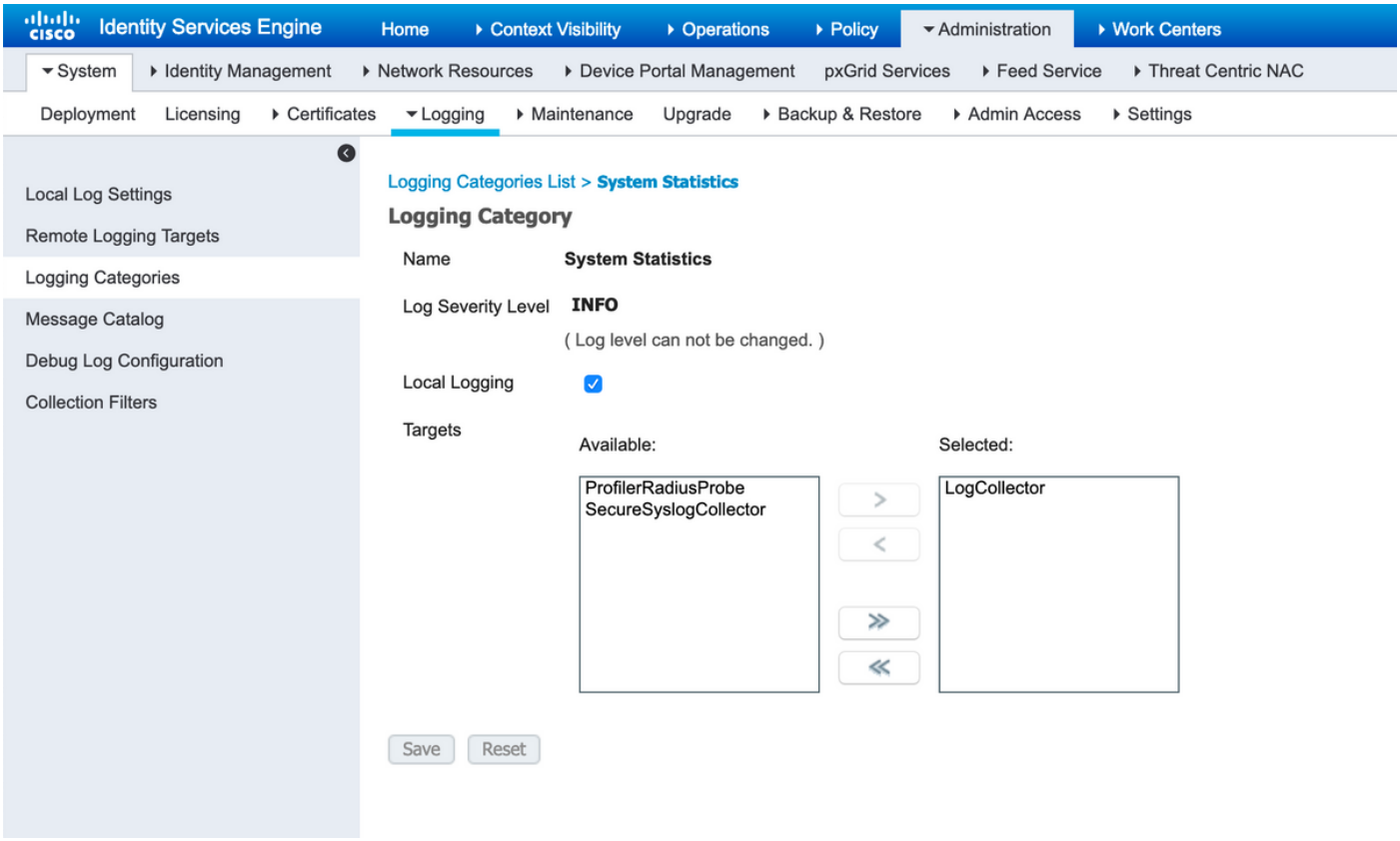
A GUI do administrador principal inclui um painel de resumo do sistema que mostra as estatísticas de CPU, memória e latência de autenticação por hora nas últimas 24 horas.

Esses dados são conduzidos por mensagens de syslog geradas por cada nó na implantação e entregues aos nós de monitoramento a cada 5 minutos.

Os nós de monitoramento coletam esses números médios de utilização de recursos de 5 minutos, que são então medidos em média ao longo da hora para exibição no Painel de resumo do sistema.



A configuração que rege isso (e que também permitirá que você envie esses dados para a coleta de syslog externa) está em Administração > Registro > Categorias de registro > Estatísticas do sistema



Com a caixa de seleção Local Logging habilitada, isso indica que cada nó registrará o Syslog localmente no arquivo localStore/iseLocalStore.log junto com o envio de uma cópia aos nós de monitoramento e a qualquer outro destino de registro remoto selecionado nesta configuração. LogCollector é o nome padrão do nó Monitoramento principal. Se sua implantação tiver dois nós de monitoramento, você também esperaria ver o LogCollector2 listado como um destino selecionado aqui. Para verificar a lista de destinos, Administration > Logging > Remote Logging Targets.

Verificação e Troubleshooting:

Você esperaria ver todos os nós na implantação enviando essas mensagens a cada 5 minutos e também registrando-as localmente.

No nó, você pode executar:

show logging application localStore/iseLocalStore.log | i "AVISO 70000"

Para revisar se o nó está realmente gerando esses syslogs.

Com o coletor em DEBUG no nó de monitoramento, você também deve ver essas mensagens sendo coletadas por meio de:

show logging application collector.log | i "AVISO 70000"

nos nós de monitoramento.

Desde que o destino de registro não esteja configurado para comunicação segura, uma captura de pacote também deve revelar se o nó está enviando dados aos nós de monitoramento. A comunicação padrão está na porta UDP 20514.

Dados a recolher:

Ative as depurações do coletor em Administração > Registro > Configuração do log de depuração > Nós de monitoramento.

O pacote captura o nó de monitoramento e o nó para o qual os alarmes de status de integridade indisponíveis estão sendo gerados.