Definir componentes para um determinado nível e gerar um pacote de suporte

Contents

Introdução

Este vídeo descreve as etapas para definir os componentes do ISE em um determinado nível e, em seguida, gerar um pacote de suporte.

Transcrição Iniciada

Olá, meu nome é Antonio García da equipe do TAC de segurança. No vídeo de hoje, você verá como definir componentes em um determinado nível e, em seguida, gerar um pacote de suporte. Essa é uma maneira ideal de informar rapidamente como coletar dados corretamente durante a solução de problemas.

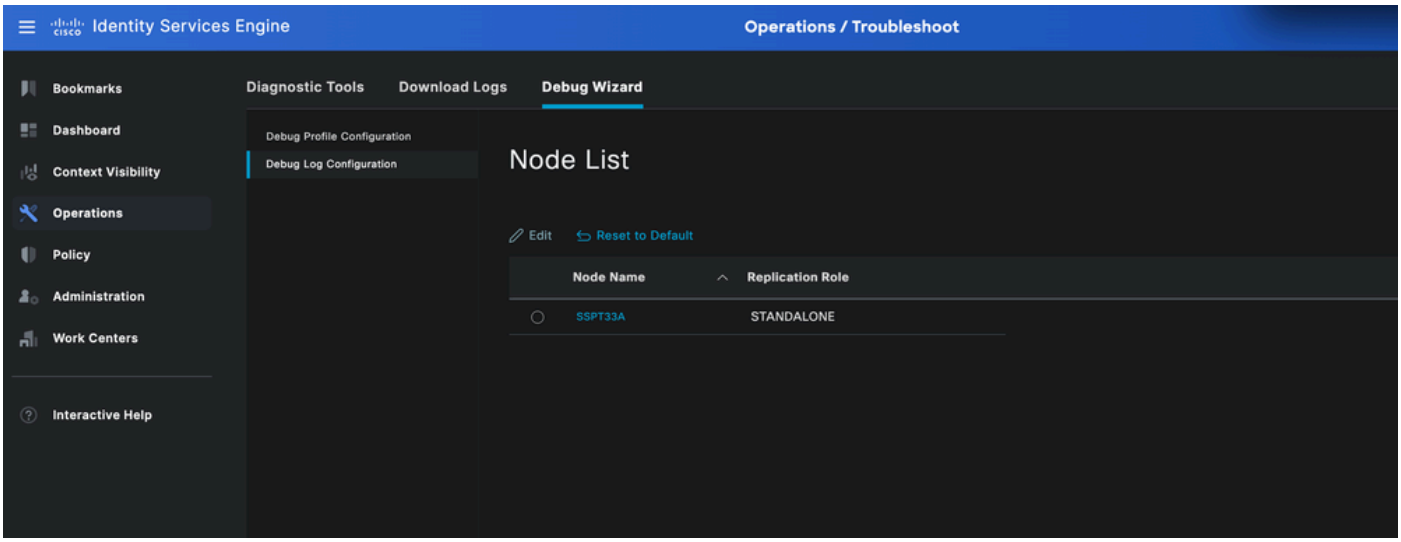
Antes de começar, observe que os componentes runtime-aaa, runtime-logging e runtime-config impactam significativamente o desempenho. Esses componentes não devem ser mantidos no modo DEBUG por mais de 15 minutos, pois isso pode causar problemas de desempenho nos nós.

Etapas

Há quatro etapas principais que devem ser abordadas durante a coleta de logs:
Fase 1- Defina os componentes para o nível necessário.
Fase 2 - Recrie o problema.
Fase 3 - Defina os componentes para o nível padrão.
Fase 4 - Gerar o pacote de suporte.

Agora vamos falar um por um sobre cada um deles:

Fase 1 - Definir os componentes para o nível necessário
Para começar, na GUI do Cisco ISE, clique no ícone Menu e escolha Operations > Troubleshoot > Debug Wizard > Debug Log configuration e selecione o nó do qual deseja obter logs. Agora você já deve ser capaz de ver uma lista de componentes. Cada componente tem arquivos de log específicos que ajudam você a entender o que pode ser um problema.



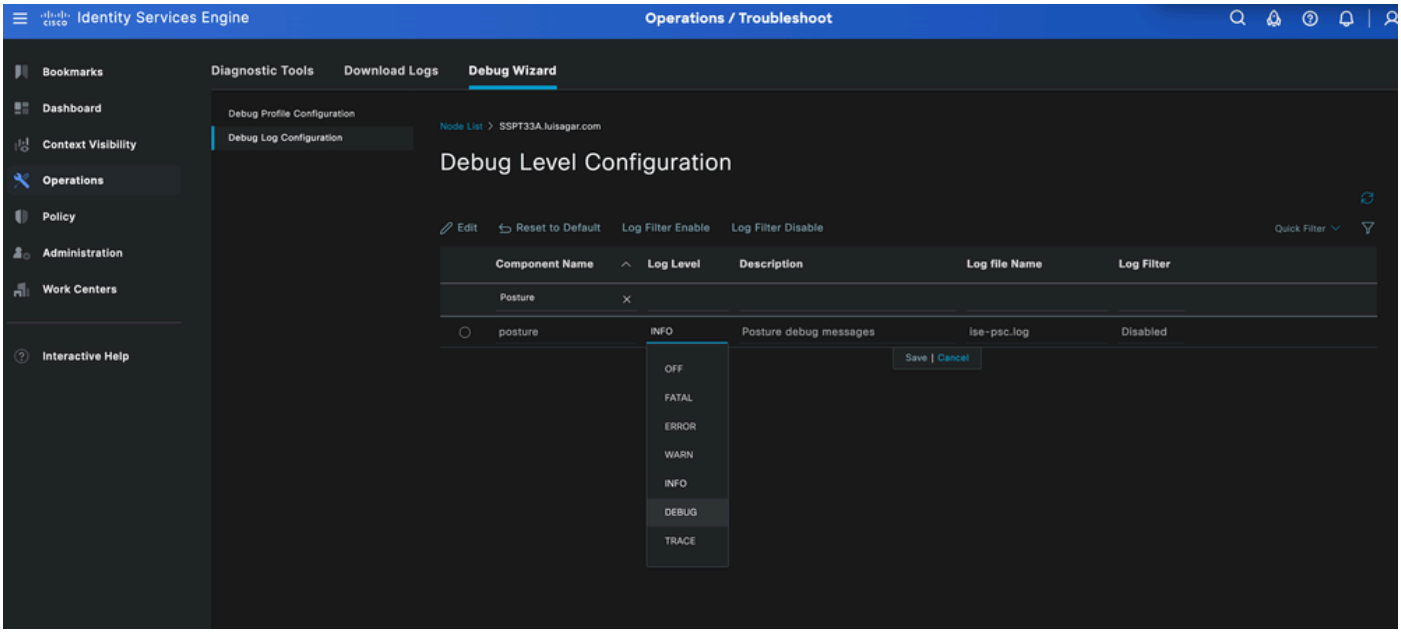
Para modificar esses componentes, você deve fazer o seguinte:

+ Selecione cada componente individualmente para modificar seu Nível de log e coletar os dados conforme solicitado.

+ Clique no ícone de filtro para que agora você possa digitar o nome do componente no campo para localizá-lo rapidamente

+ Em seguida, clique duas vezes no Nível de log atual para modificá-lo para qualquer um desses componentes. Por exemplo, clique em debug level > e, em seguida, clique em Save.

+ Você pode repetir as mesmas etapas para modificar o restante dos componentes conforme necessário.



Fase 2 - Recriar o problema
Agora você está pronto para recriar o problema para gerar logs e capturar os dados.

Você deve levar em consideração que é vital salvar um carimbo de data e hora de quando o problema ocorreu para que o engenheiro do TAC possa revisar os registros de forma eficiente.

Isso pode ser feito por:

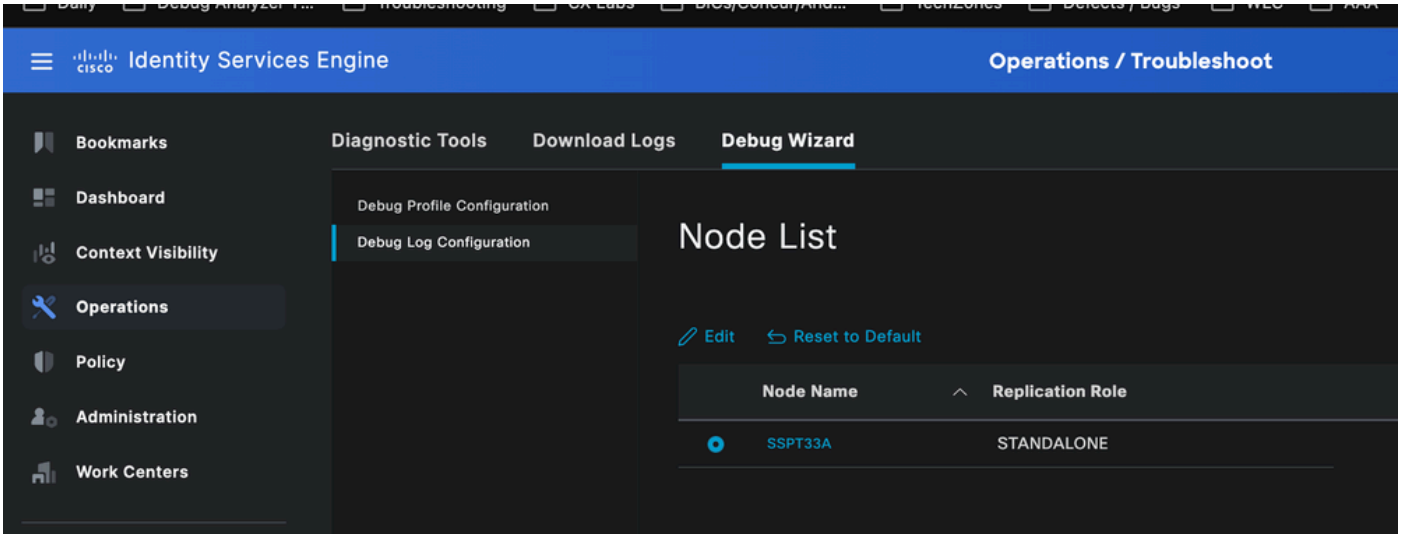
1- Usando o comando show clock logo antes de começar e quando terminar de recriá-lo. Obtenha o timestamp da perspectiva do ISE.

Ou

2-Verificando os detalhes do registro em tempo real. Pessoalmente, recomendo compartilhar um formato PDF de registro ao vivo que mostre o endereço MAC, o carimbo de data/hora, o motivo da falha, o endereço IP e a ID da sessão.

Fase 3 - Definir os componentes para o nível padrão

É essencial definir os componentes para o nível padrão, pois o desempenho pode ser afetado. Para fazer isso, na GUI do Cisco ISE, clique no ícone Menu e escolha Operations > Troubleshoot > Debug Wizard > Debug Log configuration, em seguida, selecione o nó com o qual você está trabalhando > Click on Reset to Default.



Fase 4 - Gerar o pacote de suporte

A fase final é coletar o pacote de suporte na GUI do Cisco ISE. Para fazer isso, clique no ícone Menu e escolha Operações > Solução de problemas > Logs de download e selecione o nó com o qual você está trabalhando. Você deve selecionar todas as opções, exceto a primeira e as duas últimas:

- Incluir logs de depuração
- Incluir logs locais
- Incluir arquivos principais
- Incluir logs de monitoramento e relatório
- Incluir logs do sistema

Depois de selecionar as opções, selecione as datas correspondentes de quando a ocorrência foi recriada. Se a data não for definida, o pacote de suporte incluirá todos os logs disponíveis no nó.

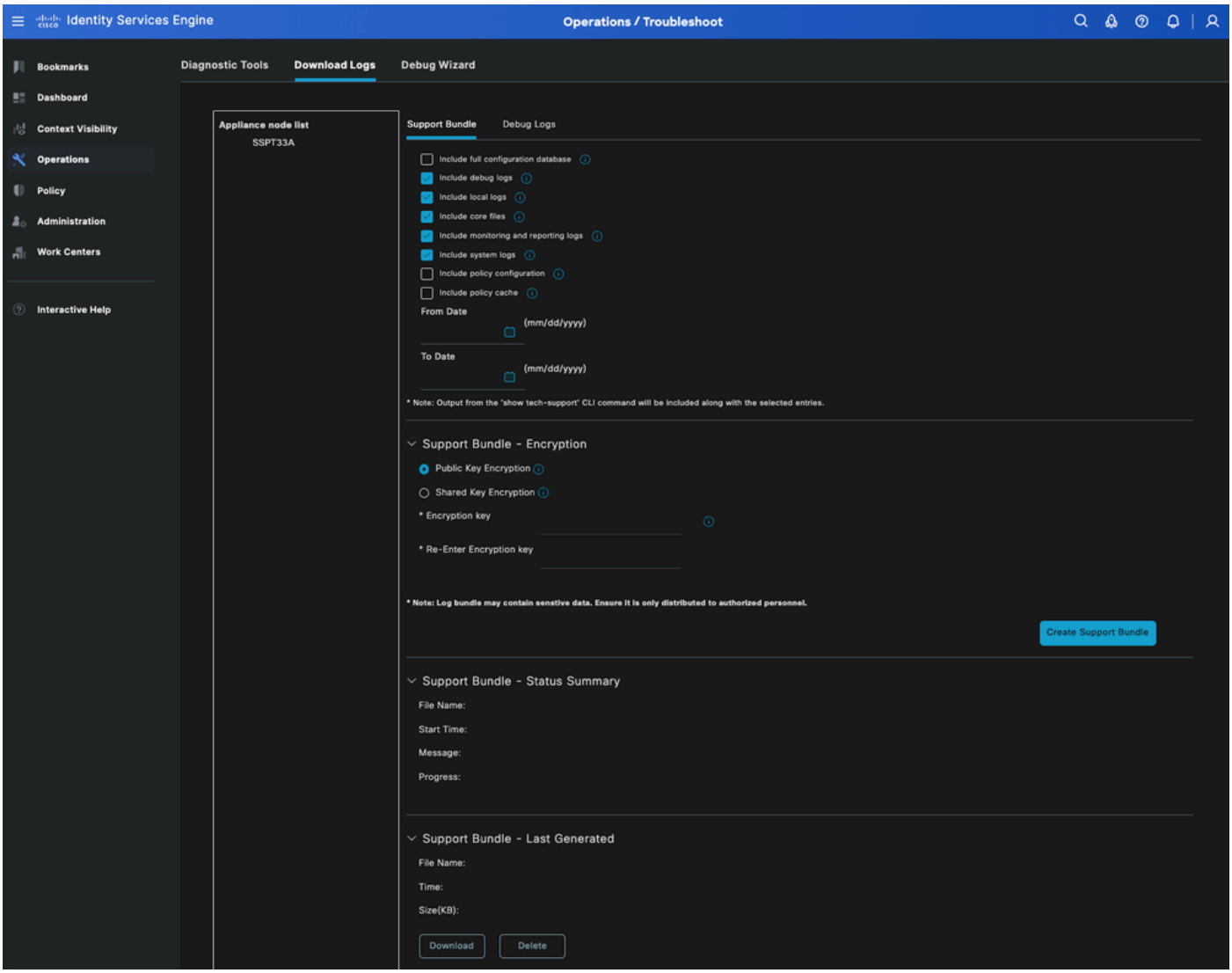
Essa abordagem é viável, mas o pacote será grande. Se possível, é preferível coletar logs de datas específicas para minimizar o tamanho do pacote.

Agora, com relação à criptografia do pacote de suporte, você tem duas opções:

1- Chave pública: Essa opção usa uma chave pública e não exige que você adicione uma chave de criptografia.

2 - Criptografia de chave compartilhada: nessa opção, você deve adicionar uma chave de criptografia. Se você selecionar essa opção, deverá carregar um arquivo .txt com a chave de criptografia para que o engenheiro do TAC possa descriptografá-lo.

Clique em Create Support Bundle, espere até que ele seja gerado, o que leva algum tempo. Em seguida, clique em download para finalmente carregá-lo no caso.



Para carregá-lo no caso, use este link: https://mycase.cloudapps.cisco.com/case

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

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

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