Identificação e solução de problemas de dispositivos XDR e integração orbital

Contents

Introdução

Este documento descreve as etapas para configurar a integração e solucionar problemas do Device Insights and Orbital integration.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Se quiser saber mais sobre a configuração, revise aqui os detalhes do módulo de integração.

Informações de Apoio

O XDR Device Insights fornece uma visão unificada dos dispositivos em sua organização e consolida inventários de fontes de dados integradas, como Orbital.

Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

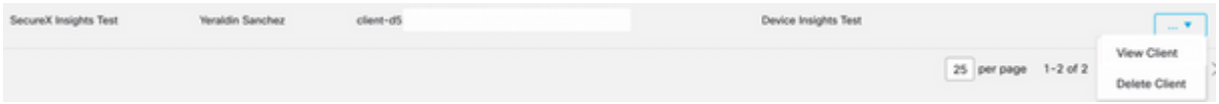
Conectividade

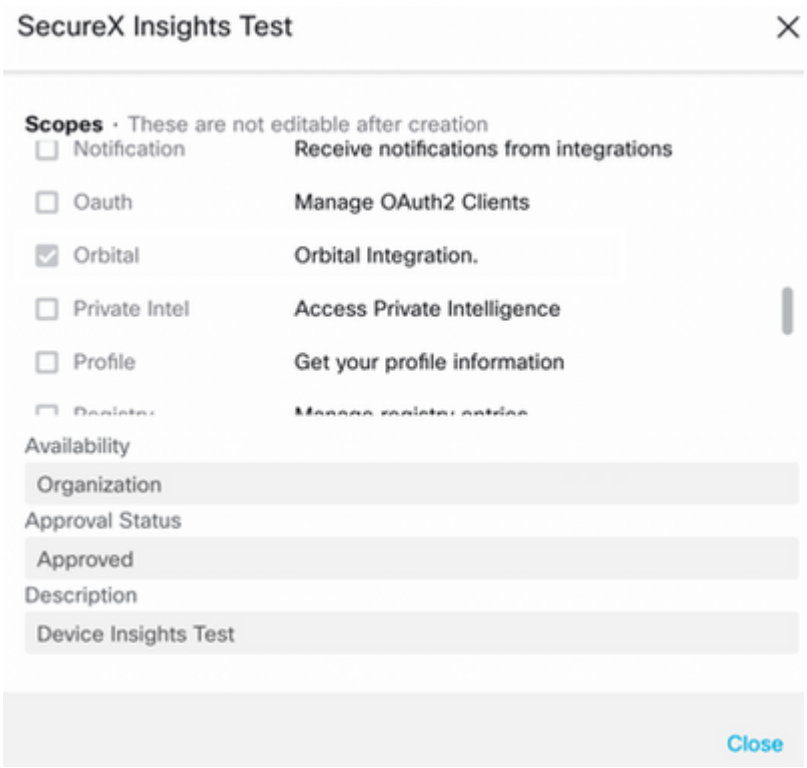
- A credencial de fontes da API REST pode ser usada para testar a conectividade básica usando ferramentas como Postman.
- Quando os resultados das consultas começarem a vir dos dados dos agentes Orbital, eles serão publicados no Remote Datastore.

- Valide se um Armazenamento de Dados Remoto foi criado para o Device Insights, isso pode ser verificado nas configurações da conta.
- No administrador de detalhes do Repositório de Dados Remotos, verifique se a ID do locatário do Device Insights e a URL do Device Insights são exibidos, o Status deve ser Autenticado.

- Navegue até a guia Resultados para ver em uma lista de Trabalhos o Trabalho criado pelo Device Insights

- No portal XDR, navegue até Administração, selecione o Cliente API e certifique-se de que Orbital esteja selecionado, como mostrado nas imagens.





- Erro "Sem resposta do endpoint, ele pode estar offline" - Esse erro significa que o endpoint está desligado ou não tem conectividade com a nuvem Orbital. Consulte o documento Endereços de servidor necessários para operações adequadas de análise de malware e endpoint seguro da Cisco para verificar se IPs, portas e URLs são permitidos.

Contagem de incompatibilidade

- Se a contagem de dispositivos não for correspondente, isso é esperado, pois a Orbital não mantém seu inventário de endpoints com mais de 90 dias desde a versão 1.14, ela inclui todos os endpoints que

tiveram um conector Orbital instalado a qualquer momento, e não apenas os ativos em seu inventário. Quando o recurso de insights do dispositivo está ativo, ele cria um trabalho diário recorrente para todos os endpoints executarem. Depois que o trabalho é executado no endpoint e as informações do dispositivo resultante são enviadas de volta à Orbital, o XDR é notificado sobre a existência desse dispositivo da Orbital. Se nenhum resultado de trabalho para esse dispositivo for recebido dentro de 90 dias, o endpoint Orbital será eliminado do inventário em insights de dispositivos.
- A reinstalação orbital resulta em um novo GUID que pode causar uma duplicação no console.

Licença

- Verifique se o Secure Endpoint Console tem a licença apropriada para ter acesso ao Orbital.

Dispositivos Mac e Linux não exibidos

- Dispositivos MacOS e Linux de origem Orbital ainda não são suportados no XDR Device Insights.

Caso o problema persista com o XDR Device Insights and Orbital integration, consulte este artigo para coletar registros HAR do navegador e entre em contato com o suporte TAC para executar uma análise mais profunda.

Informações Relacionadas

- **Guia de referência XDR**
- **Troubleshooting Orbital**
- **Suporte Técnico e Documentação - Cisco Systems**

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.