Solução de problemas de usuários do Ative Diretory ausentes do relatório de pesquisa de atividades no Umbrella

Contents

Introdução

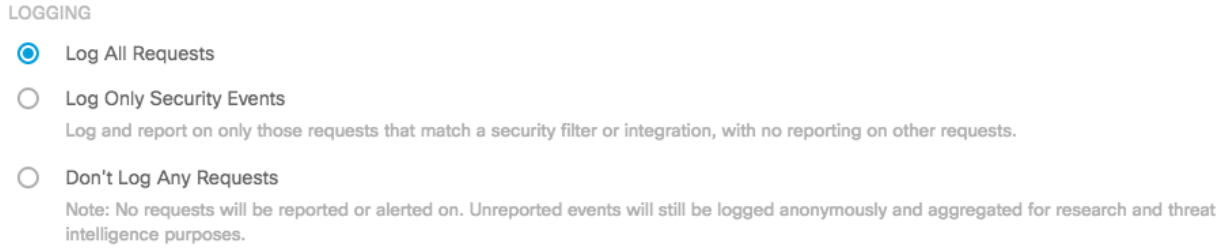
Este documento descreve o Relatório de pesquisa de atividades no Cisco Umbrella. O Relatório de pesquisa de atividades é um relatório quase ao vivo de todas as consultas DNS que seus usuários estão fazendo. Se você configurou a integração do Ative Diretory (AD) do Cisco Umbrella, pode esperar ver seus usuários do AD preenchendo a coluna Identidade em sua Pesquisa de atividades. No entanto, há situações em que os usuários estão ausentes na coluna Identidade.

Resolução

Se você acha que deve ver usuários do AD diretamente na coluna Identidade na Pesquisa de atividades, mas não os vê, ou está vendo alguns, mas não tantos como o esperado, veja algumas coisas a serem verificadas:

1. Sites e Ative Diretory
    - Verifique todos os componentes do AD para certificar-se de que não haja erros ou problemas relatados. Se você vir indicadores de status cinza, laranja ou vermelho em qualquer um dos componentes, obtenha esses detalhes e abra um ticket de suporte (umbrella-support@cisco.com).
        - Teste de diagnóstico de um usuário afetado (um usuário que não está aparecendo na Pesquisa de atividade)
        - Captura de tela do console do Virtual Appliance (VA), com todas as mensagens de erro expandidas
        - Logs de Auditoria do Conector AD
2. Configurações de log
    - Nas Configurações avançadas de cada política, há uma seção na parte inferior que diz respeito a quanto registrar. Você pode defini-lo como:
        - Registrar todas as solicitações
        - Registrar somente eventos de segurança

    - Não Registrar Solicitações
- Se sua política estiver definida atualmente como "Registrar somente eventos de segurança", isso poderá explicar por que você não está vendo tantas consultas quanto o esperado ou nenhum resultado de alguns usuários.



3. Corrigir precedência de política
    - Se você tiver uma política aplicada a uma Identidade de rede que esteja mais avançada na lista de políticas do que a sua política de usuário do AD, a política de Identidade de rede provavelmente será aplicada. Isso, por sua vez, significa que na Pesquisa de atividade, você verá a Rede como a Identidade relatada. Verifique também a documentação do Cisco Umbrella sobre práticas recomendadas e precedência de políticas.

Causa

Onde a pesquisa de atividade obtém a "identidade"?

Quando uma consulta DNS entra no Umbrella, supondo que sua Integração de AD esteja funcionando conforme esperado, estas informações são passadas adiante na consulta:

- Endereço IP interno
- Hash de identidade do AD (usuário, host ou ambos)
- IP de saída
- Domínio sendo consultado

O Hash de identidade do AD é adicionado à consulta pelo Virtual Appliance, que recebe essas informações, e o endereço IP interno correspondente para o evento de logon do AD Connector.

Em seguida, o Cisco Umbrella usa essas informações para localizar a organização e determinar qual política aplicar. Se você não tiver políticas especificamente aplicadas aos seus usuários do AD, mas tiver uma para suas Redes ou Sites, o Cisco Umbrella aplicará a política usando essa Identidade. Isso significa que quando a consulta, a identidade e a resposta são relatadas na Pesquisa de Atividade, a Identidade que disparou a política que é relatada. As outras informações ainda são marcadas na solicitação, assim você ainda pode procurar um usuário do AD e obter a atividade que relata uma rede como a Identidade. Além disso, se você exportar os dados da pesquisa de atividades para um arquivo CSV, ele mostrará todas as informações de identidade associadas à consulta.

Informações adicionais

Se você ainda não vir nenhum usuário do AD, entre em contato com o Suporte (umbrella-

support@cisco.com), com um resultado de teste de diagnóstico e com todos os Logs de Auditoria do Conector AD relevantes.

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.