Consultas básicas de pesquisa orbital para análise de ameaças

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Informações de Apoio

Acesso

Consultas Personalizadas

- 1. Itens de Inicialização
- 2.Sha256 Hashes de Processos em Execução
- 3.Processo com conexões de rede
- 4.Processo Privilegiado com Conexão de Rede Não Localhost
- 5.Monitoramento do Registro de Backup/Restauração
- 6. Pesquisa de Arquivos
- 7.Monitoramento do histórico do Powershell
- 8.Consulta Prefetch
- 9. Inspeção de Cache do Address Resolution Protocol (ARP)

Introdução

Este documento descreve as consultas básicas de pesquisa orbital para análise de ameaças.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento do interesse na compreensão de ameaças e malware e uma compreensão básica das tabelas Structured Query Language (SQL).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Endpoint Connector versão 7.1.5 ou posterior para Windows
- Secure Endpoint Connector versão 1.16 ou posterior para Mac
- Secure Endpoint Connector versão 1.17 ou posterior para Linux
- O usuário do Secure Endpoint deve receber a função de administrador para implantar o Orbital

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.

Informações de Apoio

As consultas personalizadas são aproveitadas, o que deve ajudá-lo a aprender rapidamente o poder da Orbital e da osquery para a busca de ameaças.

Orbital faz uso de tabelas de estoque osquerys, além de tabelas específicas Orbital. Os resultados retornados pela Orbital podem ser enviados para outros aplicativos, como Secure Endpoint, Secure Malware Analytics e SecureX Threat Response, e podem ser armazenados em repositórios de dados remotos (RDS), como Amazon S3, Microsoft Azure e Splunk.

Use a página Investigação Orbital para construir e executar consultas ao vivo em endpoints para coletar mais informações deles. A Orbital usa osquery, que permite consultar seus dispositivos como um banco de dados com comandos SQL básicos.

Aqui está um exemplo simples: SELECIONE column1, column2 FROM table1, table2 WHERE column2='value'.

Neste exemplo, column1 e column2 são os nomes de campo da tabela da qual você deseja escolher os dados. Para escolher todos os campos disponíveis na tabela, use esta sintaxe: SELECT * FROM table1 (SELECIONE * DA tabela 1).

Acesso

Abra o Orbital diretamente nestes locais:

América do Norte - https://orbital.amp.cisco.com

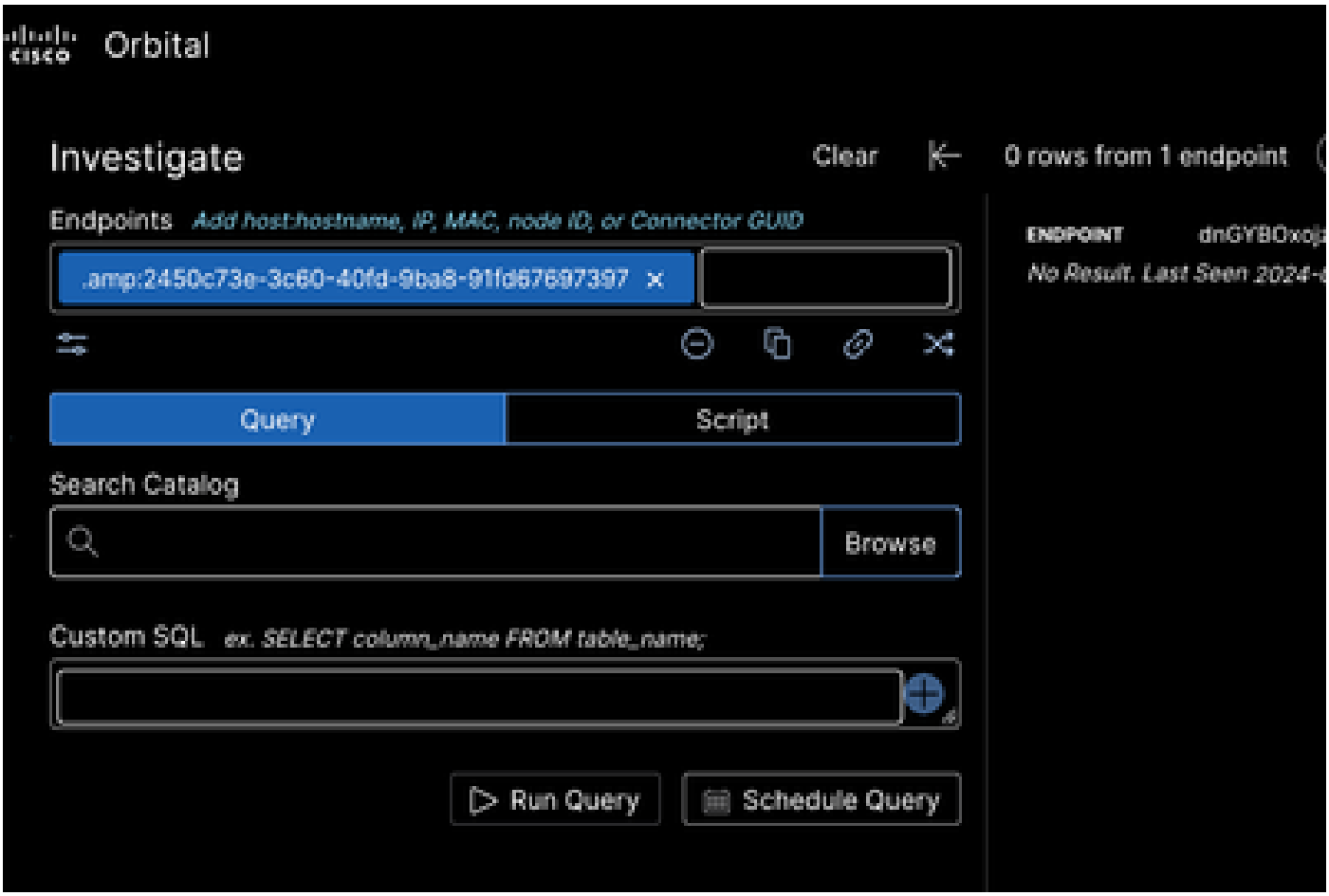
Europa - https://orbital.eu.amp.cisco.com

Pacífico Asiático - https://orbital.apjc.amp.cisco.com

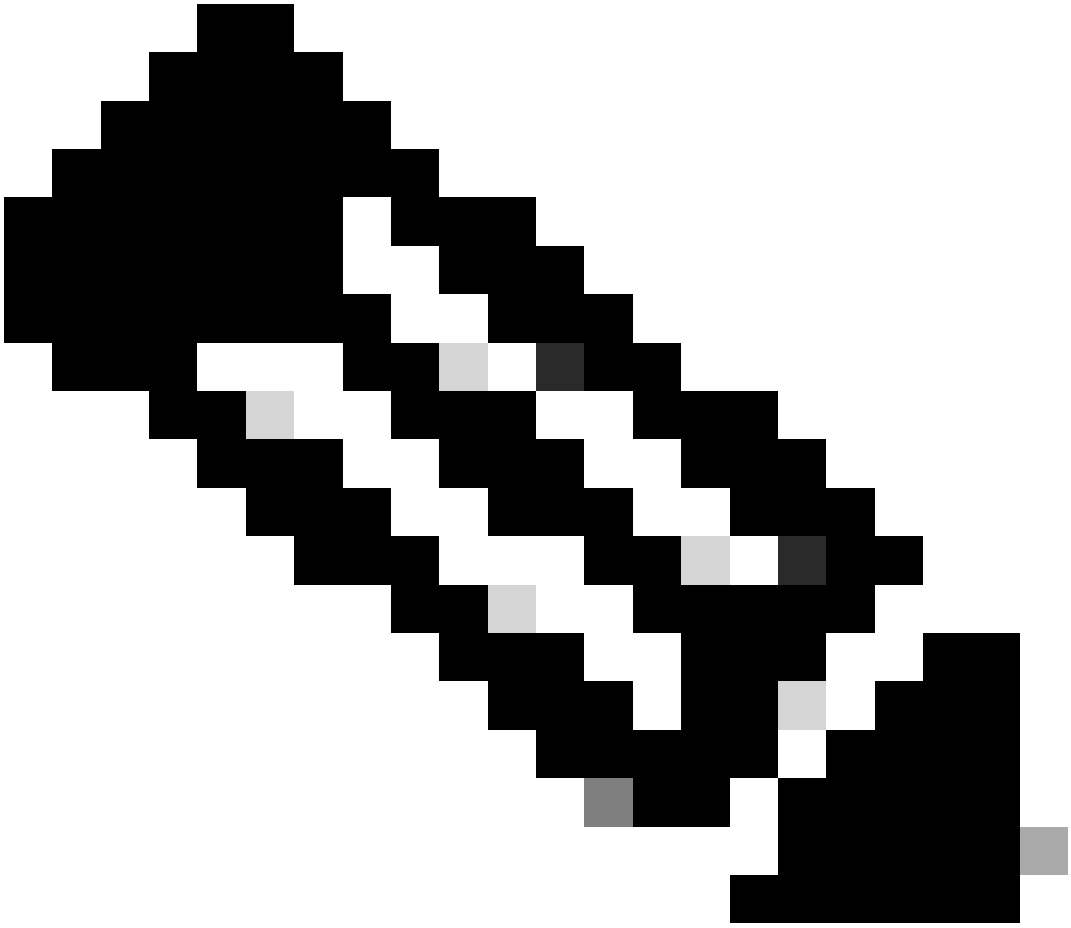
Ou

No Secure Endpoint Console, escolha o sistema Host afetado e clique em Investigar em Orbital.

Há opções para usar o Catálogo Orbital (Clique em Procurar) ou Inserir as Consultas Personalizadas na seção SQL Personalizado, conforme mencionado:



Consultas Personalizadas

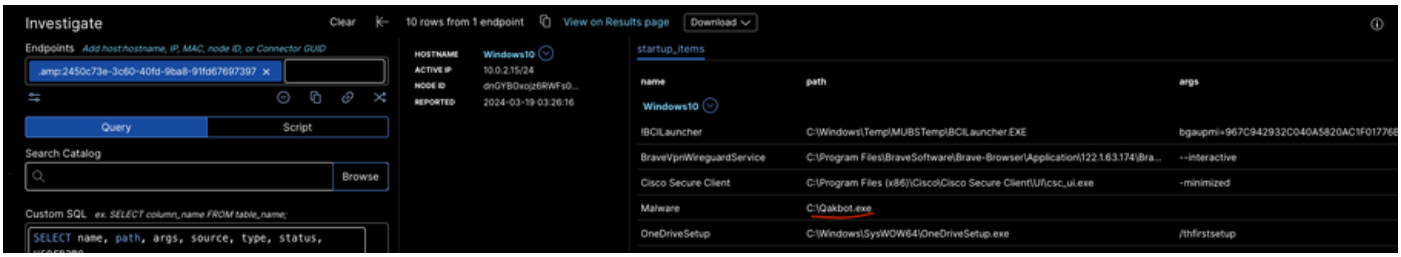


Note: O sistema host está na rede do laboratório e tenta-se manter o sistema/rede inabalável.

1. Itens de Inicialização

Os itens de inicialização podem ser explorados pelos invasores para manter a persistência em um sistema comprometido, o que significa que o software mal-intencionado continuará a ser executado ou será reiniciado automaticamente a cada reinicialização do sistema. No próximo exemplo, o Qakbot.exe está sendo executado no sistema host.

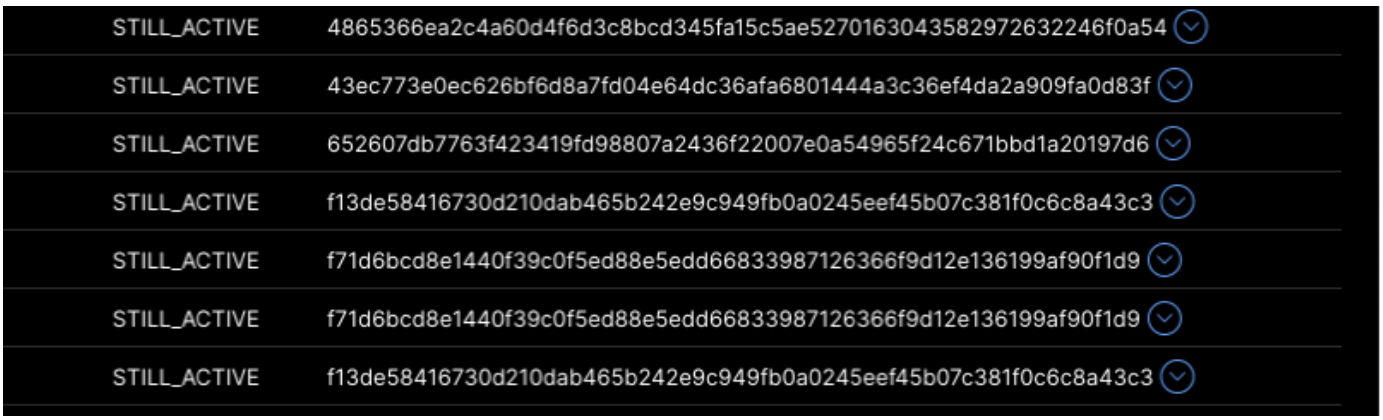
```
SELECT name, path, args, source, type, status, username
FROM startup_items;
```



2. Hashes Sha256 de Processos em Execução

Os hashes SHA256 não são associados de forma inerente aos processos em execução em seu estado natural. No entanto, software de segurança e ferramentas de monitoramento do sistema podem calcular o hash SHA256 de um processo em execução do arquivo executável para ajudar a verificar sua integridade e autenticidade.

```
 SELECT
p.pid, p.name, p.path, p.cmdline, p.state, h.sha256
FROM processes p
INNER JOIN hash h
ON p.path=h.path;
```

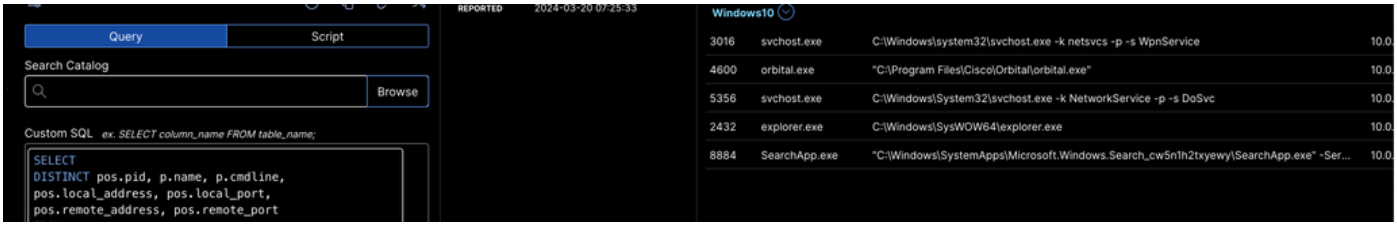


se o hash associado de um arquivo for mal-intencionado, você poderá se identificar com essa consulta.

3. Processo com Conexões de Rede

Os processos com conexões de rede são programas ou serviços do sistema que estão usando ativamente a interface de rede para se comunicar com outros dispositivos em uma rede ou pela Internet.

```
SELECT
DISTINCT pos.pid, p.name, p.cmdline, pos.local_address, pos.local_port, pos.remote_address, pos.remote_
FROM processes p
JOIN process_open_sockets pos USING (pid)
WHERE
pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1", “0");
```



4. Processo Privilegiado com Conexão de Rede Não Localhost

Executar um programa ou serviço que tenha permissões elevadas (como as de uma conta de administrador ou de sistema) e esteja se comunicando pela rede com um dispositivo ou serviço externo, ou seja, qualquer endereço IP diferente de 127.0.0.1 (localhost) ou ::1 (localhost IPv6).

```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1")
```

Depois de ter a lista de Identificadores de pacote (PID), você pode adicioná-la de acordo nas Consultas personalizadas.

```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1") and p.uid=1436
```

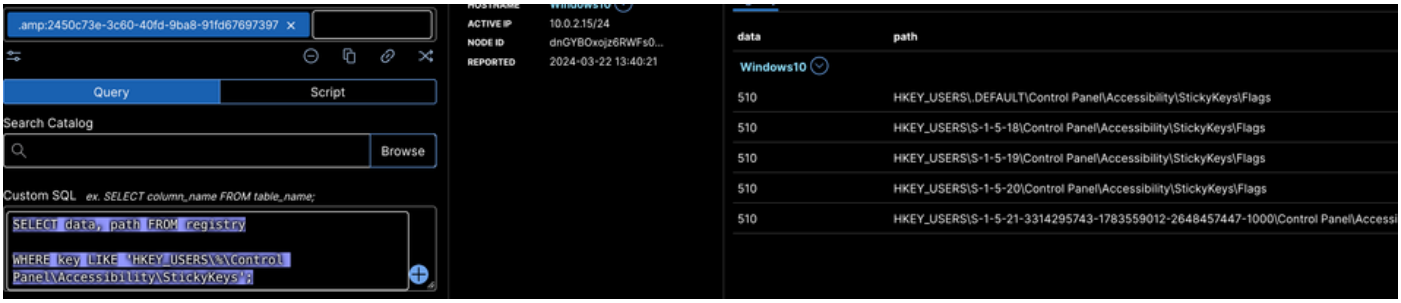
5. Monitoramento de Registro de Backup/Restauração

Rastreamento de eventos em que são feitas alterações no Registro do Windows por meio de operações de backup ou restauração. O Registro do Windows é um banco de dados hierárquico que armazena opções e definições de configuração em sistemas operacionais Microsoft

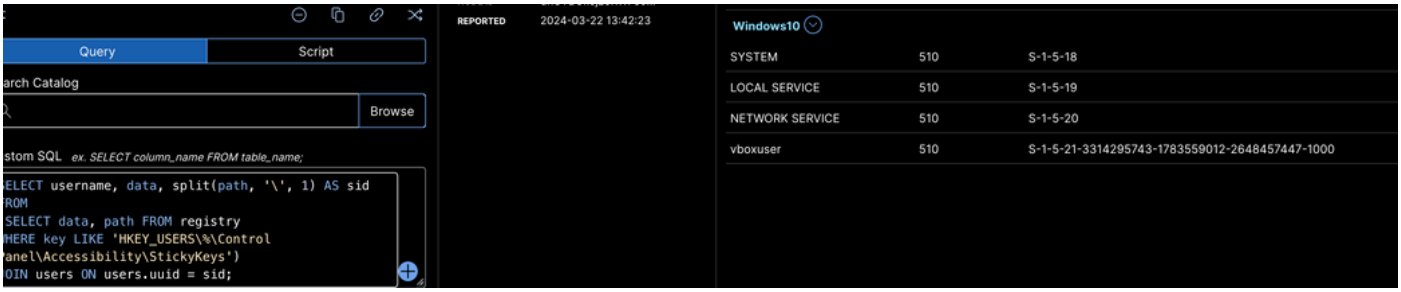
Windows.

```
SELECT key AS reg_key, path, name, data, DATETIME(mtime, "unixepoch") as last_modified
FROM registry
WHERE key LIKE "HKEY_LOCAL_MACHINE\system\currentcontrolset\control\backuprestore\filesnottosnapshot";
```

```
SELECT data, path FROM registry
WHERE key LIKE 'HKEY_USERS\%\Control Panel\Accessibility\StickyKeys';
```




```
SELECT username, data, split(path, '\', 1) AS sid
FROM
(SELECT data, path FROM registry
WHERE key LIKE 'HKEY_USERS\%\Control Panel\Accessibility\StickyKeys')
JOIN users ON users.uuid = sid;
```



6. Pesquisa de Arquivos

Permite que os usuários localizem arquivos e pastas em seus computadores usando vários critérios, como nome do arquivo, conteúdo, propriedades ou metadados.

```
SELECT
f.directory, f.filename, f.uid, f.gid,
f.mode, f.device, f.size,
f.atime,
f.mtime,
```

```
f.ctime,
f.btime,
f.hard_links, f.symlink, f.file_id, h.sha256
FROM file f
LEFT JOIN hash h on f.path=h.path
WHERE
f.path LIKE (SELECT v from __vars WHERE n="file_path") AND
f.path NOT LIKE (SELECT v from __vars WHERE n="not_file_path");
```

Navegue até PARÂMETROS > Caminho do arquivo e clique em %.dll ou %.exe ou %.png.

7. Monitoramento de Histórico do Powershell

Prática de controlar os comandos que foram executados em sessões do PowerShell. Monitorar o histórico do PowerShell pode ser particularmente importante por motivos de segurança e conformidade.

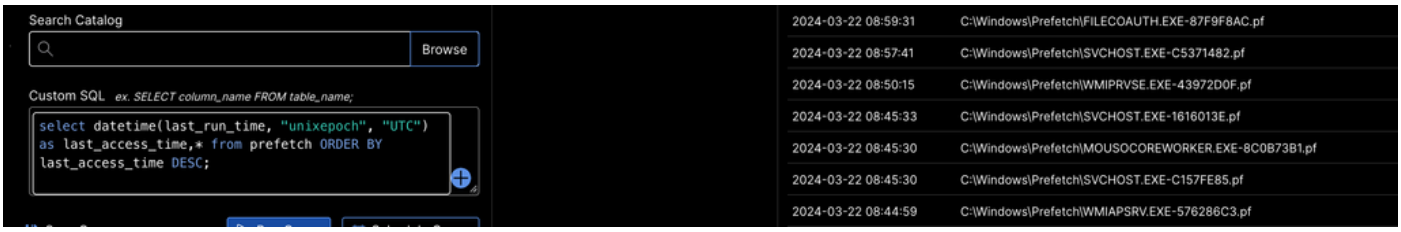
```
SELECT time, datetime, script_block_id, script_block_count, script_text, script_name, script_path
FROM orbital_powershell_events
ORDER BY datetime DESC
LIMIT 500;
```

8. Consulta Prefetch

Recurso de desempenho que acelera o carregamento de aplicativos. A pré-busca envolve analisar a forma como o software é carregado e executado em um sistema e, em seguida, armazenar informações sobre isso em arquivos específicos.

```
select datetime(last_run_time, "unixepoch", "UTC") as last_access_time,*
from prefetch
```

```
ORDER BY last_access_time DESC;
```

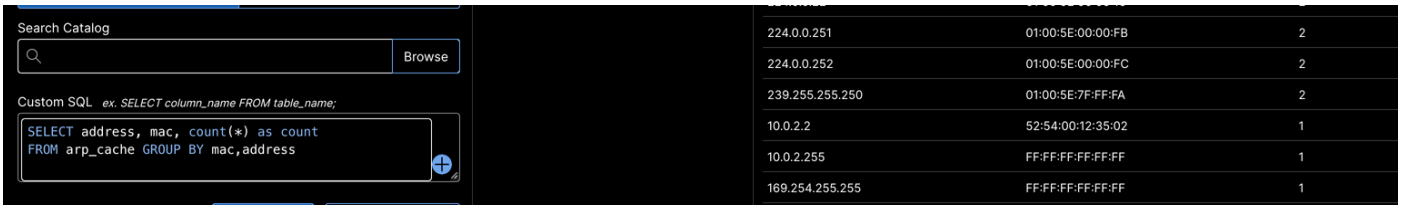


A pré-busca é um mecanismo com o qual o SQL Server pode ativar muitas solicitações de E/S em paralelo para uma junção de Loop Aninhado.

9. Inspeção de Cache do Address Resolution Protocol (ARP)

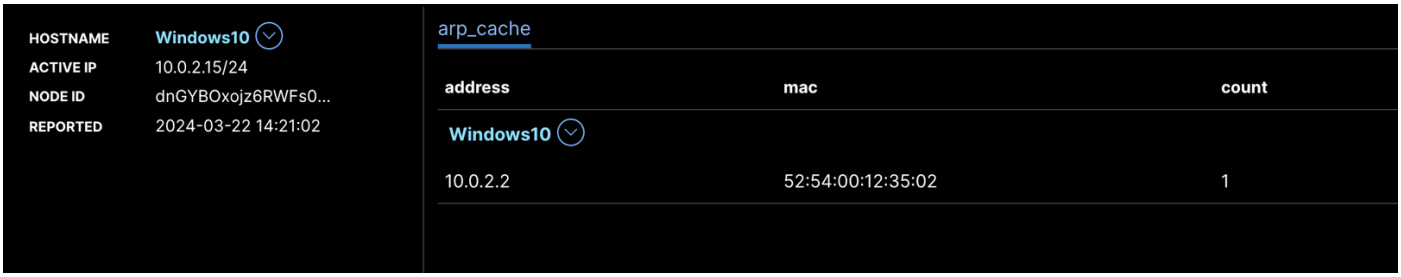
Envolve o exame do conteúdo do cache ARP em um computador ou dispositivo de rede. O cache ARP é uma tabela que armazena mapeamentos entre endereços IP e seus endereços MAC correspondentes.

```
SELECT address, mac, count(*) as count
FROM arp_cache GROUP BY mac,address;
```



O próximo exemplo mostra o endereço MAC suspeito e sua contagem do cache ARP.

```
SELECT address, mac, count(*) as count
FROM arp_cache GROUP BY mac,address
HAVING COUNT(mac) >= (SELECT count FROM arp_cache WHERE count>=1)
AND mac LIKE (SELECT mac FROM arp_cache WHERE mac="52:54:00:12:35:02");
```



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.