Consultas de búsqueda orbital básica para análisis de amenazas

Contenido

Introducción

Este documento describe las consultas de búsqueda orbital básica para el análisis de amenazas.

Prerequisites

Requirements

Cisco recomienda conocer el interés por comprender las amenazas y el malware, así como los conocimientos básicos de las tablas de lenguaje de consulta estructurado (SQL).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Secure Endpoint Connector versión 7.1.5 o posterior para Windows
- Secure Endpoint Connector versión 1.16 o posterior para Mac
- Secure Endpoint Connector versión 1.17 o posterior para Linux
- El usuario de terminal seguro debe tener asignada la función de administrador para

implementar Orbital

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las consultas personalizadas se aprovechan, lo que debe ayudarle a aprender rápidamente el poder de Orbital y osquery para la búsqueda de amenazas.

Orbital utiliza tablas de valores de osquerys además de tablas específicas de Orbital. Los resultados devueltos a través de Orbital se pueden enviar a otras aplicaciones, como Secure Endpoint, Secure Malware Analytics y SecureX Threat Response, y se pueden almacenar en almacenes de datos remotos (RDS), como Amazon S3, Microsoft Azure y Splunk.

Utilice la página Orbital Investigate (Investigación orbital) para construir y ejecutar consultas en directo en los terminales con el fin de recopilar más información de ellos. Orbital utiliza osquery, que le permite consultar sus dispositivos como una base de datos con comandos SQL básicos.

He aquí un ejemplo simple: SELECT column1, column2 FROM table1, table2 WHERE column2='value'.

En este ejemplo, column1 y column2 son los nombres de campo de la tabla de la que desea elegir datos. Para elegir todos los campos disponibles en la tabla, utilice esta sintaxis: SELECT * FROM tabla1.

Acceso

Abra Orbital directamente en estos sitios:

Norteamérica: https://orbital.amp.cisco.com

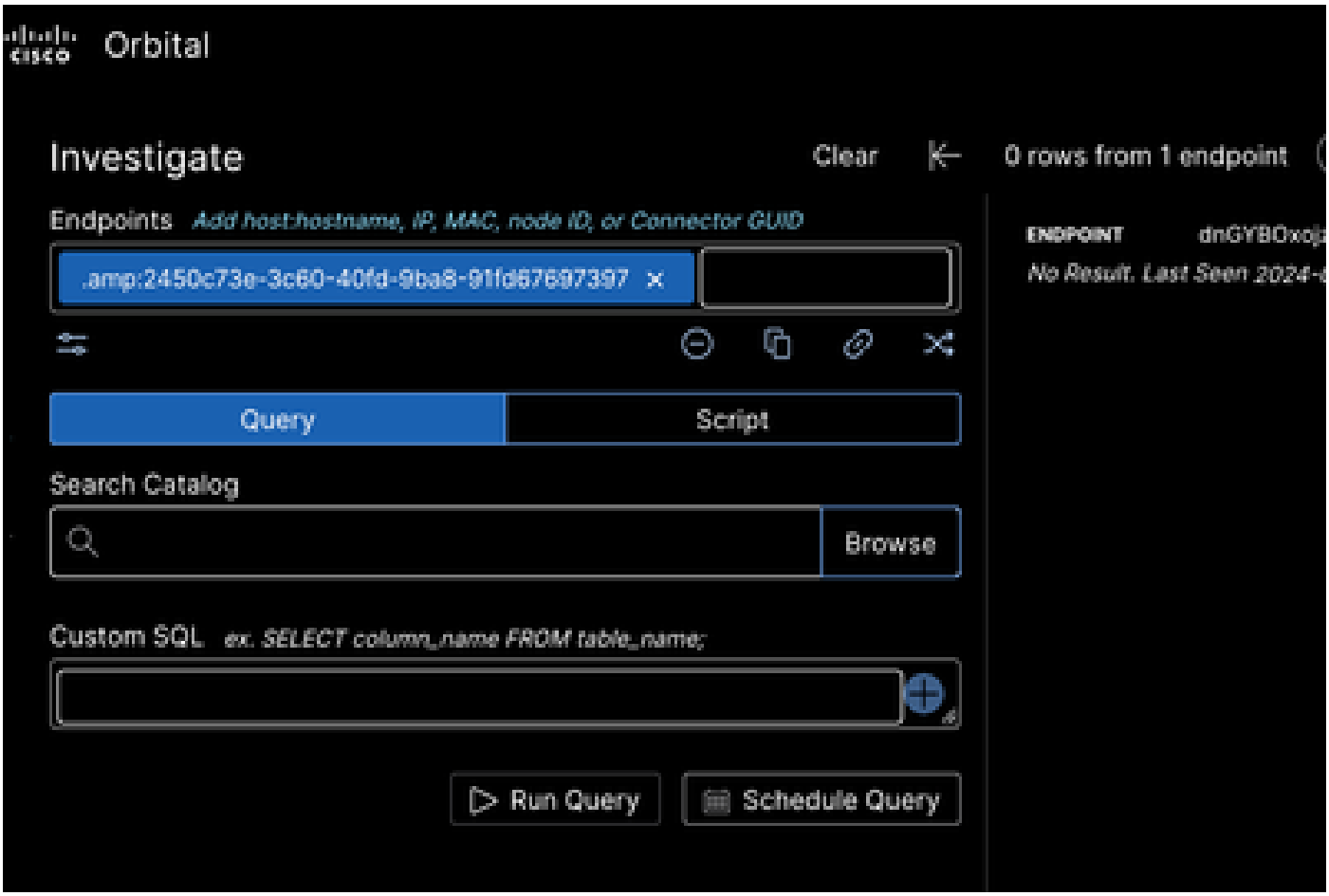
Europa: https://orbital.eu.amp.cisco.com

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

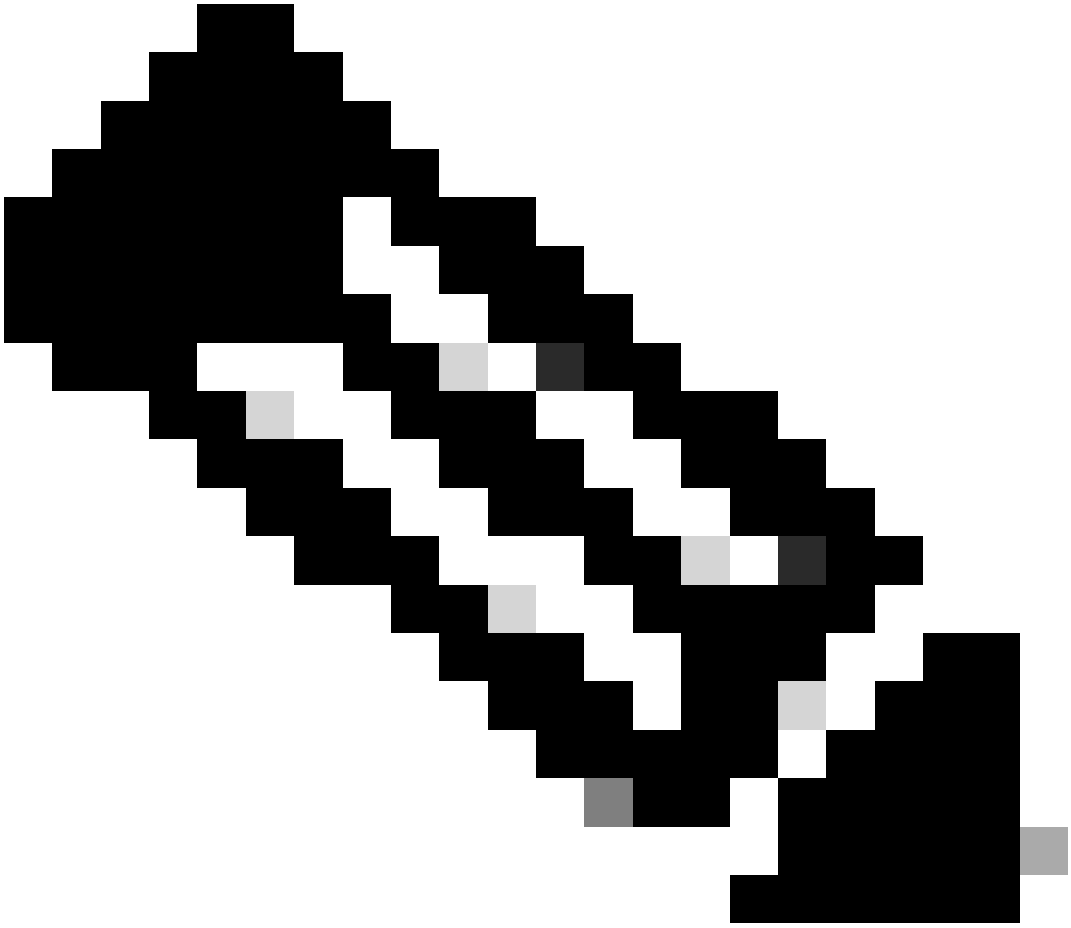
O bien

En Secure Endpoint Console, elija el sistema host afectado y haga clic en Investigate in Orbital.

Hay opciones para utilizar el Catálogo orbital (Haga clic en Browse) o Enter the Custom Queries bajo Custom SQL sección como se mencionó:



Consultas personalizadas



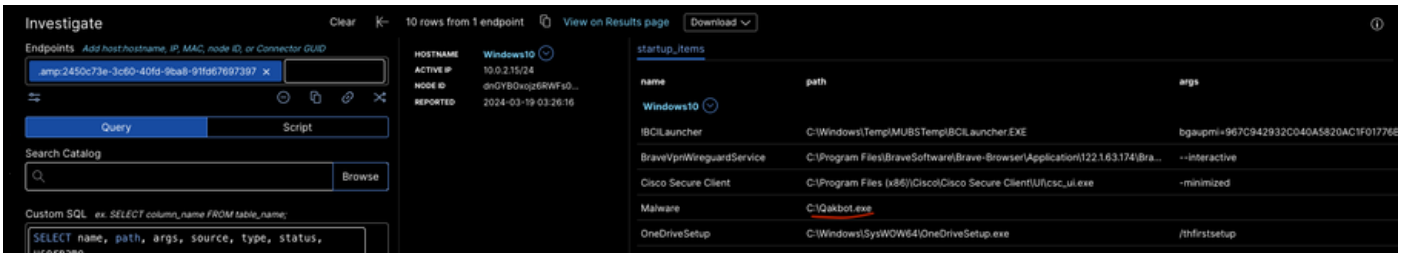
Nota: El sistema host se encuentra en la red de laboratorio y se intenta mantener el sistema/la red intactos.

---

1. Elementos de inicio

Los atacantes pueden aprovechar los elementos de inicio para mantener la persistencia en un sistema comprometido, lo que significa que el software malicioso seguirá ejecutándose o se reiniciará automáticamente con cada reinicio del sistema. En el siguiente ejemplo, Qakbot.exe se está ejecutando en el sistema host.

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



2. Hashes Sha256 de procesos en ejecución

Los hashes SHA256 no están inherentemente asociados con procesos en ejecución en su estado natural. Sin embargo, el software de seguridad y las herramientas de supervisión del sistema pueden calcular el hash SHA256 de un proceso en ejecución del archivo ejecutable para ayudar a comprobar su integridad y autenticidad.

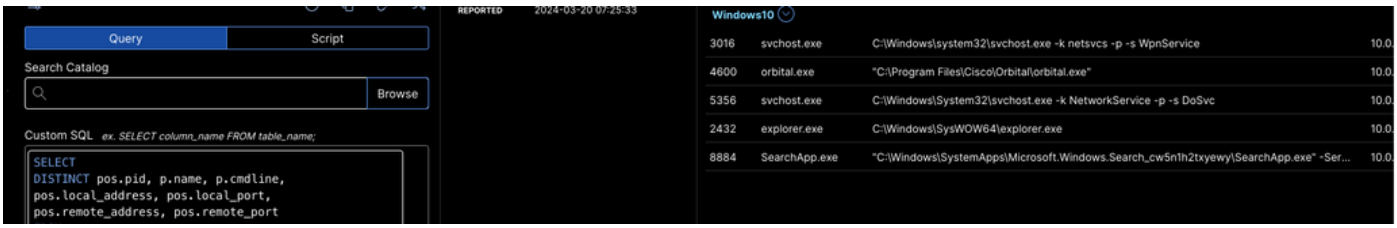
```
 SELECT
p.pid, p.name, p.path, p.cmdline, p.state, h.sha256
FROM processes p
INNER JOIN hash h
ON p.path=h.path;
```

si el hash asociado de un archivo es malicioso, podrá identificarse con esta consulta.

3. Proceso con conexiones de red

Los procesos con conexiones de red son programas o servicios del sistema que utilizan activamente la interfaz de red para comunicarse con otros dispositivos de una red o a través de 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. Proceso privilegiado con conexión de red de host no local

Programa o servicio en ejecución que tiene permisos elevados (como los de una cuenta de administrador o del sistema) y se comunica a través de la red con un dispositivo o servicio externo, lo que significa cualquier dirección IP distinta de 127.0.0.1 (host local) o ::1 (host local 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")
```

Una vez que tenga la lista de identificadores de paquetes (PID), puede agregarla en consecuencia en las 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
```

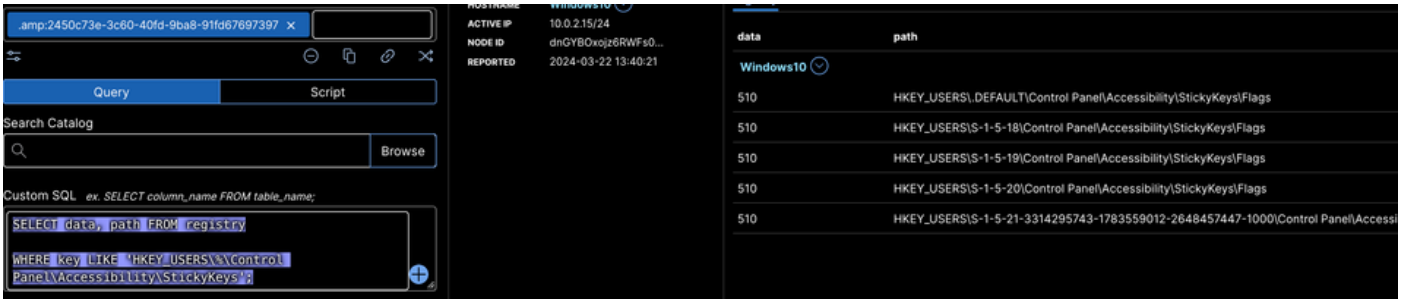
5. Copia de seguridad/Restauración de la supervisión del registro

Seguimiento de eventos en los que se realizan cambios en el Registro de Windows mediante operaciones de copia de seguridad o restauración. El Registro de Windows es una base de datos jerárquica que almacena opciones y valores de configuración en los sistemas operativos Microsoft

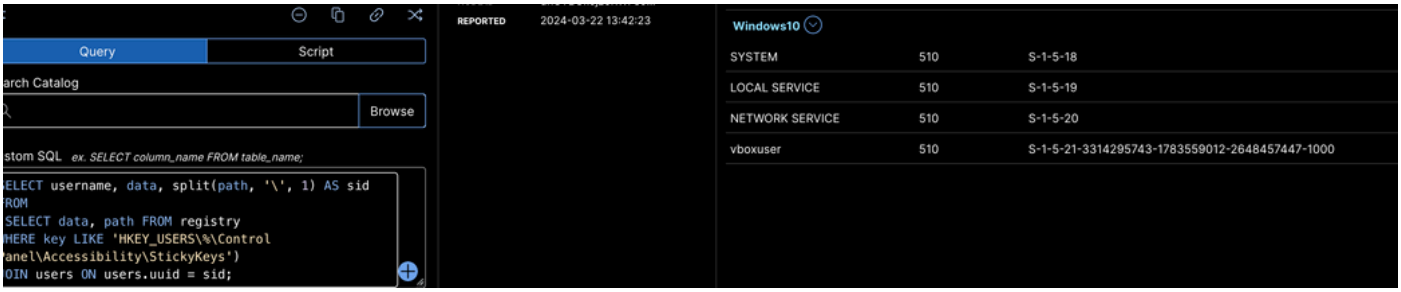
Windows.

```
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. Búsqueda de archivos

Permite a los usuarios localizar archivos y carpetas en su equipo mediante diversos criterios, como el nombre de archivo, el contenido, las propiedades o los metadatos.

```
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 hasta PARAMETERS > File Path y haga clic en %.dll o %.exe o %.png.

7. Supervisión del historial de Powershell

Práctica de realizar un seguimiento de los comandos que se han ejecutado en sesiones de PowerShell. La supervisión del historial de PowerShell puede ser especialmente importante por motivos de seguridad y cumplimiento.

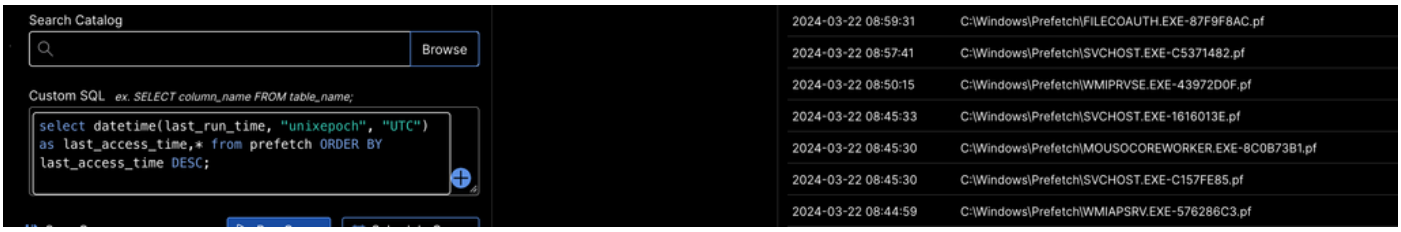
```
SELECT time, datetime, script_block_id, script_block_count, script_text, script_name, script_path
FROM orbital_powershell_events
ORDER BY datetime DESC
LIMIT 500;
```

8. Consulta de captura previa

Función de rendimiento que acelera la carga de aplicaciones. La captura previa implica analizar la forma en que se carga y ejecuta el software en un sistema y, a continuación, almacenar información sobre esto en archivos específicos.

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

```
ORDER BY last_access_time DESC;
```

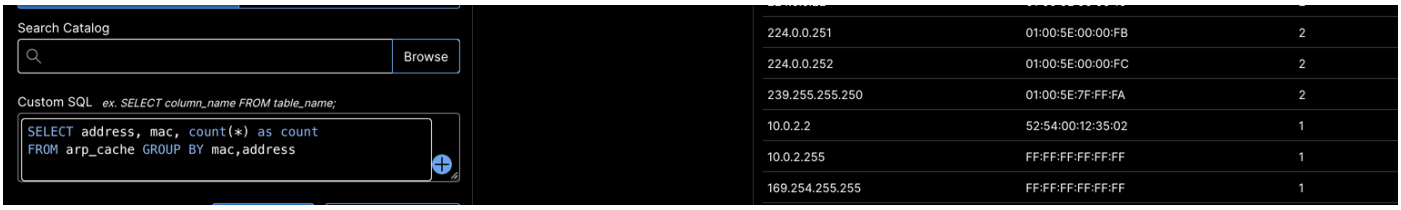


La captura previa es un mecanismo con el cual SQL Server puede activar muchas solicitudes de E/S en paralelo para una unión de loop anidado.

9. Inspección de caché del protocolo de resolución de direcciones (ARP)

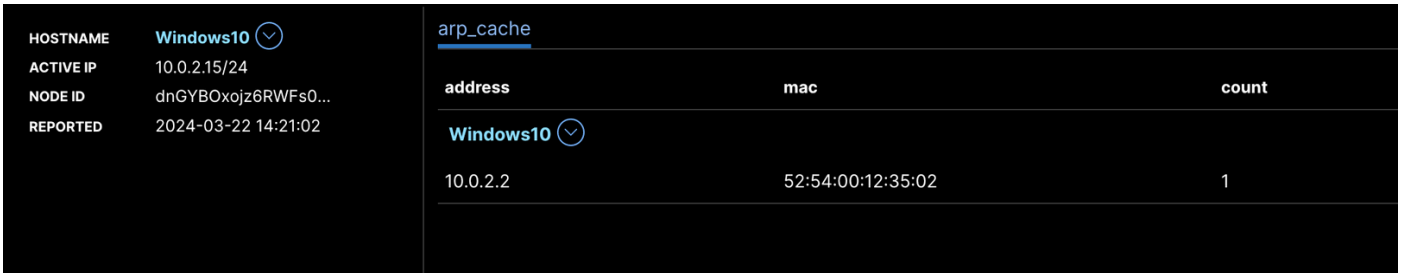
Implica examinar el contenido de la caché ARP en un equipo o dispositivo de red. La memoria caché ARP es una tabla que almacena las asignaciones entre las direcciones IP y sus direcciones MAC correspondientes.

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



En el siguiente ejemplo, se obtiene la dirección MAC sospechosa y su recuento de la memoria caché 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");
```



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).