Configure Windows Server to Forward DNS Requests to Umbrella

Contents

Introduction

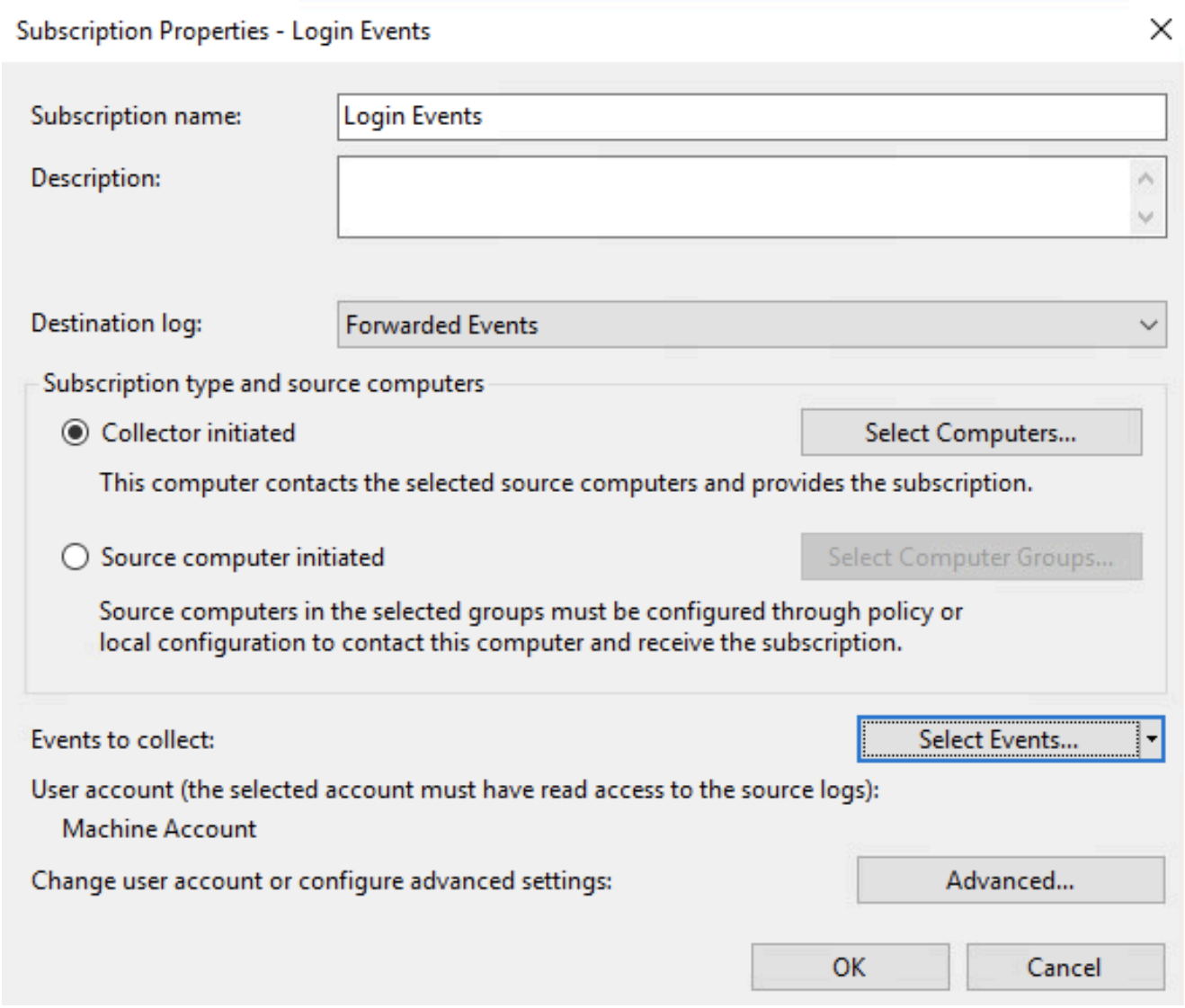
This document describes how to configure Windows Server to forward DNS requests to Umbrella for enhanced client protection and logging.

Overview

Windows Server can protect clients using a network identity by acting as a DNS forwarder. Domain Controllers or any other server with the DNS role may send DNS to Umbrella from a registered network.

Configuration Steps

1. Open **DNS Manager** (dnsmgmt.msc).
2. Right-click on the server name in the tree and select **Properties**.
3. Select the **Forwarders** tab.
4. Click **Edit...** and enter the Umbrella DNS server IP addresses.
5. Click **OK** in the Edit Forwarders window. The entries display in the list of forwarders.
6. Uncheck the box labeled **Use root hints if no forwarders are available**.



mceclip0.png

Best Practice Notes

- Ensure **Use root hints if no forwarders are available** remains unchecked. If checked, Umbrella protection and logging become inconsistent. For example, if a domain fails DNSSEC validation or is subject to a DDoS mitigation event, the Windows DNS server can consider Umbrella unresponsive and attempt direct recursion using root hints, bypassing Umbrella.

- Use only Umbrella as forwarders. Do not configure any third-party resolvers. Umbrella can only log and protect DNS queries it receives.

- For redundancy, configure all four Umbrella anycast IP addresses as forwarders as shown in the previous screenshot.

- If using Umbrella Sites and Virtual Appliances, point to a local Virtual Appliance as a forwarder instead of Umbrella anycast addresses.

    - Avoid request loops: If a Virtual Appliance lists your server as one of its local DNS servers, do

not add that Virtual Appliance as a forwarder.
    - A Virtual Appliance only sees the IP address of the DNS server, not the addresses of individual clients it serves.
    - If using Active Directory Integration with the Virtual Appliance, add the Windows DNS server IP as an exception. Navigate to **Deployments > Sites and Active Directory > Service Account Exceptions** in the Umbrella Dashboard and add the DNS server IP. This prevents incorrect attribution of user identities to server traffic.

- Do not add Umbrella servers to the **Root Hints** tab. Umbrella DNS servers are recursive resolvers and do not serve as roots for iterative lookups. Adding them as root hints results in undesirable behavior and bypass Umbrella protection and logging.