Understand Umbrella Policy Selection Involving Multiple Organizations

Contents

Introduction

This document describes the policies of multiple Umbrella organizations being considered in certain scenarios.

Overview

In certain scenarios, it is possible for the policies of multiple Umbrella organizations to be considered. An example of this would be a Roaming Client or Mobile device for one organization connecting to the Network of a different organization. This article details how the policy is currently chosen in this case, and what changes Umbrella intends to make in order to improve this behaviour.

Policy Selection with a Single Organization

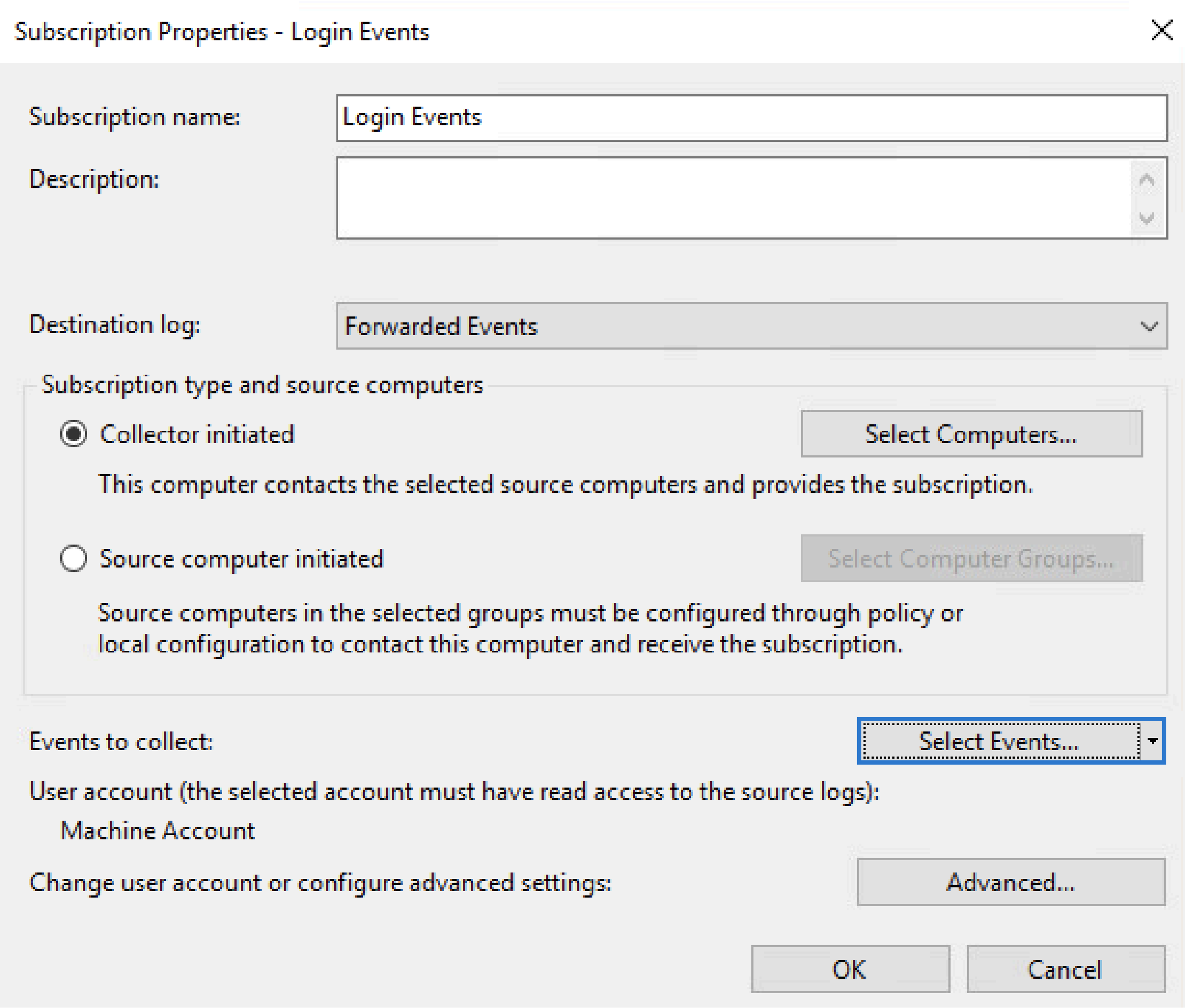
When a DNS query is sent to Umbrella, it is possible for multiple identities to be associated with the query. For example, a query from a Roaming Client (RC) behind a protected Network would include both the RC’s device ID as well as the IP address of the Network. Similarly, a query from a Virtual Appliance includes the Site ID, the Internal Network, the AD user, and the AD group.

Typically, the identities included in the query are all associated with a single organization. In this case, the policy enforced uses the policy precedence rules detailed in our documentation:

https://docs.umbrella.com/deployment-umbrella/docs/policy-precedence

In short, Umbrella assigns each policy a priority based on its order in the Dashboard , with the topmost policy having the highest priority. The Umbrella resolvers choose the highest priority policy which applies to at least one of the identities present in the query.

For example, Organization A may have these policies defined:



Subscription Properties - Login Events

Subscription name: Login Events

Description:

Destination log: Forwarded Events

Subscription type and source computers

● Collector initiated

This computer contacts the selected source computers and provides the subscription.

○ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

User account (the selected account must have read access to the source logs):

Machine Account

Change user account or configure advanced settings:

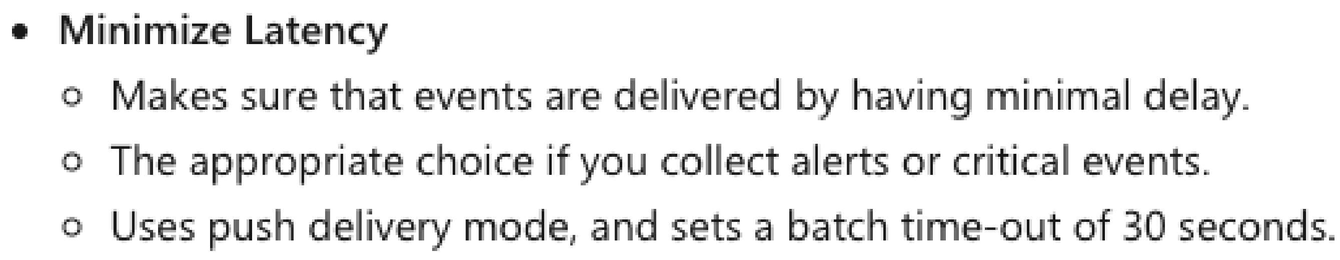
mceclip0.png

The Roaming Computer's policy has a priority of 2, while the Network's policy has a priority of 1. So, if a query comes in from a Roaming Computer that is joined to an external network, then Policy 2 would be applied. However, if the Roaming Computer was joined to one of Organization A's networks, then Policy 1 would apply, as the Network's policy has a higher priority.

Policy Selection with Multiple Organizations

This same logic is applied when there are identities from multiple organizations included in the query. However, because there are multiple organizations involved, it is the relative priority of each policy that is considered with respect to each organization's policy list.

An example explains this best. Organization A and Organization B each have these policies defined in their respective Umbrella Dashboards:



- Minimize Latency
  - Makes sure that events are delivered by having minimal delay.
  - The appropriate choice if you collect alerts or critical events.
  - Uses push delivery mode, and sets a batch time-out of 30 seconds.

mceclip2.png

A Roaming Computer from Organization A then joins a Network belonging to Organization B. The DNS query sent to Umbrella thus contains the Organization A’s RC’s device ID, and Organization B’s Network’s IP address.

Using the logic for a single organization, we get the priorities for each identity’s policy. The RC from Organization A gets policy A2, which has a priority of 2, while the Network from Organization B gets policy B1, which has a priority of 1. Thus, the policy for Organization B’s Network, policy B1, gets applied.

Reporting with Multiple Organizations

When a query contains identities from multiple organizations, the query only appears in the reports for the organization whose policy was selected. The reports for that organization ONLY shows the identities belonging to that organization. An organization NEVER has visibility into the other identities in the query that belong to other organizations.

Implications for the Current Policy Selection Behaviour

Due to the policy selection behaviour described, it is possible that an identity belonging to one organization can have their policy overridden by the policy of another organization. This includes all policy features, including security and content blocking, destination lists, block pages designs, and logging settings (noting the restrictions on reporting), with the exception of block page redirects.

Dedicated Block Pages for scenarios involving Multiple Organizations

As of July 16th, 2021, when the Umbrella resolvers detect that a query contains identities from multiple organizations, it redirects any blocked queries to a dedicated block page. This block page informs the user that more than one organization was detected, and thus that the query may have been blocked due to another organization’s policy.

Planned Changes for Policy Selection involving Multiple Organizations

Umbrella plans on changing the behaviour of policy selection when more than one organization is involved. Future changes include:

Policy Selection Behaviour

Umbrella modifies the policy selection behaviour so that the highest priority policy for each organization is selected and enforced. Then, if any of those policies would block the query, the query is blocked. This allows all organizations involved to ensure that their policies are not being bypassed. This behaviour can be best explained using an analogy:

Alice’s parents say that her individual rules are more important than house rules. Alice isn’t allowed to eat ice cream, anytime, anywhere.

Bob’s parents say that house rules are more important than individual rules. They don’t allow pizza in their house, ever.

***Current model**:*

Alice goes to Bob’s house. Bob’s house rules apply and not Alice’s individual rules. Alice can eat ice cream, but not pizza. Bob’s parents get a report that says someone ate ice cream in their house, but it doesn’t say it was Alice by name.

***Proposed model**:*

Alice goes to Bob’s house. Bob’s house rules apply, and Alice’s individual rules apply. Alice has no ice cream nor pizza. Bob’s parents get a report that says someone was denied pizza and ice cream, but it doesn’t say it was Alice by name.

Reporting for all Involved Organizations

When the policy selection behaviour is in place, Umbrella additionally ensures that any queries involving identities from multiple organizations are included in the reports of all involved organizations. The reports ONLY include identities belonging to that organization – a given organization NEVER sees the identities of another organization.