Comprendre la sélection de politiques générales impliquant plusieurs organisations

Table des matières

Introduction

Ce document décrit les politiques de plusieurs organisations-cadres prises en compte dans certains scénarios.

Aperçu

Dans certains scénarios, il est possible d'envisager les politiques de plusieurs organisations-cadres. Par exemple, un client itinérant ou un périphérique mobile pour une organisation se connectant au réseau d'une autre organisation. Cet article explique en détail comment la politique est actuellement choisie dans ce cas, et quels changements Umbrella entend apporter afin d'améliorer ce comportement.

Sélection d'une stratégie avec une seule organisation

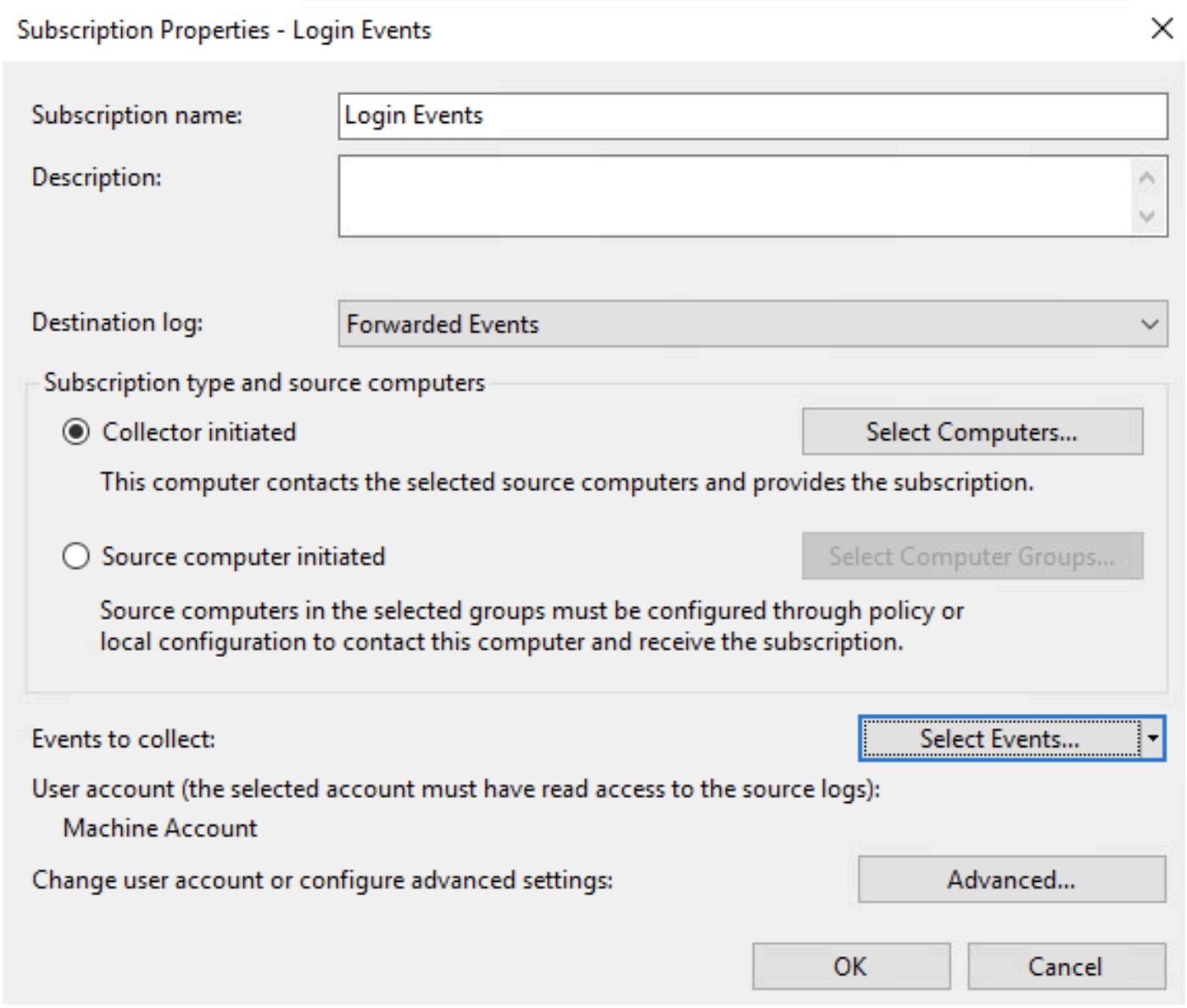
Lorsqu'une requête DNS est envoyée à Umbrella, il est possible que plusieurs identités soient associées à la requête. Par exemple, une requête d'un client d'itinérance (RC) derrière un réseau protégé inclurait à la fois l'ID de périphérique du RC et l'adresse IP du réseau. De même, une requête provenant d'une appliance virtuelle inclut l'ID de site, le réseau interne, l'utilisateur Active Directory et le groupe Active Directory.

En général, les identités incluses dans la requête sont toutes associées à une seule organisation. Dans ce cas, la stratégie appliquée utilise les règles de priorité de stratégie détaillées dans notre documentation :

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

En bref, Umbrella attribue une priorité à chaque stratégie en fonction de son ordre dans le tableau de bord , la stratégie la plus élevée ayant la priorité la plus élevée. Les résolveurs Umbrella choisissent la politique de priorité la plus élevée qui s'applique à au moins une des identités présentes dans la requête.

Par exemple, l'organisation A peut définir les politiques suivantes :



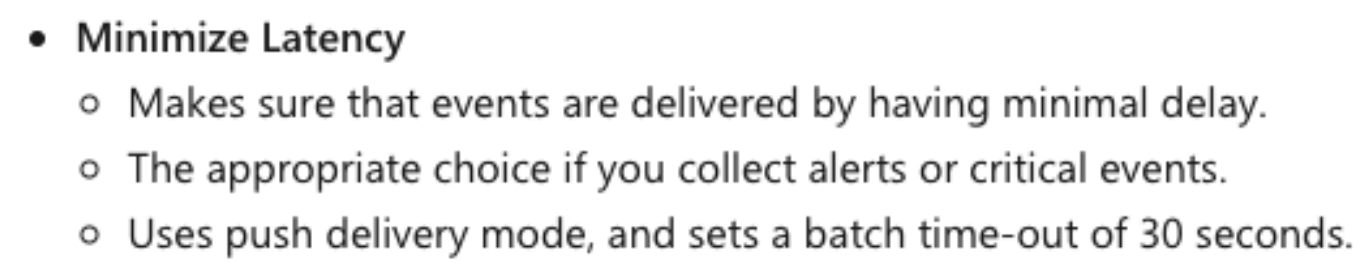
mceclip0.png

La stratégie de l'ordinateur itinérant a une priorité de 2, tandis que la stratégie du réseau a une priorité de 1. Par conséquent, si une requête provient d'un ordinateur itinérant qui est joint à un réseau externe, la stratégie 2 est appliquée. Toutefois, si l'ordinateur itinérant était connecté à l'un des réseaux de l'organisation A, la stratégie 1 s'appliquerait, car la stratégie du réseau a une priorité plus élevée.

Sélection de politiques avec plusieurs organisations

Cette même logique s'applique lorsqu'il existe des identités de plusieurs organisations incluses dans la requête. Cependant, comme il y a plusieurs organisations impliquées, c'est la priorité relative de chaque politique qui est prise en compte par rapport à la liste de politiques de chaque organisation.

Un exemple explique ce mieux. L'organisation A et l'organisation B ont chacune ces politiques définies dans leurs tableaux de bord parapluie respectifs :



mceclip2.png

Un ordinateur itinérant de l'organisation A rejoint ensuite un réseau appartenant à l'organisation B. La requête DNS envoyée à Umbrella contient donc l'ID de périphérique RC de l'organisation A et l'adresse IP du réseau de l'organisation B.

En utilisant la logique d'une seule organisation, nous obtenons les priorités de la politique de chaque identité. Le RC de l'organisation A reçoit la stratégie A2, qui a une priorité de 2, tandis que le réseau de l'organisation B reçoit la stratégie B1, qui a une priorité de 1. Ainsi, la stratégie du réseau de l'organisation B, la stratégie B1, est appliquée.

Création de rapports avec plusieurs organisations

Lorsqu'une requête contient des identités de plusieurs organisations, elle apparaît uniquement dans les états de l'organisation dont la stratégie a été sélectionnée. Les états de cette organisation n'affichent que les identités appartenant à cette organisation. Une organisation n'a JAMAIS la visibilité sur les autres identités de la requête qui appartiennent à d'autres organisations.

Implications pour le comportement actuel de sélection des stratégies

En raison du comportement de sélection de stratégie décrit, il est possible qu'une identité appartenant à une organisation puisse avoir sa stratégie remplacée par la stratégie d'une autre organisation. Cela inclut toutes les fonctionnalités de stratégie, y compris le blocage de la sécurité et du contenu, les listes de destinations, les conceptions de pages de blocage et les paramètres de journalisation (en notant les restrictions sur la création de rapports), à l'exception des redirections de pages de blocage.

Pages de blocage dédiées pour les scénarios impliquant plusieurs organisations

À compter du 16 juillet 2021, lorsque les résolveurs Umbrella détectent qu'une requête contient des identités de plusieurs organisations, ils redirigent toutes les requêtes bloquées vers une page de blocage dédiée. Cette page de blocage informe l'utilisateur que plusieurs organisations ont été détectées et que la requête a peut-être été bloquée en raison de la stratégie d'une autre organisation.

Modifications planifiées pour la sélection de politiques impliquant plusieurs organisations

L'organisme-cadre prévoit modifier le comportement de la sélection des politiques lorsque plus d'une organisation est concernée. Les changements futurs comprennent :

Comportement de sélection de stratégie

Umbrella modifie le comportement de sélection des stratégies afin que la stratégie de priorité la plus élevée pour chaque organisation soit sélectionnée et appliquée. Ensuite, si l'une de ces stratégies bloque la requête, elle est bloquée. Cela permet à toutes les organisations impliquées de s'assurer que leurs politiques ne sont pas contournées. Ce comportement peut être mieux expliqué à l'aide d'une analogie :

Les parents d'Alice disent que ses règles individuelles sont plus importantes que les règles de la maison. Alice n'est pas autorisée à manger de la crème glacée, n'importe quand, n'importe où.

Les parents de Bob disent que les règles domestiques sont plus importantes que les règles individuelles. Ils n’autorisent jamais la pizza chez eux.

Modèle actuel :

Alice se rend chez Bob. Elle est morte. Les règles de la maison de Bob s'appliquent et non les règles individuelles d'Alice. Alice peut manger de la glace, mais pas de la pizza. Les parents de Bob reçoivent un rapport qui dit que quelqu’un a mangé de la crème glacée dans leur maison, mais il ne dit pas que c’était Alice par son nom.

Modèle proposé :

Alice se rend chez Bob. Elle est morte. Les règles de la maison de Bob s'appliquent et les règles individuelles d'Alice s'appliquent. Alice n'a ni glace ni pizza. Les parents de Bob reçoivent un rapport qui dit que quelqu’un s’est vu refuser une pizza et une crème glacée, mais il ne dit pas que c’était Alice par son nom.

Création de rapports pour toutes les organisations concernées

Lorsque le comportement de sélection des stratégies est en place, Umbrella s'assure également que toutes les requêtes impliquant des identités de plusieurs organisations sont incluses dans les rapports de toutes les organisations impliquées. Les rapports incluent UNIQUEMENT les identités appartenant à cette organisation - une organisation donnée ne voit JAMAIS les identités d'une autre organisation.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.