Comprender los eventos de ventana/EventID leídos por un conector

Contenido

Introducción

En este documento se describen los eventos de ventana/eventID que lee un conector de forma predeterminada.

Overview

Técnicamente, el dispositivo virtual Umbrella (VA) solo tiene visibilidad de qué dirección IP de origen recibe una consulta DNS. Para que un usuario se asocie con la solicitud DNS, el VA funciona junto con el conector, lo que da lugar a una asignación de usuario a IP.

El conector lee los eventos con ID de evento específicos de los registros de eventos de seguridad de los controladores de dominio. A continuación, se analizan estos eventos y se envían el nombre de usuario y la dirección IP de origen al dispositivo virtual, que crea una asignación entre esa IP de origen y el usuario.

Si los controladores de dominio no están auditando estos eventos, el proceso de asignación de VA no puede llevarse a cabo correctamente. En este artículo se describe exactamente el tipo de ID de evento que el conector observa de forma predeterminada.

IDevento	Descripción
4624	El evento 4624 documenta todos y cada uno de los intentos correctos de iniciar sesión en el equipo local, independientemente del tipo de inicio de sesión, la ubicación del usuario o el tipo de cuenta.
528	El evento 528 se registra cada vez que una cuenta inicia sesión en el equipo local, excepto en el caso de los inicios de sesión en la red. El evento 528 se registra tanto si la cuenta utilizada para el inicio de sesión es una cuenta SAM local como una cuenta de dominio.
540	El evento 540 se registra cuando un usuario de otro lugar de la red se conecta a

	un recurso (como una carpeta compartida) proporcionado por el servicio Servidor de este equipo.
4768	Este evento solo se registra en controladores de dominio y se registran tanto las instancias correctas como las incorrectas de este evento.
4769	Windows utiliza este ID de evento para las solicitudes de vales de servicio correctas y fallidas.

Si el conector no puede leer los eventos directamente desde los Registros de eventos de seguridad del controlador de dominio, puede generar un vale de soporte con Umbrella solicitando que se cambie a la suscripción WMI. En el caso de las suscripciones WMI, el conector se suscribe a todos los eventos enumerados anteriormente. Además, el conector también se suscribe a los eventos de cierre de sesión con EventID, como se indica a continuación. Tenga en cuenta que, de forma predeterminada, el conector no lee estos eventos de cierre de sesión de los registros de eventos de seguridad.

IDevento	Descripción
538	El evento 538 se registra cada vez que un usuario cierra la sesión, ya sea desde una conexión de red, un inicio de sesión interactivo u otro tipo de inicio de sesión (consulte el evento 528 para ver un gráfico de los tipos de inicio de sesión).
4647	Este evento señala el final de una sesión de inicio de sesión y se puede correlacionar con el evento de inicio de sesión 4624 mediante el ID de inicio de sesión.
4634	Este evento también indica el final de una sesión de inicio de sesión y puede relacionarse con el evento de inicio de sesión 4624 mediante el ID de inicio de sesión.

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).