

Usar y administrar VMware NSX Intelligence

Última actualización: 17 de mayo de 2022
VMware NSX Intelligence 3.2



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

<https://docs.vmware.com/es/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Botí 26
2.^a planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2021-2022 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Usar y administrar VMware NSX Intelligence 6

1 Introducción a NSX Intelligence 7

- Paseo por la página de inicio de NSX Intelligence 8
- Familiarizarse con los elementos gráficos de NSX Intelligence 11

2 Descripción de las vistas y los flujos de NSX Intelligence 14

- Trabajar con la vista Grupos 15
- Trabajar con la vista Recursos informáticos 21
- Trabajar con los flujos de tráfico 26

3 Trabajar con recomendaciones de NSX Intelligence 29

- Información sobre las recomendaciones de NSX Intelligence 29
- Cómo se generan las recomendaciones de NSX Intelligence 30
- Generar una nueva recomendación de NSX Intelligence 32
- Volver a ejecutar las recomendaciones de NSX Intelligence 38
- Revisar y publicar recomendaciones generadas de NSX Intelligence 40
- Exportar NSX Intelligence como archivo JSON 44

4 Detectar tráfico de red sospechoso en NSX-T Data Center 47

- Introducción a la detección de tráfico de red sospechoso en NSX-T Data Center 47
- Requisitos previos para usar la función Tráfico sospechoso de NSX 47
- Requisitos del sistema para la función Tráfico sospechoso de NSX 48
- Descripción general de la función Tráfico sospechoso de NSX 49
- Terminología utilizada con la función Tráfico sospechoso de NSX 51
- Activar los detectores de Tráfico sospechoso de NSX 51
- Análisis de los eventos de detección de Tráfico sospechoso de NSX 53
- Administrar las definiciones de detectores de Tráfico sospechoso de NSX 57

5 Trabajar con la aplicación NSX Network Detection and Response 60

- Requisitos previos para usar la aplicación NSX Network Detection and Response 60
- Terminología utilizada con la función NSX Network Detection and Response 61
- Introducción a la interfaz de usuario de NSX Network Detection and Response 62
- Explorar la página del panel de control 65
 - Campañas activas en mi red 66
 - Resumen de redes y seguridad 66
 - Amenazas detectadas 67
 - Mapa de eventos global 68

Nuevas detecciones únicas	69
Lista de archivos descargados	69
Administrar la página Campañas	71
Trabajar con tarjetas de campaña	72
Acerca del widget Investigar	73
Página Detalles de la campaña	74
Detalles de la campaña: pestaña Descripción general	75
Detalles de la campaña: pestaña Hosts	81
Detalles de la campaña: pestaña Escala de tiempo	81
Detalles de la campaña: pestaña Historial	82
Detalles de la campaña: pestaña Evidencia	82
Propiedades de la campaña	84
Trabajar con la página Hosts	93
Filtrar accesos directos	93
Usar filtros en la página Host	94
Lista de hosts	95
Página de perfil de host	98
Perfil de host: pestaña Descripción general	98
Perfil de host: pestaña Amenazas	99
Perfil de host: pestaña Eventos	104
Perfil de host: pestaña Descargas de archivos	105
Trabajar con la página Eventos	106
Mapa de eventos global	107
Amenazas detectadas en la página Eventos	107
Usar filtros en la página Eventos	109
Eventos de detección	110
Barra lateral de resumen de eventos	111
Ventana emergente WHOIS	114
Ventana emergente de documentación del detector	114
Página de perfil del evento	115
Administrar la página Incidentes	119
Infecciones a lo largo del tiempo	120
Amenazas detectadas	121
Usar filtros en la página Incidentes	122
Lista de incidentes	124
Trabajar con la página de archivos descargados	128
Pestaña Único	129
Archivos descargados a lo largo del tiempo	129
Usar filtros en la página Archivos descargados	130
Lista de archivos descargados únicos	131
Detalles de archivos descargados	132

Pestaña Todo	136
Uso de la página de administración de alertas	139
Trabajar con la barra lateral Administrar alerta	140
Sintaxis de reglas de alerta	143
Uso del informe Análisis	148
Informe de análisis: pestaña Descripción general	148
Informe de análisis: pestaña Informe	151
Widget Relaciones del análisis	152
Informe de archivos de análisis	153
Actividades de archivo de análisis	154
Artefactos de archivo de análisis	155
Informe de URL de análisis	156
6 Administración y operaciones de NSX Intelligence	158
Control de acceso basado en funciones en NSX Intelligence	158
Recopilar paquetes de soporte de NSX Intelligence	160
Búsqueda de entidades de NSX Intelligence	161
Buscar entidades de NSX Intelligence	163
Administrar la configuración de NSX Intelligence	165
Administrar los rangos de IP privadas para NSX Intelligence	166
7 Solucionar problemas relacionados con el uso de NSX Intelligence	168
Comprobar el estado de la función NSX Intelligence	168
Hay servicios degradados después de una activación correcta de NSX Intelligence	169
Incoherencias en los informes de topología incremental	170
La información de flujo de FTP aún se muestra después de que se detenga la sesión de FTP	171
La vista Grupos no se actualiza con los datos de flujo de tráfico	172

Usar y administrar VMware NSX Intelligence

El documento *Usar y administrar VMware NSX Intelligence* incluye información sobre cómo utilizar y administrar la función VMware NSX® Intelligence™.

Público objetivo

Esta información está destinada a cualquier usuario que tenga permiso para usar y administrar la función NSX Intelligence. La información se proporciona a administradores de sistemas con experiencia que estén familiarizados con la tecnología de virtualización y las operaciones de seguridad de red.

Documentación relacionada

- Documentación de VMware NSX-T Data Center™ 3.2 o versiones posteriores en <https://docs.vmware.com/es/VMware-NSX-T-Data-Center/index.html>.
Use la interfaz de usuario de NSX Manager para instalar y configurar la función VMware NSX® Intelligence™.
- Documento *Implementar y administrar VMware NSX Application Platform* incluido en la documentación de NSX-T Data Center 3.2 o versiones posteriores disponible en <https://docs.vmware.com/es/VMware-NSX-T-Data-Center/index.html>.
Primero debe implementar VMware NSX® Application Platform antes de activar la función NSX Intelligence.
- Documento *Activar y actualizar VMware NSX Intelligence* de la versión 3.2 o posterior para obtener información sobre cómo activar y actualizar la función NSX Intelligence.
Este documento está incluido en la documentación de NSX Intelligence disponible en <https://docs.vmware.com/es/VMware-NSX-Intelligence/index.html>.
- *Guía de activación y administración de VMware NSX Network Detection and Response* para obtener información sobre cómo activar y administrar la función VMware NSX® Network Detection and Response™.
Este documento está incluido en la documentación de NSX Intelligence disponible en <https://docs.vmware.com/es/VMware-NSX-Intelligence/index.html>.

Introducción a NSX Intelligence

1

Para comenzar a utilizar la función VMware NSX® Intelligence™, debe activarla y, a continuación, familiarizarse con la interfaz de usuario de NSX Intelligence.

Descripción general

A partir de la versión 3.2, NSX Intelligence pasó de ser un dispositivo basado en máquinas virtuales a ser una aplicación moderna alojada en VMware NSX® Application Platform, una plataforma basada en una arquitectura de microservicios.

La función NSX Intelligence ofrece una visualización de la postura de seguridad del entorno de VMware NSX-T Data Center™ local. La visualización utiliza los flujos de tráfico de red agregados dentro del período de tiempo especificado.

La función NSX Intelligence también le ayuda a planificar la microsegmentación realizando recomendaciones de reglas de firewall que usan análisis de tráfico de red con la aplicación de directivas de seguridad.

Además, la función Tráfico sospechoso de NSX y la función VMware NSX® Network Detection and Response™ están disponibles para su uso a partir de NSX Intelligence 3.2. Estas dos funciones utilizan análisis de tráfico de red para detectar actividades de tráfico de red sospechosas que se producen en el entorno de NSX-T Data Center 3.2 o versiones posteriores. Debe tener una licencia válida equivalente a NSX Firewall con Advanced Threat Prevention Edition para utilizar estas funciones.

Requisitos previos

Antes de poder utilizar las funcionalidades de NSX Intelligence disponibles, debe activar la función NSX Intelligence en NSX Application Platform. También debe configurar desde qué hosts o clústeres de hosts debe recopilar los datos de tráfico de red la función NSX Intelligence. De forma predeterminada, la función NSX Intelligence recopila datos de tráfico de red de todos los hosts y clústeres conocidos de los hosts del entorno de NSX-T Data Center. Consulte *Activar y actualizar VMware NSX Intelligence* para obtener más información.

Empezar a utilizar la función NSX Intelligence

Después de activar y configurar la función NSX Intelligence, las funcionalidades de visualización, recomendación y tráfico sospechoso pasan a estar disponibles en la interfaz de usuario de NSX Manager.

- Para ver las entidades de NSX-T visualizadas y los flujos de tráfico que se produjeron entre ellas, haga clic en **Planificar y solucionar problemas > Detectar y realizar acción**. Consulte [Capítulo 2 Descripción de las vistas y los flujos de NSX Intelligence](#).
- Para obtener recomendaciones de reglas de firewall distribuido para la planificación de microsegmentación, utilice **Planificar y solucionar problemas > Recomendaciones**. Consulte [Capítulo 3 Trabajar con recomendaciones de NSX Intelligence](#).
- Para usar la función Tráfico sospechoso de NSX para detectar eventos de tráfico sospechosos, haga clic en **Seguridad > Tráfico sospechoso**. Si la función NSX Network Detection and Response está activada, los eventos sospechosos detectados se marcarán y se enviarán al servicio de nube de VMware NSX® Advanced Threat Prevention. Si se detecta que los eventos de detección están relacionados, se correlacionarán con una campaña, que se puede investigar más a través de la interfaz de usuario de NSX Network Detection and Response. Consulte [Capítulo 4 Detectar tráfico de red sospechoso en NSX-T Data Center](#) para obtener detalles.

Este capítulo incluye los siguientes temas:

- [Paseo por la página de inicio de NSX Intelligence](#)
- [Familiarizarse con los elementos gráficos de NSX Intelligence](#)

Paseo por la página de inicio de NSX Intelligence

Para acceder a la página de inicio de NSX Intelligence, haga clic en **Planificar y solucionar problemas > Descubrir y realizar acción** en la interfaz de usuario de NSX Manager.

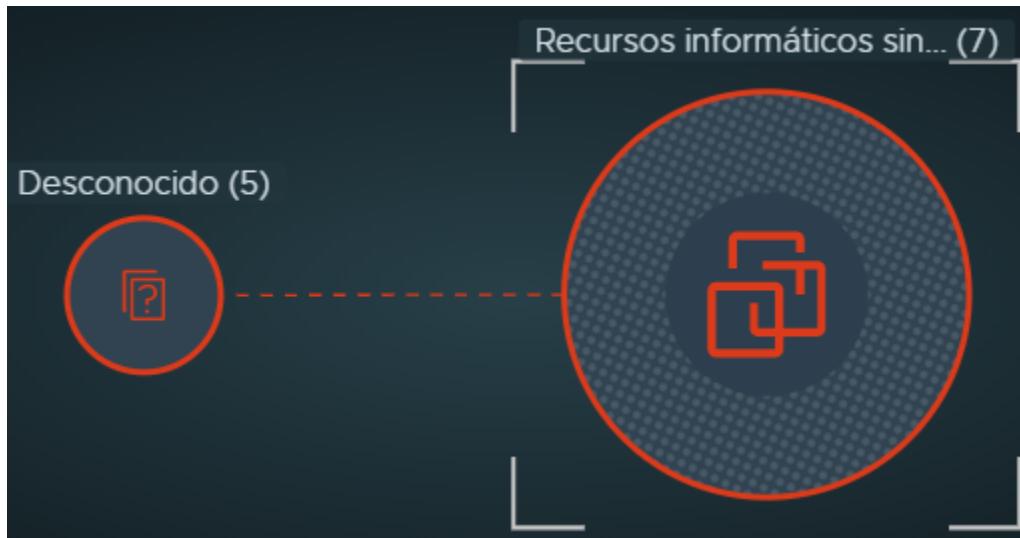
Después de activar y configurar NSX Intelligence por primera vez, al hacer clic en **Planificar y solucionar problemas > Detectar y realizar acción**, NSX Intelligence empezará a procesar algunas visualizaciones después de que se reciban algunos datos de tráfico de red de los nodos de transporte, así como información sobre el inventario de NSX Manager.

De forma predeterminada, al hacer clic en **Detectar y realizar acción**, se mostrará la visualización de la postura de seguridad de todos los grupos definidos en su inventario local de NSX-T Data Center.

- Si aún no hay ningún grupo definido, no se mostrarán grupos.
- Es posible que los grupos hayan tenido flujos de tráfico permitidos, bloqueados y sin protección entre sus entidades informáticas durante la última hora.
- Si hay máquinas virtuales o servidores físicos, pero no pertenecen a ningún grupo, verá el icono del grupo Recursos informáticos sin categorizar.

- Si hay direcciones IP que no pertenecen a ningún grupo, verá el icono Desconocido.

Los dos iconos de los grupos Recursos informáticos desconocidos y Sin categorizar se muestran en la siguiente imagen.



Si ya tiene grupos definidos y datos de tráfico de red capturado, es posible que se muestre una visualización similar a esta captura de pantalla. La siguiente tabla describe las secciones numeradas en la captura de pantalla.

Número	Descripción
1	Menú desplegable para 'Flujos' (Flows)
2	Botón para aplicar un filtro
3	Filtros para los tipos de flujo: Sin protección, Bloqueado, Permitido
4	Botón para ver los flujos actualizados recientemente
5	Botón para borrar la configuración
6	Botón para filtrar por la actividad más reciente
7	Icono que muestra 'Recursos informáticos sin...' (7)
8	Visualización de los flujos de red capturados
9	Botones para realizar acciones con el elemento seleccionado

Sección	Descripción
1	<p>El área de selección de la vista Seguridad es donde se selecciona el tipo de visualización de seguridad que se va a mostrar. Existen dos tipos de vistas de seguridad disponibles: Grupos y Recursos informáticos. Al hacer clic en Detectar y realizar acción, la vista de seguridad predeterminada que se muestra es la vista Grupos de todos los objetos de grupo en el entorno de NSX-T Data Center.</p> <ul style="list-style-type: none"> ■ Para seleccionar grupos específicos en la vista Grupos, haga clic en la flecha hacia abajo que aparece junto a TODO, seleccione un grupo en el menú desplegable y haga clic en Aplicar. ■ Para seleccionar la vista Recursos informáticos, haga clic en la flecha hacia abajo junto a Grupos, seleccione Recursos informáticos y haga clic en Aplicar. Se mostrarán todas las máquinas virtuales, las direcciones IP y los servidores físicos que existen en el entorno de NSX-T Data Center. ■ Para seleccionar las máquinas virtuales, las direcciones IP o los servidores físicos específicos que desea incluir en la vista Recursos informáticos, haga clic en la flecha hacia abajo que aparece junto a TODO, haga clic en Mostrar todos los tipos y seleccione un tipo de recurso informático (Máquinas virtuales, Direcciones IP o Servidores físicos) en el menú desplegable. También puede seleccionar o anular la selección de recursos informáticos específicos en el menú desplegable y hacer clic en Aplicar. ■ Para borrar las selecciones específicas en cualquiera de los tipos de vista, haga clic en Borrar en la parte superior derecha de la página de visualización y confirme haciendo clic en BORRAR en el cuadro de diálogo Borrar todos los filtros. Si hace clic en BORRAR en la vista Recursos informáticos, los filtros de selección se borrarán y se colocarán en la vista Grupos. <p>Consulte Trabajar con la vista Grupos y Trabajar con la vista Recursos informáticos para obtener más información sobre cómo trabajar con los dos tipos de vista.</p>
2	<p>En la sección Aplicar filtro puede ajustar los criterios utilizados para la visualización actual. Haga clic en Aplicar filtro, seleccione un criterio de filtro y haga clic en Aplicar. Para especificar varios filtros, haga clic de nuevo en Aplicar filtro.</p>
3	<p>En la sección Flujos puede seleccionar qué tipo de flujo de tráfico desea incluir en la visualización durante el período de tiempo seleccionado. En esta sección también se muestran los colores utilizados en la visualización de los tipos de flujo.</p> <ul style="list-style-type: none"> ■ Línea discontinua roja para los flujos Sin protección ■ Línea sólida azul para flujos Bloqueados ■ Línea sólida verde para los flujos Permitidos <p>De forma predeterminada, se seleccionan todos los tipos de flujo de tráfico para la visualización actual de NSX Intelligence. Consulte Trabajar con los flujos de tráfico para obtener más información.</p>
4	<p>La sección Estado de actualización proporciona información sobre la última vez que se actualizó el gráfico de visualización. Para forzar la actualización de la vista actual, haga clic en el ícono de actualización.</p>
5	<p>Al hacer clic en el ícono de engranaje, se proporcionarán vínculos a las siguientes páginas de configuración en el cuadro de diálogo Configuración relacionada con NSX Intelligence.</p> <ul style="list-style-type: none"> ■ Configuración específica para la función NSX Intelligence en Configuración del sistema > NSX Intelligence. Consulte Administrar la configuración de NSX Intelligence para obtener más información. ■ Ajustes de privacidad en Configuración general de seguridad > Privacidad. ■ Rangos de IP privadas en Configuración general de seguridad > Rangos de IP privados. Para obtener más información, consulte Administrar los rangos de IP privadas para NSX Intelligence.

Sección	Descripción
6	<p>En esta sección, seleccione el período de tiempo que se utilizará para determinar qué datos de flujo de red se usan para generar la visualización y recomendación deseadas. La selección determina los datos históricos que se utilizan en la vista Grupos o la vista Recursos informáticos. El período de tiempo va desde la hora actual hasta un determinado período de tiempo en el pasado.</p> <p>Ahora es el período de tiempo predeterminado utilizado. Esta opción muestra los datos de flujo de tráfico más recientes que capturó el sistema, hasta los millones de flujos de tráfico procesados más recientes.</p> <p>Para cambiar el período de tiempo seleccionado actualmente, haga clic en él y seleccione otro en el menú desplegable. Puede seleccionar Ahora, Última hora, Últimas 12 horas, Últimas 24 horas, Última semana, Últimas 2 semanas o Último mes.</p>
7	<p>Esta sección de lienzo muestra el gráfico de visualización de las posturas de seguridad de los grupos o las entidades informáticas en su entorno de NSX-T Data Center local. También incluye la visualización de los flujos de tráfico que se produjeron durante el período de tiempo seleccionado. En esta sección, puede colocar el cursor en un nodo específico o a una flecha de flujo para obtener detalles sobre esa entidad específica.</p> <p>Para obtener más información, consulte Familiarizarse con los elementos gráficos de NSX Intelligence y Capítulo 2 Descripción de las vistas y los flujos de NSX Intelligence.</p>
8	<p>Este minimapa es un mapa general de todo el gráfico de visualización. Cuando se amplían las entidades específicas que se muestran en el gráfico, el mapa parcial se actualiza para mostrar dónde se encuentra la vista actual en relación con el gráfico general. Al hacer clic en la ventana del minimapa y arrastrar la superposición rectangular opaca, también se actualiza la vista actual del gráfico de visualización.</p>
9	<p>Use estos botones de control de visualización para acercar y alejar la imagen, aplicar la relación de aspecto 1:1, cambiar el tamaño para ajustarse a la vista, y entrar o salir del modo de pantalla completa. También puede utilizar las teclas de acceso rápido del teclado para administrar los controles de visualización. Para mostrar la ventana Ayuda de los métodos abreviados de teclado, pulse Mayús+/-.</p> <p>Para desplazarse hasta una visualización usada anteriormente, utilice el botón Atrás del navegador web. Cuando esté en modo de pantalla completa, presione ESC para salir de este modo y utilizar el botón de retroceso del navegador web.</p>

Familiarizarse con los elementos gráficos de NSX Intelligence

La interfaz de usuario de NSX Intelligence incluye varios elementos gráficos para ayudar a visualizar las entidades de NSX-T Data Center, los flujos de tráfico y ciertas actividades en el entorno de NSX-T Data Center.

La siguiente tabla muestra un glosario de elementos gráficos de NSX-T Data Center que se pueden ver en un gráfico de visualización de NSX Intelligence.

Elemento gráfico	Descripción
	Este icono representa un grupo en el que se pueden aplicar directivas de seguridad, incluidas las reglas de firewall de este a oeste. Un grupo puede ser una colección de máquinas virtuales, servidores físicos o conjuntos de direcciones IP. Consulte Trabajar con la vista Grupos .
	Este es el icono usado para las máquinas virtuales que forman parte del entorno de NSX-T Data Center. Una máquina virtual puede pertenecer a más de un grupo. Consulte Trabajar con la vista Recursos informáticos .
	Este icono representa un servidor físico que forma parte de su entorno de NSX-T Data Center. Un servidor virtual puede pertenecer a más de un grupo. Consulte Trabajar con la vista Recursos informáticos .
	Este es el icono de las direcciones IP públicas de Internet. Si al menos una entidad informática del entorno de NSX-T Data Center se comunicó con una dirección IP pública durante el período de tiempo seleccionado, ese flujo de tráfico se incluirá en la visualización actual.
	Este icono representa una dirección IP, como una dirección IP de unidifusión, difusión o multidifusión, que participó en las actividades de tráfico de red dentro del entorno de NSX-T Data Center durante el período de tiempo seleccionado.
	Este icono de nodo se utiliza para el grupo de entidades informáticas (máquinas virtuales, servidores físicos o conjuntos de direcciones IP) que no pertenecen actualmente a un grupo.
	<p>Esta flecha representa un flujo de tráfico de red producido entre dos grupos o entidades informáticas durante un período de tiempo seleccionado. Existen tres tipos diferentes de flechas.</p> <ul style="list-style-type: none"> ■ una flecha roja discontinua para flujos sin protección ■ una flecha azul continua para flujos bloqueados ■ una flecha verde continua para flujos permitidos <p>Consulte Trabajar con los flujos de tráfico para obtener más información.</p>
	El nodo seleccionado como el nodo actual enfocado aparece rodeado de un círculo discontinuo. Es el nodo anclado durante el modo de selección y en la vista que se está mostrando.
	Este icono aparece en el borde de un nodo de grupo si el grupo se agregó al inventario de NSX-T Data Center durante el período de tiempo seleccionado. Si NSX-T Data Center detectó una nueva entidad informática, como una máquina virtual o un servidor físico, durante el período de tiempo seleccionado, el icono aparecerá en el borde del nodo de la entidad informática.

Elemento gráfico	Descripción
	<p>Este ícono aparece en el borde del nodo de grupo si el grupo se quitó del inventario de durante el período de tiempo seleccionado. Sus entidades informáticas se han podido eliminar o no.</p> <p>En el borde de un nodo de entidad informática , este ícono indica que la entidad informática se eliminó del inventario durante el período de tiempo seleccionado.</p> <p>Aunque una entidad informática o un grupo se eliminen del inventario, seguirá apareciendo en la visualización actual para mostrar una vista histórica que indique que la entidad informática se eliminó durante el período seleccionado.</p>
	<p>Este ícono aparece cada vez que vemos un grupo y entidades informáticas juntos. Por ejemplo, en una vista de grupos de análisis profundo o entidades informáticas relacionadas de un grupo.</p> <p>El ícono aparece en el borde de un nodo de entidad informática cuando la entidad informática se elimina del grupo actual que se está visualizando. Aparece en el borde de un nodo de una entidad informática en los siguientes casos.</p> <ul style="list-style-type: none"> ■ si la entidad informática se movió fuera del grupo que se está viendo actualmente durante el período de tiempo seleccionado ■ si, en algún momento durante el período de tiempo seleccionado, la entidad informática formó parte del grupo que se está viendo actualmente, pero ya no forma parte de ese grupo
	<p>Este ícono aparece en el borde de un nodo de entidad informática si la función Tráfico sospechoso de NSX detectó que la entidad informática formaba parte de una actividad de tráfico de red sospechosa durante el período de tiempo especificado. Consulte Capítulo 4 Detectar tráfico de red sospechoso en NSX-T Data Center para obtener detalles.</p>

Descripción de las vistas y los flujos de NSX Intelligence

2

La visualización de NSX Intelligence se compone de los grupos o las entidades informáticas y los flujos de tráfico de red que se produjeron con dichos grupos o entidades informáticas durante el período de tiempo seleccionado.

La función NSX Intelligence 3.2 o una versión posterior que se activa mediante NSX-T Data Center 3.2 o una versión posterior admite grupos con tipos de miembros que sean una máquina virtual, un servidor físico, una dirección IP o una combinación de esas entidades informáticas.

Importante La visualización que se muestra para un período de tiempo específico representa todos los flujos de tráfico de red y las actividades de carga de trabajo que se produjeron en NSX-T Data Center durante ese período de tiempo. Estas actividades incluyen la adición, la eliminación o el movimiento de entidades informáticas (máquinas virtuales, servidores físicos, conjuntos de direcciones IP) y grupos. Es posible que una máquina virtual aparezca más de una vez en la visualización. Por ejemplo, si una máquina virtual estaba conectada a un host ESXi que originalmente no estaba administrado, y el host se pasa a administrarse a través de VMware vCenter Server™ durante el período seleccionado, la máquina virtual aparecerá dos veces en la vista Recursos informáticos. De forma similar, si un host ESXi se desconecta de vCenter Server y se vuelve a agregar durante el mismo período de tiempo seleccionado, las máquinas virtuales asociadas al host aparecerán eliminadas y nuevas durante el período de tiempo seleccionado. En una vista Grupos, si una máquina virtual estaba en el grupo sin clasificar y se agregó un grupo durante el mismo período seleccionado, la máquina virtual aparecerá tanto en el grupo Sin clasificar como en su nuevo grupo.

La función NSX Intelligence admite grupos con máquinas virtuales, servidores físicos o direcciones IP. Si tiene otros tipos de miembros, es posible que la vista Grupos muestre solo flujos de tráfico correlacionados entre los grupos con tipos de miembros admitidos en lugar de grupos reales en la regla de seguridad.

El gráfico de visualización que se muestra se actualiza a medida que cambia la postura de seguridad en NSX-T Data Center. Por ejemplo, si se agrega un nuevo grupo, se mostrará un nuevo nodo de grupo en el lienzo de visualización sin necesidad de actualizar el navegador web. La sección Actualizar estado de la sección superior derecha del lienzo de virtualización muestra el momento en que se actualizó la vista por última vez.

Consulte en esta sección más información sobre cómo trabajar con la vista Grupos, la vista Recursos informáticos y los distintos tipos de flujo de tráfico.

Este capítulo incluye los siguientes temas:

- Trabajar con la vista Grupos
- Trabajar con la vista Recursos informáticos
- Trabajar con los flujos de tráfico

Trabajar con la vista Grupos

La vista Grupos se muestra en la página de inicio de NSX Intelligence de forma predeterminada. La vista Grupos muestra todos los grupos y los flujos de tráfico que se produjeron en la última hora.

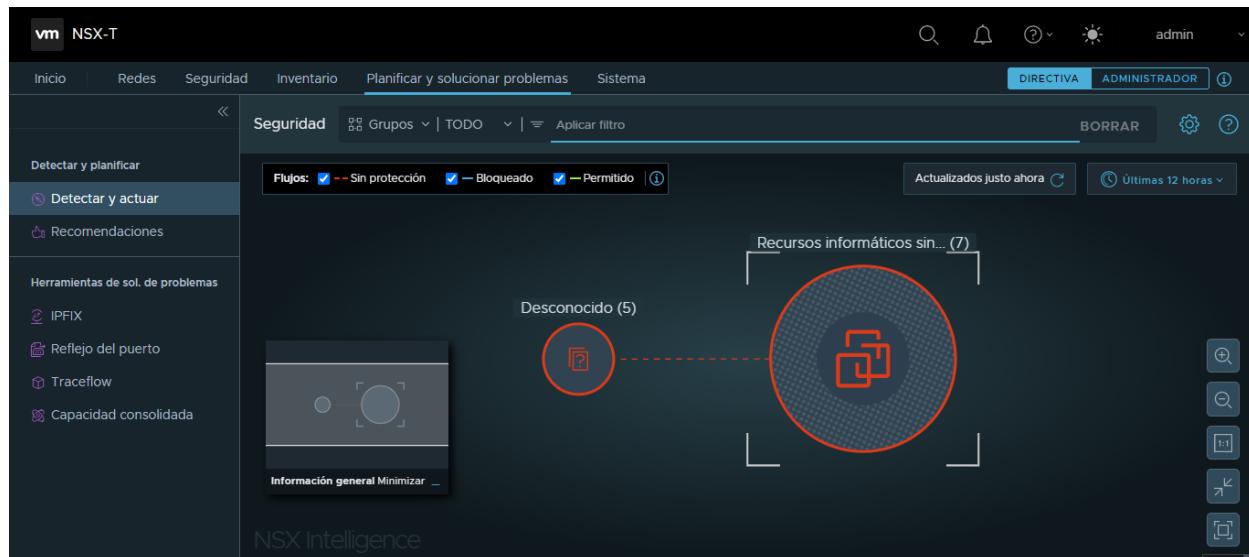
Ver selección

Si no ve la vista Grupos, haga clic en la flecha hacia abajo situada junto a la etiqueta **Recursos informáticos** en el área de selección de la vista Seguridad y seleccione **Grupos**. En el menú desplegable que se abre, puede seleccionar **Todos los grupos** o grupos específicos de la lista y, a continuación, hacer clic en **Aplicar**.

Utilice el cuadro de texto **Buscar** para filtrar la lista de grupos disponibles. Si sale del menú desplegable sin seleccionar nada o si selecciona **Todos los grupos**, se aplicará la opción **Todos los grupos** a la vista Grupos.

Nodos en una vista Grupos

Un nodo de una vista Grupos representa un grupo de entidades informáticas de NSX, como máquinas virtuales, servidores físicos y direcciones IP o un grupo de máquinas virtuales sin categorizar en su inventario de NSX-T Data Center. La vista Grupos también incluye nodos que representan entidades que se comunican con miembros de los grupos, pero que no forman parte de su inventario de NSX-T Data Center. En la siguiente captura de pantalla se muestra un ejemplo de una vista Grupos.



En la siguiente tabla se incluyen los tipos de nodos que se pueden ver en la vista Grupos.

Tipo de nodo de grupo	Icono	Descripción
Grupo normal		Un nodo de grupo normal en el gráfico de visualización de NSX Intelligence representa cualquier recopilación de entidades informáticas administradas en su entorno de NSX-T Data Center. El gráfico de NSX Intelligence admite grupos normales con entidades informáticas que incluyan máquinas virtuales, servidores físicos, direcciones IP o una combinación de dichas entidades. Una entidad de NSX puede pertenecer a más de un grupo y puede aparecer en más de un nodo de grupo normal.
Grupo sin categorizar		Un nodo de grupo sin clasificar representa una colección de entidades de NSX de recursos informáticos que no pertenecen a ningún grupo, pero no en el inventario de NSX-T Data Center.
Grupo desconocido		Un nodo de grupo desconocido representa un conjunto de entidades informáticas varias que no se encuentran en el inventario de NSX-T Data Center, pero se encuentran dentro del centro de datos y se comunican con una o varias entidades NSX en NSX-T Data Center.
Grupo de IP públicas		Un nodo de grupo de IP públicas representa una colección de direcciones IP públicas (IPv4 o IPv6) que se comunican con los objetos de NSX de NSX-T Data Center. Cualquier dirección IP que no pertenezca a ninguna de las anotaciones CIDR incluidas en Configuración de rango de IP privada para NSX Intelligence se clasifica como una dirección IP pública.

Tamaño y color del nodo

El tamaño de un nodo en la vista Grupos depende del número de miembros que pertenezcan a ese grupo. Cuanto más grande sea el tamaño del nodo del grupo, más entidades informáticas pertenecen a ese grupo. El nombre del grupo y su número total de miembros se muestran sobre el nodo.

El color del borde del nodo indica los tipos de flujos de tráfico que se produjeron en las entidades informáticas que pertenecen a ese grupo.

Tipo de nodo de grupo	Descripción
	Un nodo de grupo con un borde rojo indica que se detectó al menos un flujo de tráfico no protegido, independientemente de cuántos flujos permitidos o bloqueados se detectaron durante el período de tiempo seleccionado.
	Un borde azul en un nodo significa que no se detectaron flujos de tráfico no protegidos, pero que sí se detectó al menos un flujo bloqueado, independientemente de cuántos flujos permitidos se detectaran durante el período de tiempo seleccionado.

Tipo de nodo de grupo	Descripción
Un nodo con un borde verde indica que no se detectaron flujos sin protección ni bloqueados durante el período seleccionado, pero sí se detectó al menos un flujo permitido.	
Un nodo con un borde de color gris significa que, durante el período de tiempo seleccionado, no se detectó ningún flujo de tráfico para las entidades informáticas que pertenecen a ese grupo.	

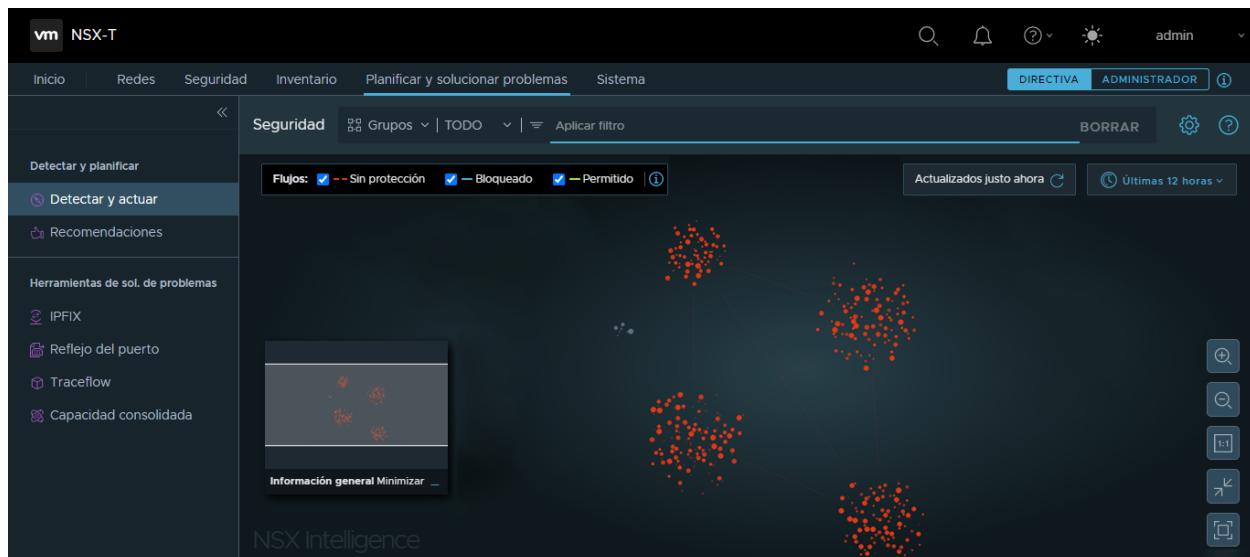
Flechas en una vista de grupos

Las flechas entre los nodos de grupo representan los flujos de tráfico que se han producido durante el período de tiempo seleccionado entre las entidades informáticas de esos nodos de grupo conectados. Una flecha de autorreferencia en un nodo de grupo indica que al menos una entidad informática se está comunicando con otra entidad informática dentro del mismo grupo. Consulte [Trabajar con los flujos de tráfico](#) para obtener más información.

Clústeres de nodos de grupo

Si se deben mostrar 100 o más nodos de grupo y 1000 o más flujos de tráfico, el gráfico de NSX Intelligence mostrará los nodos de grupo en clústeres. Estos clústeres de grupo se basan en la conectividad entre las entidades informáticas de esos grupos durante el período de tiempo seleccionado. La función de agrupar en clústeres ofrece una vista de alto nivel de las actividades en su entorno de NSX-T Data Center durante el período de tiempo seleccionado.

En la siguiente captura de pantalla se muestra un ejemplo de una visualización de clúster de grupos. Los colores de los nodos corresponden a los tipos de flujos de tráfico producidos en esos grupos durante el período de tiempo seleccionado. Los grupos que no tengan ningún miembro que se comunique con miembros de otros grupos durante el período de tiempo seleccionado se mostrarán juntos en un clúster independiente.



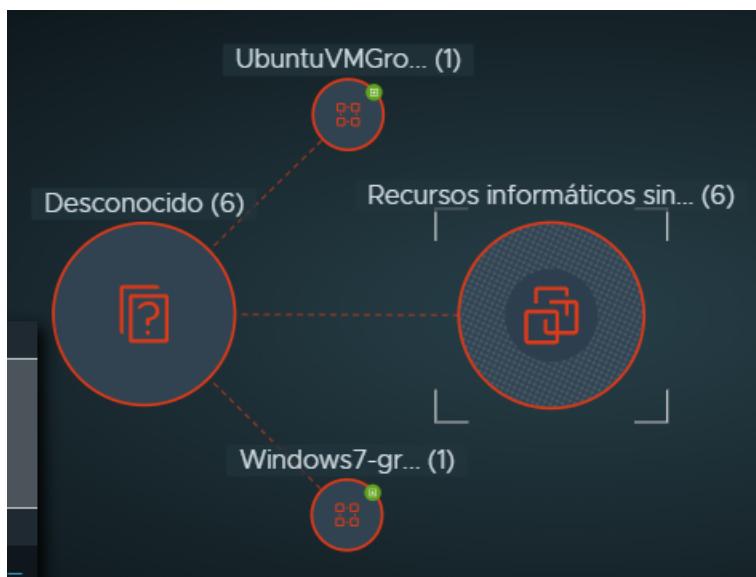
Al colocar el cursor sobre un clúster de grupo específico, se mostrará un número sobre el área del clúster. Este número indica cuántos grupos hay en esa visualización de clústeres en concreto. Para ver más detalles sobre un clúster específico y los grupos que forman parte de ese clúster, amplíe el gráfico. A medida que amplíe los nodos y las flechas, los detalles del flujo de tráfico y del grupo estarán más visibles y serán más fáciles de seleccionar. También puede aplicar filtros para delimitar los grupos que se muestran en el gráfico de visualización.

Selección de nodos en la vista Grupos

Si coloca el cursor sobre un nodo de grupo, se mostrará información sobre ese grupo, como puede verse en el siguiente ejemplo del grupo UbuntuVMGroup. Si el grupo se agregó durante el período de tiempo seleccionado, se mostrará un icono de la etiqueta Nuevo verde y los detalles de cuándo se creó el grupo. Se muestra el número total de flujos y el número y los tipos de flujos detectados durante el período de tiempo seleccionado. Si hay alguna, también se mostrará el número de recomendaciones disponibles para el grupo.



Al hacer clic en el nodo de un grupo, se marcará la selección con un círculo discontinuo como un nodo de máquina virtual anclado. Los otros grupos que están conectados al nodo de grupo seleccionado también se harán más visibles en la vista. Los demás nodos se atenuarán. Por ejemplo, en la siguiente captura de pantalla, el nodo UbuntuVMGroup está seleccionado y se convierte en el nodo de grupo anclado. El grupo de Recursos informáticos sin categorizar compartió al menos un flujo de tráfico con al menos un miembro de UbuntuVMGroup durante el período de tiempo seleccionado y, por lo tanto, también se destaca. Los demás grupos que no se comunicaron con UbuntuVMGroup aparecerán atenuados en la vista.

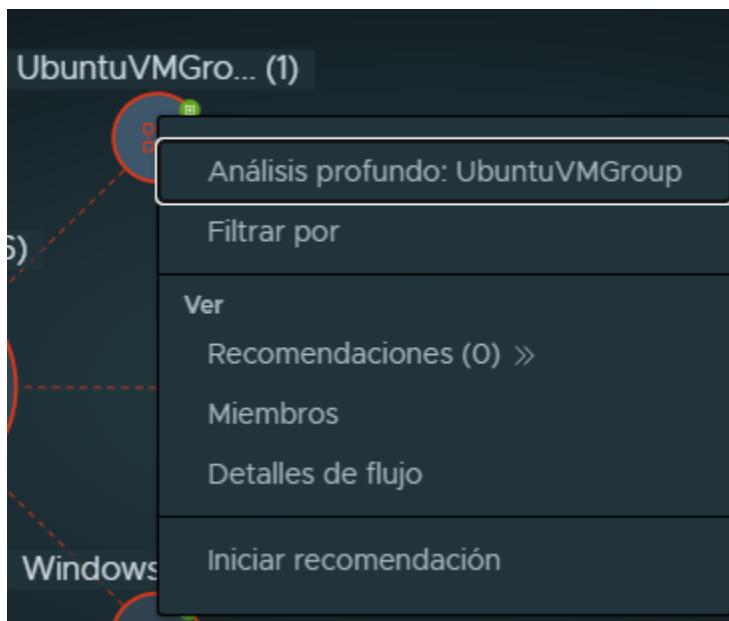


Para borrar la selección fija, haga clic en cualquier área vacía del lienzo de visualización.

Si se aleja la vista Grupos y los detalles de los nodos ya no están visibles, coloque el cursor en cualquier parte visible de un nodo para ver información detallada.

Acciones disponibles en la vista Grupos

Al hacer clic con el botón secundario en el nodo de un grupo, como se muestra en la siguiente imagen, se mostrará un menú contextual con la información o las acciones disponibles.



- Al seleccionar **Análisis profundo:Nombre_grupo** se rodea el nodo del grupo seleccionado con un círculo discontinuo para marcarlo como el nodo de grupo anclado o el grupo actualmente en el foco. Las entidades informáticas que pertenecen al grupo se muestran dentro del nodo del grupo. Todos los grupos que tuvieron flujos de tráfico con los miembros

del grupo anclado durante el período de tiempo seleccionado, también aparecerán en la vista Grupos. En el siguiente ejemplo, el grupo Windows7-group es el grupo anclado. Los otros grupos están en la vista porque sus miembros tenían flujos de tráfico de red con la única máquina virtual del grupo Windows7-group durante el período de tiempo seleccionado.



- Al seleccionar **Filtrar por**, el grupo actual se agrega al filtro de visualización utilizado para la vista Grupos actual.
- Al seleccionar **Recomendaciones**, se muestra la tabla de recomendaciones disponibles para el grupo actual. En la tabla **Recomendaciones**, puede ver los detalles de la recomendación y realizar las acciones disponibles. Consulte [Capítulo 3 Trabajar con recomendaciones de NSX Intelligence](#) para obtener más información.
- Al seleccionar **Miembros**, se muestra una tabla de todas las entidades informáticas que pertenecían al grupo anclado actual durante el período de tiempo seleccionado. En la tabla **Miembros** puede ver los detalles de las máquinas virtuales, direcciones IP y servidores físicos que pertenecen al grupo seleccionado, así como los grupos a los que pertenece cada entidad informática. Para agregar una máquina virtual, una dirección IP o un servidor físico específicos al filtro de visualización actual, haga clic en el ícono de filtro que se encuentra situado a la derecha.
- Al seleccionar **Detalles de flujo**, el cuadro de diálogo **Detalles de flujo de un grupo** mostrará una tabla para el grupo seleccionado actualmente. La tabla muestra los detalles de los flujos que se han completado y los flujos que estaban activos durante el período de tiempo seleccionado. Consulte [Trabajar con los flujos de tráfico](#) para obtener más información.
- Si selecciona **Iniciar recomendación**, se mostrará el asistente **Iniciar nueva recomendación**, que le ayudará a generar una nueva recomendación de regla de microsegmentación. Consulte [Generar una nueva recomendación de NSX Intelligence](#) para obtener detalles.

Trabajar con la vista Recursos informáticos

Un nodo de la vista Recursos informáticos representa una de las entidades informáticas en su entorno local de NSX-T Data Center. Una entidad informática es una máquina virtual, un servidor físico o una dirección IP.

Ver selección

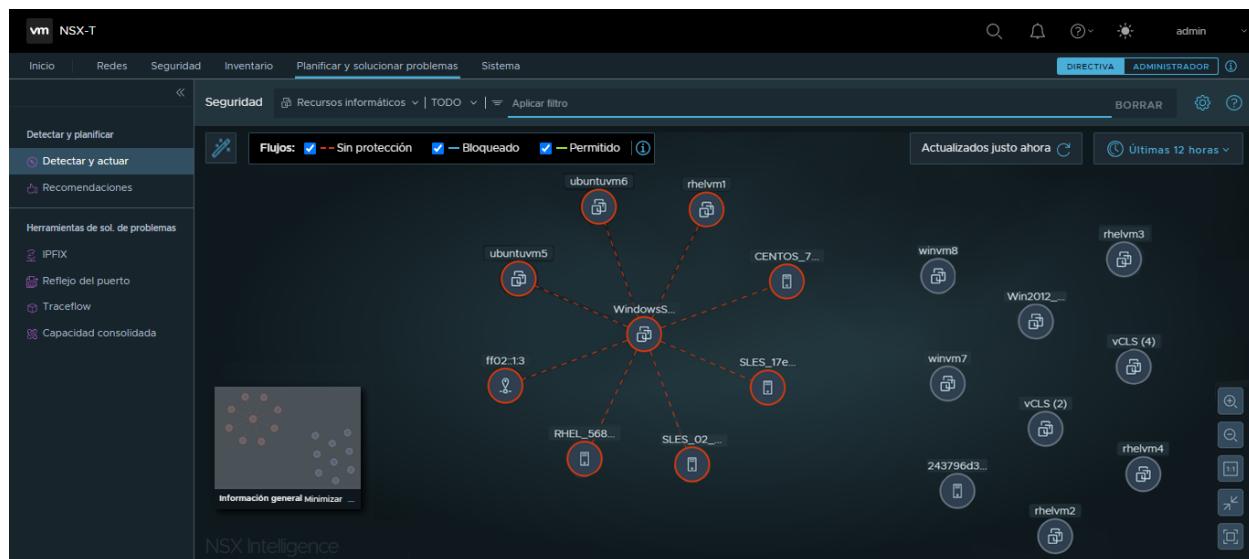
Si no ve la vista Recursos informáticos, haga clic en la flecha hacia abajo situada junto a **Grupos** en el área de selección de la vista Seguridad y seleccione **Recursos informáticos**. En el menú desplegable, puede seleccionar **Seleccionar todos los recursos informáticos** para mostrar todas las entidades informáticas durante el período de tiempo seleccionado. Para mostrar solo las máquinas virtuales, las direcciones IP o los servidores físicos, haga clic en **Mostrar todos los tipos** y seleccione **Máquinas virtuales**, **Direcciones IP** o **Servidores físicos** en el menú desplegable.

También puede seleccionar entidades informáticas específicas de la lista **Elementos disponibles**. Utilice el cuadro de texto **Buscar** para filtrar la lista de selección. Haga clic en **Aplicar** después de realizar sus selecciones.

Si sale del menú desplegable sin seleccionar nada o si selecciona **Seleccionar todos los recursos informáticos**, se aplicará la opción **Seleccionar todos los recursos informáticos** a la vista Recursos informáticos.

Nodos en la vista de equipos

En la vista Recursos informáticos, los límites de los grupos no están visibles. Cualquier nodo que se esté comunicando con una de las entidades informáticas del entorno de NSX-T Data Center, pero que no se haya identificado como parte del inventario de NSX-T Data Center, también se incluirá en la vista Recursos informáticos. A continuación, se muestra una vista Recursos informáticos sencilla.



En la siguiente tabla se incluyen los tipos de nodos de máquinas virtuales que se pueden ver en la vista Máquinas virtuales.

Tipo de nodo de entidad informática	Icono	Descripción
Máquina virtual normal		Un nodo de máquina virtual normal representa una máquina virtual que forma parte del entorno de NSX-T Data Center. Una máquina virtual puede pertenecer a más de un grupo.
IP pública		Un nodo de IP pública representa una dirección IP pública, ya sea IPv4 o IPv6, que se comunica con el entorno de NSX-T Data Center. Al hacer clic con el botón derecho en este ícono, se mostrarán todas las direcciones IP públicas que tuvieron actividad de tráfico de red durante el período de tiempo seleccionado. Al apuntar a una flecha de flujo de tráfico conectada a este nodo, se mostrará la dirección IP real que participó en ese intercambio de flujo de tráfico.
IP		Un nodo IP representa una dirección IP que participó en las actividades de tráfico de red durante el período de tiempo seleccionado. Una dirección IP puede ser una dirección IP de unidifusión, difusión o multidifusión.
Servidor físico		Este nodo representa un servidor físico que forma parte de su entorno de NSX-T Data Center. Un servidor virtual puede pertenecer a más de un grupo. Los servidores físicos compatibles actualmente son los siguientes. <ul style="list-style-type: none"> ■ RHEL Server versiones 7.9, 8.2, 8.4 ■ Ubuntu 16.04, 18.04 ■ CentOS 7.9, 8.4 ■ SUSE 12 SP4 ■ Windows Server 2016, 2019

Color del nodo

El color del borde de un nodo de entidad informática indica el tipo de flujos de tráfico que se han producido con la entidad informática durante el período de tiempo seleccionado.

- Un nodo con un borde rojo indica que se detectó al menos un flujo de tráfico no protegido, independientemente de cuántos flujos permitidos o bloqueados se detectaron durante el período de tiempo seleccionado.
- Un borde azul en un nodo significa que no se detectaron flujos de tráfico no protegidos, pero que sí se detectó al menos un flujo bloqueado, independientemente de cuántos flujos permitidos se detectaran durante el período de tiempo seleccionado.
- Un nodo con un borde verde indica que no se detectaron flujos sin protección ni bloqueados durante el período seleccionado, pero sí se detectó al menos un flujo permitido.
- Un nodo con un borde de color gris significa que, durante el período de tiempo seleccionado, no se detectó ningún flujo de tráfico para esa entidad informática.

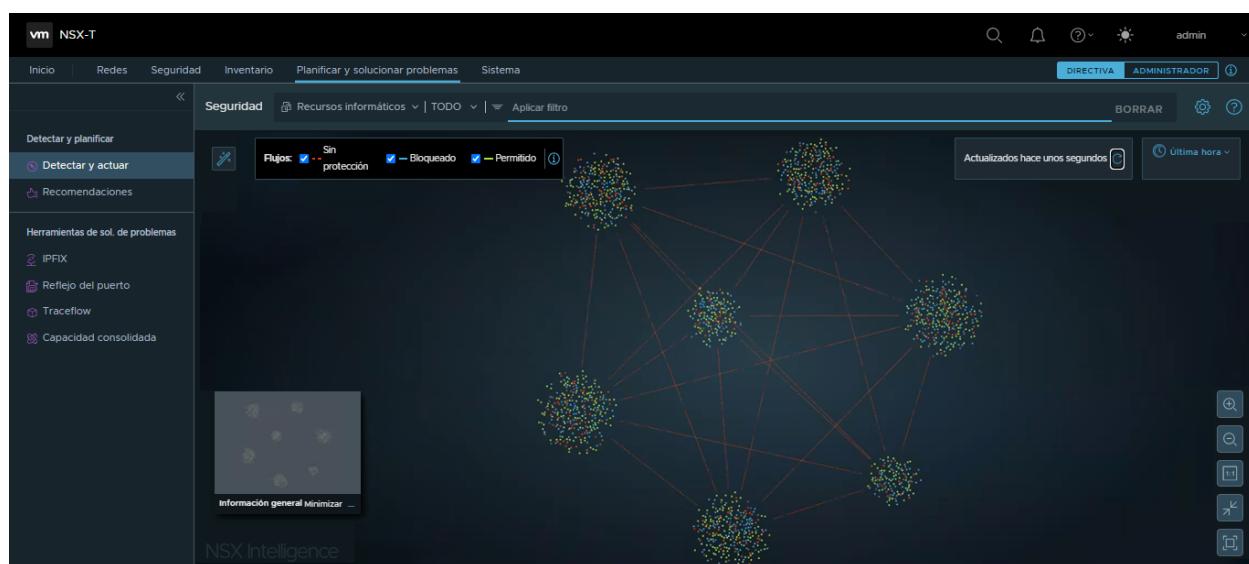
Flechas en la vista de equipos

Las flechas entre los nodos de entidad informática representan los flujos de tráfico producidos entre las entidades informáticas durante el período de tiempo seleccionado. Consulte [Trabajar con los flujos de tráfico](#) para obtener más información.

Clústeres de nodos de entidad informática

Si se deben mostrar 100 o más nodos de entidades informáticas y 1000 o más flujos de tráfico, el gráfico de NSX Intelligence mostrará los nodos de entidades informáticas en clústeres. Estos clústeres de entidades informáticas se basan en la conectividad entre las entidades informáticas durante el período de tiempo seleccionado. Agrupar las entidades informáticas en clústeres ofrece una vista de alto nivel de las actividades del tráfico de red de todo el entorno de NSX-T Data Center durante el período de tiempo seleccionado.

En la siguiente captura de pantalla se muestra un ejemplo de esta visualización de clúster de grupos. Los distintos colores de los nodos y las flechas corresponden a los tipos de flujos de tráfico producidos en las entidades informáticas durante el período de tiempo seleccionado. Las entidades informáticas que no tienen ninguna comunicación con otras entidades informáticas durante el período de tiempo seleccionado se mostrarán juntas en un clúster independiente.



Al colocar el cursor sobre un clúster específico, se mostrará un número sobre el área del clúster. Este número indica cuántas entidades informáticas hay en esa visualización de clústeres en concreto. Para ver más detalles sobre un clúster específico y las entidades informáticas que forman parte de ese clúster, amplíe el gráfico. A medida que amplíe los nodos y las flechas, los detalles sobre las entidades informáticas y los flujos de tráfico estarán más visibles y serán más fáciles de seleccionar. También puede aplicar filtros para limitar las entidades informáticas que se muestran en el gráfico de visualización.

Selección de nodos en la vista Recursos informáticos

Cuando se coloca el cursor sobre un nodo de entidades informáticas, se muestra información sobre el nodo, como puede verse en el siguiente ejemplo. Se muestra también el número y los tipos de flujos a las entidades informáticas detectadas durante el período de tiempo seleccionado. Si la entidad informática se agregó durante el período de tiempo seleccionado, se mostrará también el icono Nueva etiqueta y los detalles de cuándo se agregó la entidad informática.

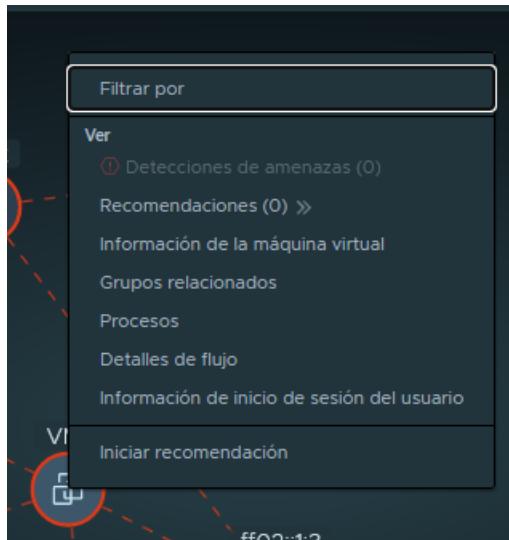


Al hacer clic en el nodo de entidad informática, se marcará la selección con un círculo discontinuo como un nodo de entidad informática anclado. Otros nodos de entidad informática que tengan flujos de tráfico con ese nodo de entidad informática anclado también se harán más prominentes en la vista Recursos informáticos. Los demás nodos se atenúan para que sean menos visibles. Para borrar la selección fija, haga clic en cualquier área vacía de la vista Recursos informáticos.

Si reduce el zoom de la vista Recursos informáticos y los detalles de los nodos de entidad informática ya no están visibles, coloque el cursor en cualquier parte visible del nodo de la entidad informática. Se muestran los detalles de la entidad informática.

Acciones disponibles en la vista Recursos informáticos

Al hacer clic con el botón secundario en el nodo de una entidad informática, como se muestra en la siguiente imagen, se muestra un menú contextual con las acciones disponibles.



Selección	Descripción
Filtrar por	La entidad informática se agregará al filtro de visualización utilizado para la vista Recursos informáticos actual.
Actividades de red sospechosas <n>	Si se detecta actividad de red sospechosa que involucra a esta entidad informática, se podrá seleccionar este elemento. (n) indica el número de actividades sospechosas detectadas. Consulte Capítulo 4 Detectar tráfico de red sospechoso en NSX-T Data Center para obtener más información.
Recomendaciones (<n>)	Se muestra la tabla de recomendaciones de la entidad informática actual. (n) indica el número de recomendaciones disponibles. En la tabla Recomendaciones, puede ver los detalles de la recomendación y realizar las acciones disponibles. Consulte Capítulo 3 Trabajar con recomendaciones de NSX Intelligence para obtener más información.
Información de <Tipo de entidad informática>	<p>Se muestran los detalles de la entidad informática seleccionada actualmente durante el período de tiempo seleccionado. Los detalles dependen del tipo y pueden incluir el nombre, la dirección IP, el identificador, la información del sistema operativo y muchos más.</p> <p>Nota Si una máquina virtual está asociada al perfil de segmentos como el perfil predeterminado de detección de direcciones IP y tiene TOFU (Trust On First Use) habilitado, la máquina virtual obtendrá inicialmente una dirección IP de DHCP. Si se libera la dirección IP de DHCP y se cambia la dirección IP de la máquina virtual a una dirección IP estática, se mostrarán las direcciones DHCP e IP estática en Información de la máquina virtual. Si se deshabilitó TOFU en el perfil predeterminado de detección de direcciones IP, cuando se libera la dirección IP de DHCP asignada inicialmente y se cambia la dirección IP de la máquina virtual a una dirección estática, solo se mostrará la dirección IP estática en Información de la máquina virtual.</p>
Grupos relacionados	Muestra la tabla Grupos con información sobre los grupos a los que pertenecía la entidad informática durante el período de tiempo seleccionado.
Procesos	(Solo para nodos de máquina virtual) Muestra la tabla Procesos que incluye los detalles de los procesos que implican flujos de tráfico en los que se enviaron o recibieron los datos a o desde la máquina virtual.
Detalles de flujo	<p>En esta tabla se muestran los detalles de los flujos completados y los flujos que están activos actualmente en la entidad informática durante el período de tiempo seleccionado.</p> <p>Nota Los flujos activos durante el período de tiempo seleccionado tienen más de 2,5 minutos de antigüedad en el momento en que se muestran los detalles.</p> <p>Entre los detalles, se incluyen los siguientes.</p> <ul style="list-style-type: none"> ■ tipo de flujo: completado o activo ■ grupos de origen y destino del flujo ■ servicios que se utilizaron ■ Información de capa 7: ID de aplicación y FQDN ■ tipo del flujo más reciente: desprotegido, bloqueado, permitido ■ hora de finalización del flujo <p>Puede hacer clic en algunos de los detalles para obtener más información. Consulte Trabajar con los flujos de tráfico para obtener más información.</p>
Información de inicio de sesión del usuario	(Solo para nodos de máquina virtual) Muestra la información de inicio de sesión del usuario para la máquina virtual seleccionada.
Iniciar recomendación	Muestra el asistente Iniciar nuevas recomendaciones . Consulte Capítulo 3 Trabajar con recomendaciones de NSX Intelligence para obtener detalles.

Trabajar con los flujos de tráfico

Las flechas entre los nodos de grupo o de entidad informática representan los flujos de tráfico de red producidos entre las entidades informáticas durante el período de tiempo seleccionado.

Los flujos de tráfico de red se basan en las reglas de firewall distribuido (DFW) de capa 3 y en los flujos de tráfico que se produjeron durante el período de tiempo seleccionado. Todos los flujos de tráfico de red que coincidieron con una regla de DFW de capa 3 con estado que utilizaban IPv4 o IPv6 con protocolos TCP, UDP, GRE, ESP y SCTP se incluyen en los detalles de visualización y flujo. Los flujos TCP y UDP tienen detalles de nivel de IP y puerto y otros solo tienen detalles de nivel de IP.

Los flujos de tráfico se clasifican en los siguientes tipos.

Tipo de flujo	Gráfico	Descripción
Sin protección		Una flecha roja indica que el sistema detectó que el flujo de tráfico encontró una regla (Origen: Cualquiera Destino: Cualquiera Acción: Permitir, Rechazar o Anular) y que se requieren directivas de seguridad más detalladas. Esta regla puede ser la predeterminada o puede residir en cualquier parte del firewall distribuido de este a oeste.
Bloqueado		Una flecha azul indica que el sistema detectó que el flujo de tráfico cumplió una regla "Rechazar" o "Anular" más detallada que la que se menciona en la definición de flujo "Sin protección".
Permitido		Una flecha verde indica que el sistema detectó que el flujo de tráfico cumplió una regla "Permitir" más detallada que la que se menciona en la definición de flujos "Sin protección".

Para ver los detalles de los flujos de tráfico en los que participa un grupo o una entidad informática en particular, haga clic con el botón secundario en el nodo de visualización y seleccione **Detalles de flujo**. El cuadro de diálogo **Detalles de flujo** muestra una tabla, como se muestra en la siguiente imagen de un nodo de grupo.

The screenshot shows a table titled '5 Flujos' (5 Flows) under the 'Flujos completados' (Completed Flows) tab. The table has columns for Origen (Source) and Destino (Destination). The Source columns include Cómputo (Compute), Grupo (Group), Usuario (User), and Proceso (Process). The Destination columns include Cómputo (Compute), Grupo (Group), Servicios (Services), Identificador de aplicación (Application Identifier), FQDN (Fully Qualified Domain Name), Último flujo (Contra la última directiva) (Last flow (against the last directive)), and Hora de finalización (End Time). The table lists five completed flows from VM1 to various destinations, all marked as 'Sin protección' (No protection) and ending on 28/11/2023 at 23:52.

Origen				Destino		Servicios	Identificador de aplicación	FQDN	Último flujo (Contra la última directiva)	Hora de finalización
Cómputo	Grupo	Usuario	Proceso	Cómputo	Grupo					
> VM1	UbuntuV...	N/A	N/A	[redacted]	Desconocido	Win - R... 1 más			● Sin protección	28/11/2023 23:52
> VM1	UbuntuV...	N/A	N/A	ff02:12	Desconocido	DHCPv6 Servei			● Sin protección	28/11/2023 23:51
> VM1	UbuntuV...	N/A	N/A	[redacted]	Desconocido	NetBio... 4 más			● Sin protección	28/11/2023 23:22
> VM1	UbuntuV...	N/A	N/A	[redacted]	Desconocido	Win - R... 1 más			● Sin protección	28/11/2023 23:22
> VM1	UbuntuV...	N/A	N/A	ff02:13	Desconocido	Win - R... 1 más			● Sin protección	28/11/2023 23:22

1-5 de 5 Flujos

CERRAR

La tabla incluye las pestañas **Flujos completados** y **Flujos activos** que muestran detalles sobre los respectivos flujos que se han completado o que han estado activos durante el período de tiempo seleccionado. Los detalles incluyen la información de origen y destino del flujo, los grupos a los que pertenecen (si se sabe), los servicios que se utilizaron y el tipo de flujo más reciente.

Al expandir una fila, se mostrará información adicional, como cualquier identificador de aplicación de capa 7 (L7) e información de FQDN, cuándo finalizó el flujo, el recuento total de paquetes recibidos/transmitidos desde el origen y el destino, así como las direcciones IP de origen y destino. Puede hacer clic en los vínculos de detalles proporcionados en la tabla para obtener más información. Por ejemplo, si las IP públicas participaban en un flujo, puede hacer clic en el vínculo **IP públicas** para ver las direcciones IP reales de esas IP públicas.

Para centrarse solo en entidades informáticas con ciertos tipos de flujos de tráfico, utilice el área de selección de la vista **Seguridad** para seleccionar el tipo de vista, y use el atributo de filtro **Flujo > Tipo** para delimitar la selección.

Si anula la selección de un tipo de flujo en la sección **Flujos**, las líneas de flujo de ese tipo se ocultarán del gráfico de visualización. A menos que se apliquen filtros que excluyan determinados objetos, todas las entidades informáticas o grupos permanecerán visibles, independientemente de los tipos de flujo de tráfico que se hayan producido con esas entidades durante el período de tiempo seleccionado. Por ejemplo, si anula la selección del tipo de flujo "Permitido", todas las líneas de flujo permitidas se ocultarán en el gráfico. Sin embargo, se seguirán mostrando todos los objetos de NSX, incluso aquellos que solo tengan flujos de tráfico permitidos durante el período de tiempo seleccionado.

La dirección de las flechas de flujo indica el origen y el destino de cada flujo de tráfico detectado. En la vista Grupos, una flecha de autorreferencia en un nodo de grupo indica que al menos una entidad informática se está comunicando con otra entidad informática dentro del mismo grupo. En la vista Recursos informáticos, una flecha de autorreferencia indica que un objeto de NSX de la entidad informática se comunicó con otro objeto de NSX en la misma entidad informática.

Cuando se coloca el cursor sobre una flecha de flujo, se muestra información sobre los flujos relacionados con el grupo o la entidad informática, como se muestra en el siguiente ejemplo del nodo Windows7-group.



Al hacer clic en una flecha de flujo, se muestra el cuadro de diálogo Detalles de flujo. Muestra los detalles de los flujos activos y completados que se produjeron durante el período de tiempo seleccionado. Para obtener información más detallada sobre el origen, el destino, el tipo de servicio y el tipo de cada flujo, haga clic en los vínculos de la tabla.

Cuando amplié la imagen a una vista Recursos informáticos, la información sobre los protocolos y los puertos L4 aparecerá en las líneas de flujo. Si hay más de un detalle de L4, también aparecerá un vínculo con el número de detalles adicionales en la línea de flujo. Haga clic en este número, como se muestra en la siguiente imagen, para ver la lista de protocolos y puertos L4.



Trabajar con recomendaciones de NSX Intelligence

3

La función NSX Intelligence puede proporcionar recomendaciones de microsegmentación basadas en los patrones de flujos de tráfico de red que se han producido entre las máquinas virtuales, los servidores físicos o las direcciones IP de su entorno de NSX-T Data Center durante el periodo de tiempo seleccionado.

Este capítulo incluye los siguientes temas:

- Información sobre las recomendaciones de NSX Intelligence
- Generar una nueva recomendación de NSX Intelligence
- Volver a ejecutar las recomendaciones de NSX Intelligence
- Revisar y publicar recomendaciones generadas de NSX Intelligence
- Exportar NSX Intelligence como archivo JSON

Información sobre las recomendaciones de NSX Intelligence

Las recomendaciones de microsegmentación proporcionadas por la función NSX Intelligence incluyen directivas de seguridad, grupos de seguridad de directivas y servicios para las aplicaciones.

Descripción general de funciones

Las recomendaciones de NSX Intelligence se basan en los patrones de flujo de tráfico de red que se produjeron entre los miembros informáticos de un grupo de directivas seleccionado, de máquinas virtuales o de servidores físicos. Las recomendaciones pueden ayudarle a aplicar una directiva de seguridad más dinámica al correlacionar los patrones de tráfico de comunicación que se produjeron dentro de su entorno de NSX-T Data Center.

- Las recomendaciones de la directiva de seguridad son de la categoría Directivas de seguridad de firewall distribuido (DFW) de este-oeste de aplicación.
- Las recomendaciones de los grupos de seguridad consisten en las máquinas virtuales o los servidores físicos cuyos flujos de tráfico de red que se analizaron según el periodo de tiempo y el límite de la máquina virtual que especificó.

- Las recomendaciones de servicio son objetos de servicio utilizados por aplicaciones de las máquinas virtuales o los servidores físicos que especificó, pero estos servicios aún no están definidos en el inventario de NSX-T Data Center.

Descripción general del flujo de trabajo de recomendación

Existen varias formas de solicitar la recomendaciones de NSX Intelligence, pero la más sencilla es usar la pestaña **Planificar y solucionar problemas > Recomendaciones** y hacer clic en **Iniciar nueva recomendación**.

Proporcione lo siguiente como entrada al solicitar que se genere una recomendación de NSX Intelligence.

- Cualquier entidad informática (grupos, máquinas virtuales o servidores físicos) o la sección de firewall distribuido (DFW) existente en el entorno de NSX-T.
- Intervalo de tiempo en el que se analizarán los flujos de tráfico de red para las entidades informáticas proporcionadas o las reglas de directiva de seguridad existentes.

Para las reglas existentes, el sistema puede recomendar actualizaciones que se puedan realizar en las reglas de esa sección a fin de conectar las fugas detectadas para los flujos de entrada, salida o dentro de las aplicaciones entre las cargas de trabajo. Consulte [Generar una nueva recomendación de NSX Intelligence](#) para obtener más información.

Una vez que haya finalizado el análisis de la recomendación, podrá consultarla de forma detallada y, si es necesario, modificarla antes de publicarla. Consulte [Revisar y publicar recomendaciones generadas de NSX Intelligence](#) para obtener detalles.

También puede exportar una recomendación de NSX Intelligence generada a un archivo con formato JSON. Si es necesario, modifique ese archivo JSON usando una herramienta REST API externa antes de enviarlo a NSX Policy Manager para su procesamiento. Consulte [Exportar NSX Intelligence como archivo JSON](#) para obtener más información.

Cómo se generan las recomendaciones de NSX Intelligence

Según el ámbito de tráfico que seleccionó en el momento de comenzar a generar una recomendación, el trabajo del servicio Recomendación selecciona flujos de tráfico de entrada, de salida o dentro de la aplicación desde y entre las entidades del límite de recomendación seleccionado.

A continuación, el servicio (puerto o protocolo) en el que se comunican estos flujos agrega los flujos. A continuación, se agrupan juntos los orígenes y destinos de cada uno de los flujos de un servicio concreto. Durante la agrupación, se intenta reutilizar los grupos existentes que ya existen en el inventario en función del umbral especificado por el usuario para la proporción de coincidencia.

Si no se encuentra ningún grupo que pueda satisfacer el umbral de agrupación establecido, se creará un nuevo grupo.

Según el valor que establezca para la opción **Crear reglas para**, solo se considerarán los flujos de tráfico en una dirección específica al generar una regla de recomendación. Si el ámbito del flujo de tráfico era todo el tráfico, entrante y saliente, o entrante y dentro de la aplicación, los flujos de tráfico en estas direcciones se agregarán juntos para formar la regla, en función del servicio.

Tomemos estos flujos como ejemplo.

- El límite se establece mediante VM1 y VM2
- Grupos: CG con VM1 y VM2 como miembros
- Grupos: G3 con VM3 y VM4 como miembros
- Umbral de coincidencia supuesto: 50 %

Los flujos de tráfico no deseados son los siguientes.

- De VM3 a VM1 mediante SSH
- De VM1 a VM2 mediante SSH

A continuación se muestra la recomendación de microsegmentación resultante, que es una regla única para SSH.

Nuevo grupo de origen	Grupo de destino	Servicio	Grupo aplicado a
Grupo con VM1 y VM3 como miembros	CG con VM1 y VM2 como miembros	SSH	Grupo: CG con VM1 y VM2 como miembros

Si los flujos de tráfico se originan fuera de la máscara configurada de direcciones IP privadas, los flujos desde y hacia dichas direcciones IP que no se incluyan en la lista de prefijos de IP privada se marcarán como "CUALQUIER".

Tenga en cuenta los siguientes flujos no deseados.

- CUALQUIER flujo a VM1 mediante SSH
- Flujos de VM1 a VM3 mediante SSH
- El límite se establece mediante VM1 y VM2
- El grupo definido es CG con VM1 y VM2 como miembros

En este caso, cuando se agregan los flujos de entrada y salida, se convierten en CUALQUIER flujo de VM1 a VM1 y VM3 mediante SSH.

A su vez, esto da como resultado la siguiente regla de microsegmentación.

Origen	Destino	Servicio	Se aplica a
ANY	[VM1] en CG, [VM3] en G3	SSH	CG [VM1, VM2]

Nota Todas las reglas solo se aplican a los miembros del límite de recomendación que especificó antes de generar la recomendación. La agregación de motivos se utiliza para reducir el número de reglas que resultan en función del servicio.

Generar una nueva recomendación de NSX Intelligence

La función Recomendaciones de NSX Intelligence proporciona recomendaciones para ayudarle a microsegmentar sus aplicaciones.

Generar una recomendación de NSX Intelligence implica recomendaciones de las directivas de seguridad, los grupos de seguridad de directivas y los servicios de la aplicación. Las recomendaciones se basan en el patrón de tráfico de comunicación entre las máquinas virtuales y los servidores físicos de NSX-T Data Center.

Puede generar una recomendación si selecciona las entidades de entrada de grupos o hasta 100 máquinas virtuales y servidores físicos; una combinación de grupos, máquinas virtuales y servidores físicos; o directivas de seguridad existentes. La cantidad total de máquinas virtuales y servidores físicos que puede seleccionar como entrada no puede ser superior a 100 de esas entidades. El número total de máquinas virtuales y servidores físicos efectivos que se pueden utilizar en una entrada que incluye grupos, máquinas virtuales o servidores físicos no puede ser superior a 250 entidades de entrada.

Por ejemplo, si selecciona 50 máquinas virtuales y 50 servidores físicos como parte de las entidades de entrada de recomendación, solo podrá seleccionar grupos que no tengan más de 150 miembros informáticos.

Importante Solo puede generar una nueva recomendación para grupos de seguridad que se crearon en el modo Directiva. Los grupos de seguridad deben tener al menos uno de los tipos de miembros compatibles para que la función NSX Intelligence inicie un análisis de recomendaciones para esos grupos de seguridad. Entre los tipos de miembros compatibles, se incluyen las máquinas virtuales, los servidores físicos, las interfaces de red virtual (VIF), los puertos lógicos y los conmutadores lógicos. Si hay al menos un tipo de miembro admitido en el grupo de seguridad, el análisis de recomendaciones podrá continuar, pero durante el análisis no se tendrán en cuenta los tipos de miembro no admitidos.

Existen varias formas de generar una recomendación con la interfaz de usuario de NSX Intelligence. A continuación se describen los métodos disponibles que se pueden utilizar.

Requisitos previos

- Active la función NSX Intelligence 3.2 o una versión posterior en NSX Application Platform. Consulte la documentación de *Activar y actualizar VMware NSX Intelligence 3.2*.
- Asegúrese de tener los privilegios necesarios para generar recomendaciones. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.

Procedimiento

- 1 En un navegador, inicie sesión con los privilegios necesarios en una instancia de NSX Manager desde `https://<dirección-ip-nsx-manager>`.

- 2** Inicie la generación de una nueva recomendación utilizando uno de los siguientes métodos.

Dónde empezar	Próximo paso
Seleccione Planificar y solucionar problemas > Recomendaciones.	Haga clic en Iniciar nueva recomendación .
Para obtener recomendaciones de un grupo, seleccione Planificar y solucionar problemas > Detectar y realizar acción.	<ol style="list-style-type: none"> 1 Compruebe que la vista Grupos esté seleccionada en el área de selección de vista Seguridad. 2 Haga clic con el botón derecho en el nodo del grupo en el que desea generar una recomendación. 3 En el menú desplegable, seleccione Iniciar recomendación.
Para obtener recomendaciones para máquinas virtuales o servidores físicos, seleccione Planificar y solucionar problemas > Detectar y realizar acción.	<p>Seleccione al menos una máquina virtual o un servidor físico, o bien una combinación de ambos.</p> <ol style="list-style-type: none"> 1 En el área de selección de vista Seguridad, haga clic en la flecha hacia abajo situada junto a Grupos y seleccione Recursos informáticos. 2 Haga clic en Mostrar todos los tipos y seleccione Máquinas virtuales o Servidores físicos. Como alternativa, en la lista de elementos disponibles, seleccione máquinas virtuales o servidores físicos específicos. 3 Haga clic en Aplicar. 4 Haga clic en el icono de la varita de recomendación  situado en el lado izquierdo de la barra Flujos. 5 Seleccione Iniciar recomendaciones para los equipos filtrados.

- 3** En el asistente **Iniciar nueva recomendación**, cambie el valor predeterminado del cuadro de texto **Nombre de recomendación**

Asigne un nombre que indique la aplicación para la que se realiza la segmentación. El nombre se utilizará como prefijo para los nombres de todos los grupos y reglas recomendados que se crearon durante el análisis de recomendaciones.

- 4** Cambie el valor predeterminado del cuadro de texto **Descripción** para que sea más fácil recuperar la información sobre la recomendación.

- 5 Defina o modifique las máquinas virtuales o los servidores físicos que se utilizarán como límite para la recomendación de la directiva de seguridad.
 - a En **Entidades seleccionadas en el alcance**, haga clic en **Seleccionar entidades**. Si ya seleccionó los grupos, las máquinas virtuales o los servidores físicos, haga clic en el vínculo al número de entidades seleccionadas para modificar la selección actual.
 - b En el cuadro de diálogo **Seleccionar entidades**, haga clic en **Grupos** para seleccionar uno o varios grupos. Para seleccionar las máquinas virtuales o los servidores físicos que desea utilizar como límite para el análisis, haga clic en las pestañas **Máquinas virtuales** o **Servidores físicos** y realice la selección.

Puede seleccionar grupos y hasta 100 máquinas virtuales o servidores físicos, pero no más de 250 entidades informáticas efectivas para usar como límite de recomendaciones. Anule la selección de lo que no quiera incluir. También puede hacer clic en **Filtro** y seleccionar los atributos que desea utilizar para filtrar los grupos, las máquinas virtuales o los servidores físicos que desea seleccionar.

- c Haga clic en **Guardar**.
 - d (opcional) Si el sistema detectó que existe una sección de firewall distribuido (DFW) asociada a los grupos seleccionados en el paso anterior, en el cuadro de diálogo **Seleccionar la sección de FW distribuido**, seleccione si desea utilizar la sección de firewall distribuido (DFW) existente o cree una nueva. Haga clic en **Guardar**.

En el asistente **Iniciar nueva recomendación**, el vínculo de número en el cuadro de texto **Entidades seleccionadas en el alcance** indica el número de entidades seleccionadas.

Si seleccionó utilizar una sección de DFW distribuido existente durante el análisis de recomendaciones, el sistema indica que en el cuadro de texto **Entidades seleccionadas en el alcance**.

- 6 En el cuadro de texto **Intervalo de tiempo**, opcionalmente, cambie el valor predeterminado que se utilizará para generar la recomendación.

El valor del intervalo de tiempo predeterminado es **Último mes**. Los flujos de tráfico de red que se produjeron entre las máquinas virtuales o los servidores físicos, o bien los grupos de máquinas virtuales o servidores físicos se utilizarán para el análisis de recomendaciones. Otros valores que se pueden seleccionar son **Última hora**, **Últimas 12 horas**, **Últimas 24 horas**, **Última semana**, **Últimas 2 semanas** o **Último mes**.

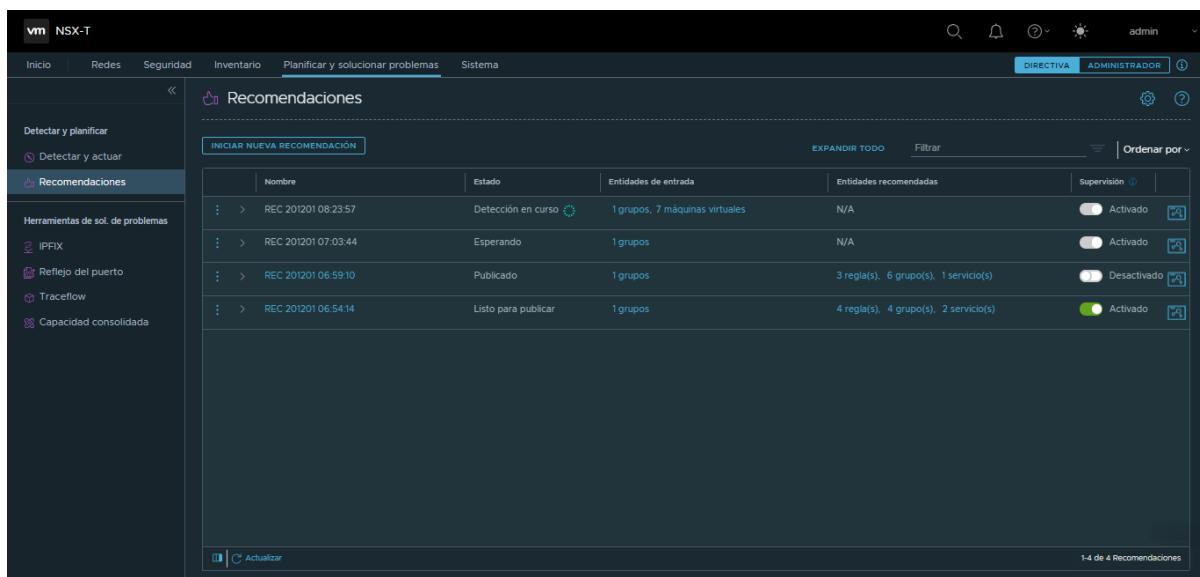
- 7 Expanda la sección **Opciones avanzadas** y modifique los valores predeterminados asignados, si es necesario.

Si no utiliza una sección de DFW existente, puede modificar los valores asignados predeterminados. Si decidió utilizar una sección de DFW existente, los valores que se muestran en esta sección se obtendrán de esa sección de DFW.

- a En el menú desplegable **Crear reglas para**, seleccione el tipo de flujos de tráfico que desea tener en cuenta en el análisis de recomendaciones. El valor predeterminado es **All Traffic**.
 - **Tráfico entrante y saliente**: se tienen en cuenta todos los tipos de flujo de tráfico que se originan dentro del límite de la aplicación hacia fuera del límite y desde fuera del límite de la aplicación hacia dentro del límite.
 - **Tráfico entrante**: solo se tienen en cuenta los flujos de tráfico que se originan fuera del límite de la aplicación.
 - **Todo el tráfico**: se tienen en cuenta todos los tipos de flujo de tráfico saliente, entrante y dentro de la aplicación.
 - **Tráfico entrante y dentro de la aplicación**: se consideran todos los tipos de flujo de tráfico que se originan dentro y fuera del límite de la aplicación.
- b En el menú desplegable **Regla predeterminada**, seleccione la estrategia de conectividad que se utilizará para crear la regla predeterminada para la directiva de seguridad. Se establece una acción adecuada en la regla en función del valor de la estrategia de conectividad. El valor predeterminado es **Ninguna**.
 - **Lista de no permitidos**: crea una regla de permiso predeterminada.
 - **Lista de permitidos**: crea una regla de descarte predeterminada.
 - **Ninguno**: no se crea ninguna regla predeterminada.
- c Cambie el valor predeterminado de **Salida de recomendación**, si es necesario.

Basado en cómputo es el modo de salida predeterminado utilizado. Este modo significa que la recomendación de directiva de DFW que generó el motor de recomendaciones contiene grupos cuyos miembros son máquinas virtuales, servidores físicos o ambos. Si se selecciona el modo de salida recomendación **Basado en IP**, la recomendación de directiva de DFW generada contendrá grupos cuyos miembros son objetos IPSet con una lista estática de direcciones IP. Una recomendación basada en IP no está vinculada estrechamente a una máquina virtual. Si se elimina una máquina virtual y se asigna su dirección IP a una máquina virtual nueva, la nueva máquina virtual se asignará al mismo grupo. Las directivas de DFW para el grupo también se aplicarán a la nueva máquina virtual.

- d Si es necesario, cambie el valor de **Tipo de servicio de recomendación**.
El tipo predeterminado es **Servicios L4**, que está compuesto por los respectivos protocolo y puerto de capa 4. Si lo prefiere, puede seleccionar **Perfiles de contexto de Capa 7** para los perfiles de contexto de Capa 7.
 - e Cambie el valor predeterminado de **Umbral de reutilización de grupos** como considere adecuado al generar la recomendación de regla.
Puede establecer el valor del porcentaje de umbral de 10 a 100. El valor especifica cómo de estricto es el sistema al reutilizar grupos para cubrir los flujos detectados que no están en microsegmentos. Utilice este valor para controlar si se deben reutilizar los grupos existentes o se deben crear nuevos grupos. La función de reutilización de grupos se aplica a cualquier trabajo de recomendación con una directiva de seguridad existente o una nueva directiva de seguridad.
Si se establece este valor en 100, solo los grupos con exactamente los mismos miembros que las entidades informáticas que el sistema busca agrupar se pueden seleccionar como orígenes o destinos de reglas adicionales. El uso de un valor muy alto puede provocar la creación de más grupos nuevos, ya que es menos probable que los grupos existentes se reutilicen en las reglas que se modifican.
Si se establece este valor en valores inferiores, como 10 o 20, significa que se pueden elegir como orígenes o destinos de regla adicionales incluso los grupos con miembros extraños, excepto las entidades informáticas que el sistema quiere agrupar. El uso de un valor inferior puede provocar una reutilización agresiva de grupos y, por lo tanto, se recomienda crear menos grupos nuevos.
 - f Si es necesario, cambie los valores predeterminados seleccionados en el cuadro de texto **Excluir flujos** para especificar los tipos de flujo de tráfico que desea excluir durante el análisis de recomendaciones.
Esta función está disponible a partir de NSX Intelligence 3.2.1. Los valores predeterminados son **Flujos de difusión** y **Flujos de multidifusión**. Estos tipos de flujo no son relevantes para las reglas de categoría de aplicaciones. La exclusión de los flujos de difusión, los flujos de multidifusión o ambos tipos de flujo puede ayudar a optimizar el análisis de recomendación de reglas de DFW.
- 8** Para iniciar el análisis de recomendaciones, haga clic en **Iniciar detección**.
- Las recomendaciones se procesan en serie. De media, puede tardar entre 3 y 4 minutos en finalizar cada recomendación, en función de si existen otras recomendaciones en espera de su procesamiento. Si hay un gran número de flujos de tráfico entre las máquinas virtuales o los servidores físicos que se deben analizar, una recomendación puede tardar entre 10 y 15 minutos en generarse.
- La tabla **Recomendaciones** muestra las recomendaciones que inició, como se muestra en la siguiente imagen.



- Puede realizar un seguimiento de los estados del análisis de recomendaciones en la columna **Estado** de la tabla **Recomendaciones**. El estado pasa de Esperando a Detección en curso, a Listo para publicar y a Publicado. Si el sistema no genera una recomendación, el valor de **Estado** se establecerá en No hay recomendaciones disponibles. Si se produjo un error en el análisis de recomendaciones por algún motivo, se mostrará el estado Error.
- La columna **Entidades de entrada** muestra las entidades que se utilizaron para generar la recomendación. Al hacer clic en el texto vinculado de esta columna, se muestra el cuadro de diálogo **Entidades seleccionadas** en modo de solo lectura.
- La columna **Supervisión** indica si se están supervisando los cambios de las entidades de entrada originales que se utilizan para generar la recomendación. Esta función está disponible para las recomendaciones con el estado Listo para publicar, No hay recomendaciones disponibles o Error. Puede activar o desactivar el botón **Supervisión**. Cuando el botón de alternancia está activado, se comprobarán los cambios en el ámbito de las entidades de entrada o la estrategia de conectividad cada hora.
- Si se produjo algún cambio con alguna de las entidades de entrada utilizadas, el icono de cambio detectado 🟢 se mostrará junto al estado Listo para publicar, No hay recomendaciones disponibles o Error. Puede revisar los cambios y volver a ejecutar la recomendación. Consulte [Volver a ejecutar las recomendaciones de NSX Intelligence](#) para obtener más información.
- Al hacer clic en el icono de lienzo 🖥 situado en el extremo derecho de la fila de la recomendación, se mostrará la visualización de las entidades seleccionadas en el lienzo gráfico debajo de la interfaz de usuario **Planificar y solucionar problemas > Detectar y realizar acción**. Si el estado de la recomendación que se muestra es Publicado, al hacer clic en el icono de lienzo, los grupos recomendados se mostrarán en el lienzo gráfico **Detectar y realizar acción**.

- 9 Cuando el valor de **Estado** es **Listo para publicar**, revise la recomendación generada y decida si desea publicarla. Consulte [Revisar y publicar recomendaciones generadas de NSX Intelligence](#).

Volver a ejecutar las recomendaciones de NSX Intelligence

Si el icono de cambio detectado aparece junto a un estado **Listo para publicar**, **No hay recomendaciones disponibles** o **Error**, revise los cambios en el ámbito original de las entidades de entrada de recomendaciones de NSX Intelligence. Vuelva a ejecutar el análisis de recomendaciones si fuera necesario.

El icono de cambio detectado  indica que se han producido algún cambio con las entidades de entrada que se utilizaron para generar la recomendación de NSX Intelligence anterior. Si se produce al menos una de las siguientes situaciones, el icono de cambio detectado aparecerá en la tabla Recomendaciones, junto a la recomendación afectada.

- Se agregaron o eliminaron nuevos miembros efectivos de las entidades seleccionadas originales que se utilizaron para generar la recomendación de NSX Intelligence.
- Si "se aplica al ámbito" de la directiva de seguridad cambió del valor que se utilizó al inicio del proceso de recomendación de NSX Intelligence.

Requisitos previos

- Debería haber generado una recomendación de NSX Intelligence anteriormente. Consulte [Generar una nueva recomendación de NSX Intelligence](#).
- Asegúrese de tener los privilegios necesarios para volver a ejecutar las recomendaciones de NSX Intelligence. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.

Procedimiento

- 1 En un navegador, inicie sesión con los privilegios necesarios en una instancia de NSX Manager desde `https://<dirección-ip-nsx-manager>`.
- 2 Seleccione **Planificar y solucionar problemas > Recomendaciones**.
- 3 Para revisar y volver a ejecutar la recomendación de NSX Intelligence, seleccione uno de los siguientes métodos.
 - Haga clic en el icono de cambio detectado  situado a la derecha del estado y seleccione **Volver a ejecutar recomendación**.
 - Haga clic en el menú de tres puntos  situado a el extremo izquierdo de la fila de la recomendación y seleccione **Revisar y volver a ejecutar**.
- 4 Revise los cambios en el cuadro de diálogo **Revisar y volver a ejecutar**.
Aparecerá un cuadro de diálogo similar al siguiente.

Origen	Destino	Servicios	Identificador de aplicación	FQDN	Último flujo (Contra la última directiva)	Hora de finalización
Computo	Computo					
VM2	N/A	N/A	ff02:12	DHCPv6 Server	● Sin protección	1/12/20 1:15
VM1	N/A	N/A	██████████	Win - R... 1 más	● Sin protección	1/12/20 1:14

Todos los flujos **Todos los miembros (7)** **Miembros agregados (0)** **Miembros eliminados (0)**

DESCARTAR **SE RECOMIENDA VOLVER A EJECUTAR**

El gráfico de visualización situado en la mitad superior del cuadro de diálogo muestra las entidades informáticas que se agregaron o eliminaron desde que se generó la recomendación anterior. Un nodo de entidad informática con el borde gris indica que se quitó del ámbito del límite de recomendaciones. Un nodo con el borde verde indica que se agregó la nueva entidad de proceso en el ámbito del límite de recomendaciones.

- a Haga clic en las pestañas **Todos los flujos** y **Todos los miembros** para revisar los flujos y las entidades informáticas que se tuvieron en cuenta para generar la recomendación.
- b Para revisar los cambios en las entidades informáticas que se utilizaron como entidades de entrada, haga clic en la pestaña **Miembros agregados** o **Miembros eliminados**.
- 5 (opcional) Si desea cambiar las entidades informáticas originales que se utilizan como límite para el análisis de recomendación anterior, haga clic en la pestaña **Ajustes de nueva ejecución** y modifique la configuración según sea necesario.
- 6 Para salir del cuadro de diálogo sin generar otro análisis de recomendación, haga clic en **Descartar**.
- 7 Para generar otro análisis de recomendaciones, haga clic en **Se recomienda volver a ejecutar**.

Resultados

Después de seleccionar **Se recomienda volver a ejecutar**, la recomendación generada anteriormente se eliminará y no se podrá restaurar. La función NSX Intelligence regenerará la recomendación utilizando las entidades de entrada modificadas como el límite de la recomendación. Los flujos y las entidades informáticas detectadas para el período de tiempo seleccionado también se incluirán en el análisis de recomendaciones. Los flujos de tráfico de las entidades informáticas que se eliminaron de las entidades de entrada originales no se tendrán en cuenta en el análisis.

Pasos siguientes

Una vez que la nueva recomendación tenga el estado **Listo para publicar**, revise la recomendación utilizando la información de [Revisar y publicar recomendaciones generadas de NSX Intelligence](#).

Revisar y publicar recomendaciones generadas de NSX Intelligence

Una vez que la recomendación de NSX Intelligence generada alcance el estado **Listo para publicar**, podrá revisarla, modificarla si es necesario y decidir si desea publicarla.

Requisitos previos

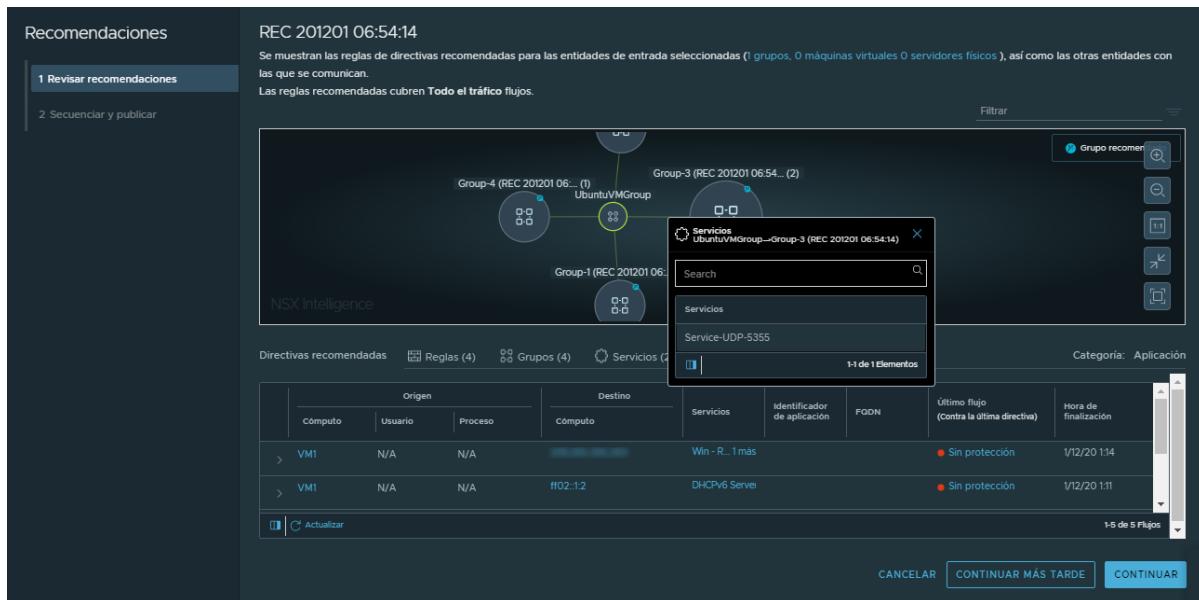
- Genere una nueva recomendación. Consulte [Generar una nueva recomendación de NSX Intelligence](#).
- Asegúrese de tener los privilegios necesarios antes de publicar las recomendaciones. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.

Procedimiento

- 1 En un navegador, inicie sesión con los privilegios necesarios en una instancia de NSX Manager desde `https://<dirección-ip-nsx-manager>`.
- 2 Haga clic en **Planificar y solucionar problemas > Recomendaciones**.
- 3 (opcional) Para limitar la lista de recomendaciones que se muestran, haga clic en **Filtro** en la parte superior derecha de la interfaz de usuario. Haga clic en **Aplicar filtro** y seleccione uno o varios filtros en el menú desplegable.
Por ejemplo, después de hacer clic en **Aplicar filtro**, seleccione **Detalles básicos > Supervisión > Activado** para mostrar solo las recomendaciones que tienen el parámetro de supervisión Activado.
- 4 (opcional) Si decide no utilizar la recomendación generada, haga clic en el  y seleccione **Eliminar**.

- 5 Para comenzar a revisar y administrar los detalles de la recomendación cuyo estado sea **Lista para publicar**, haga clic en el vínculo del nombre de la recomendación o haga clic en el  y seleccione **Revisar y publicar**.

Se abrirá el asistente **Recomendaciones**, que tiene un aspecto similar a la siguiente imagen. En el panel **Revisar recomendaciones**, los detalles de las recomendaciones se mostrarán en una vista dividida. La mitad superior del panel mostrará las recomendaciones en formato gráfico. La mitad inferior del panel mostrará las recomendaciones en formato tabular.



- 6 Utilice la mitad superior del panel para examinar una visualización gráfica de las recomendaciones.

Puede hacer clic en nodos y flechas de flujo específicos para ver los detalles de las recomendaciones. También puede apuntar a la flecha de flujo situada entre dos nodos de grupo para ver qué reglas de directiva se han aplicado entre grupos o qué servicios se han creado. Haga clic con el botón derecho en la flecha de flujo para filtrar la recomendación según las reglas de la directiva correspondiente.

Los nodos con el icono de la varita de recomendación  en la instancia de Edge indican que dicho nodo representa un grupo recomendado. Puede hacer clic con el botón derecho en un nodo para obtener una recomendación del grupo, cambiar el nombre del grupo o editar los miembros de la entidad informática que pertenecen a ese grupo. También puede hacer clic con el botón derecho en un nodo de grupo para cambiarle el nombre, verlo o editar sus miembros, o bien seleccionar **Filtrar por** para utilizar el grupo actual como el filtro utilizado para mostrar los detalles de la recomendación generada.

Los cambios que se realizan mediante la vista gráfica de las recomendaciones se aplicarán en la tabla que se encuentra en la mitad inferior del panel. De forma similar, los cambios realizados en la información de las recomendaciones de la tabla se aplicarán en la visualización gráfica.

- 7 En la mitad inferior del panel **Revisar recomendaciones**, puede utilizar la vista tabular de las recomendaciones para consultar los detalles de las reglas, los grupos y los servicios que se incluyen en la recomendación. Utilice la pestaña **Flujos utilizados para recomendaciones** para ver los flujos de tráfico no protegidos que se utilizaron para generar las recomendaciones.

Para examinar y modificar cualquiera de los detalles de la recomendación, haga clic en la pestaña **Reglas**, **Grupos** o **Servicios**.

En la sección **Directivas recomendadas** se muestran números en las pestañas **Reglas**, **Grupos** y **Servicios**. Estos números indican el número de reglas, grupos y servicios que se recomiendan. No existían en el inventario de NSX-T en el momento en que se generaron las recomendaciones. Por ejemplo, en la captura de pantalla anterior, la recomendación **Servicios** muestra cero servicio recomendados. Los servicios utilizados por los grupos existían en el inventario de NSX-T en el momento en que se generó la recomendación. Por lo tanto, no se recomiendan nuevos servicios.

Los cambios que se apliquen a las reglas de la pestaña **Reglas** (por ejemplo, añadir, eliminar o editar una regla o sección) se reflejarán inmediatamente en la tabla de reglas y en el panel visualización gráfica. En la tabla Reglas, las reglas que tienen la etiqueta **Nuevo** a la izquierda de su nombre indican que la regla es una regla recién generada, en lugar de una regla de DFW ya existente asociada a las entidades seleccionadas. Si se utilizó una regla existente, pero no se realizaron cambios en ella, la fila de la regla aparecerá atenuada. Si el motor de recomendación modificó una regla existente, la fila de esa regla no aparecerá atenuada y no tendrá la etiqueta Nuevo junto a ella.

- a Para editar los detalles de las columnas **Orígenes**, **Destinos** o **Se aplica a**, coloque el puntero en la columna correspondiente y haga clic en el icono Editar (lápiz).

En el cuadro de diálogo que aparezca (por ejemplo, **Establecer grupos de origen**), revise la regla recién recomendada o los grupos existentes que seleccionó el motor de recomendaciones. Si realiza cambios, haga clic en **Guardar**.

- b Para definir cómo se deben gestionar los paquetes cuando se cumple la regla de DFW, seleccione **Permitir**, **Anular** o **Rechazar** en la columna **Acción**.
- c Para activar o desactivar la regla de DFW, active el botón situado en el lado derecho de la columna **Acción**. De forma predeterminada, la regla que se generó está configurada como **Activated** cuando se publicó la recomendación.
- d Para revisar los detalles de los grupos de la recomendación, haga clic en la pestaña **Grupos**.

Antes de eliminar un grupo, asegúrese de que no lo utilice ninguna regla.

- e Haga clic en el vínculo de la columna **Miembros** para revisar los detalles de las máquinas virtuales, las direcciones IP y los servidores físicos que se establecieron para la recomendación de grupo.

- f Haga clic en el  situado junto al nombre del grupo y seleccione **Editar** para modificar la recomendación de grupo.

- g Haga clic en la pestaña **Servicios** y revise los detalles.
 - h Haga clic en el  situado junto al nombre del servicio y seleccione **Editar** para modificar el nombre o la descripción.

Antes de eliminar un servicio, asegúrese de que no lo utilice ninguna regla.
- 8 Para continuar con la publicación de la recomendación, haga clic en **Continuar**. Si lo prefiere, haga clic en **Continuar más tarde** para guardar los cambios que haya realizado y salir de la sesión de revisión de la recomendación.
- 9 En el panel **Secuenciar y publicar**, defina el orden en el que se aplicarán las directivas de seguridad recomendadas recientemente en relación con las reglas de DFW existentes.
- a Seleccione la fila de la nueva recomendación de directiva de seguridad.
 - b Haga clic en el  situado en el extremo izquierdo de la fila de una de las directivas de seguridad que aparecen.
 - c Para mover la fila seleccionada de la directiva de seguridad recién recomendada a una ubicación superior o inferior a la fila de la directiva de seguridad actual, seleccione **Mover las directivas seleccionadas encima de esta directiva** o **Mover las directivas seleccionadas debajo de esta directiva** en el menú.

Si lo prefiere, puede arrastrar la fila de recomendaciones de la nueva directiva seleccionada actualmente hacia arriba o hacia abajo hasta alcanzar la ubicación que deseé.
- 10 Haga clic en **Publicar**.
- Para interrumpir la revisión de la recomendación, haga clic en **Cancelar**.
- 11 En el cuadro de diálogo **Publicar recomendaciones**, haga clic en **Sí**.
- 12 En el cuadro de diálogo **Directivas publicadas**, haga clic en **Descartar** para cerrar el cuadro de diálogo, o haga clic en **Ver en la tabla Firewall distribuido** para ver las directivas de seguridad que se publicaron en la pestaña **Seguridad > Firewall distribuido > Todas las reglas**.
- De nuevo en el panel **Planificar y solucionar problemas > Recomendaciones**, la columna **Estado** de la recomendación que acaba de publicar se cambiará a **Publicado** en la tabla **Recomendaciones**.

Resultados

Una vez que las recomendaciones de la directiva de seguridad se hayan publicado correctamente, estarán en modo de solo lectura en la pestaña **Planificar y solucionar problemas > Recomendaciones**.

Recomendaciones. Para ver y administrar las recomendaciones de reglas publicadas, vaya a **Seguridad > Firewall distribuido**.

Importante Despues de haber publicado las recomendaciones de la regla, la visualización continuará mostrando los flujos afectados entre las entidades informáticas como flechas naranjas (flujos sin proteger) hasta que se generan nuevos flujos entre las entidades informáticas afectadas. La visualización solo notifica los flujos de tráfico en función de la hora en la que se produjeron en el host, y no refleja el conjunto de reglas publicadas después de que se hayan producido los flujos de tráfico. Una vez que se publica el conjunto de reglas y se generan nuevos flujos de tráfico, los nuevos flujos se mostrarán como flechas verdes (flujos permitidos).

Exportar NSX Intelligence como archivo JSON

Cuando una recomendación de NSX Intelligence generada alcanza el estado **Listo para publicar**, tiene la opción de exportarla como archivo JSON. Puede realizar modificaciones en este archivo antes de enviarlo como una solicitud de REST API para que la procese NSX Policy Manager.

Requisitos previos

- Genere una nueva recomendación. Consulte [Generar una nueva recomendación de NSX Intelligence](#).
- Asegúrese de tener los privilegios necesarios antes de exportar la recomendación. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.

Procedimiento

- 1 En un navegador, inicie sesión con los privilegios necesarios en una instancia de NSX Manager desde `https://<dirección-ip-nsx-manager>`.
- 2 Haga clic en **Planificar y solucionar problemas > Recomendaciones**.
- 3 (opcional) Muestre solo las recomendaciones de NSX Intelligence con el estado **Listo para publicar**.
 - a Haga clic en **Filtrar** en la zona superior derecha.
 - b En el menú desplegable **Aplicar filtro**, seleccione los filtros **Estado** y **Listo para publicar**.
 - c Haga clic en **Aplicar**.

- 4** En la lista de recomendaciones **Listo para publicar**, haga clic en el icono del  situado a la izquierda del nombre de la recomendación de NSX Intelligence que desea exportar. Seleccione **Exportar como JSON** en el menú desplegable.

En el siguiente fragmento de código se muestra un ejemplo de contenido parcial de un archivo JSON exportado.

```
{
  "resource_type": "Infra",
  "id": "Infra",
  "children": [
    {
      "resource_type": "ChildDomain",
      "id": "default",
      "marked_for_delete": false,
      "Domain": {
        "resource_type": "Domain",
        "id": "default",
        "children": [
          {
            "resource_type": "ChildGroup",
            "marked_for_delete": false,
            "Group": {
              "resource_type": "Group",
              "id": "Group-384fe490-837e-11eb-9688-dd7fccb572d0-904d61f0-0d71-4bc9-ac18-632b6b02efc9",
              "display_name": "Group-1 (REC 210312 01:59:18)",
              "description": "Created from REC 210312 01:59:18",
              "marked_for_delete": false,
              "expression": [
                {
                  "resource_type": "ExternalIDExpression",
                  "marked_for_delete": false,
                  ...
                  ...
                  "marked_for_delete": false
                }
              ]
            }
          }
        ]
      }
    }
  ]
}
```

- 5** Realice las modificaciones necesarias en el archivo JSON exportado antes de enviarlo como REST API que NSX Policy Manager pueda procesar.

Tenga en cuenta que a partir de NSX-T Data Center 3.1.1, debe eliminar la línea con la propiedad `"id" : "Infra"` del archivo JSON exportado antes de enviar la carga útil de JSON como una solicitud PATCH. De lo contrario, recibirá una respuesta 400 `Solicitud incorrecta` de NSX Policy Manager.

- 6 Con una herramienta de REST API externa, envíe el archivo JSON que contiene la recomendación de NSX Intelligence a NSX Policy Manager para su procesamiento.

Cuando envíe la recomendación de NSX Intelligence como una carga útil de JSON a su configuración de NSX-T Data Center mediante una herramienta REST API externa, como Postman, la aplicación NSX Intelligence no sabe si la recomendación se ha procesado correctamente. Esa recomendación de NSX Intelligence seguirá apareciendo con el estado **Listo para publicar** en la lista de recomendaciones. Si intenta revisar la recomendación haciendo clic en su nombre, recibirá el siguiente mensaje.

No se encontraron directivas recomendadas sin publicar. Es posible que se haya importado y publicado una versión de estas directivas recomendadas en NSX-T Data Center mediante una herramienta externa, o que se hayan eliminado.
- 7 Después de enviar correctamente la recomendación exportada como una carga útil de JSON, elimine manualmente esa recomendación de la lista de recomendaciones con el estado **Listo para publicar** en la tabla **Planificar y solucionar problemas > Recomendaciones**.

Detectar tráfico de red sospechoso en NSX-T Data Center

4

Puede detectar tráfico sospechoso, como actividad anómala y comportamiento malintencionado, en el entorno de NSX-T Data Center mediante la función Tráfico sospechoso de NSX disponible a partir de la versión 3.2 de la función NSX Intelligence.

Utilice la información de esta sección para comenzar a utilizar la función Tráfico sospechoso de NSX, analizar eventos de detección y administrar las definiciones de detectores de Tráfico sospechoso de NSX.

Este capítulo incluye los siguientes temas:

- [Introducción a la detección de tráfico de red sospechoso en NSX-T Data Center](#)
- [Análisis de los eventos de detección de Tráfico sospechoso de NSX](#)
- [Administrar las definiciones de detectores de Tráfico sospechoso de NSX](#)

Introducción a la detección de tráfico de red sospechoso en NSX-T Data Center

Debe conocer los requisitos previos que deben cumplirse antes de comenzar a utilizar la función Tráfico sospechoso de NSX. Obtenga una descripción general de cómo funciona, conozca la terminología utilizada con la función y prepare los detectores que desea utilizar para supervisar el flujo de tráfico de red en su entorno de NSX-T Data Center.

Requisitos previos para usar la función Tráfico sospechoso de NSX

El entorno de NSX-T Data Center debe cumplir los siguientes requisitos previos para poder utilizar la función Tráfico sospechoso de NSX.

- Compruebe que se cumplan todos los requisitos de licencia y software, incluida la configuración de la función NSX Intelligence.
Consulte [Requisitos del sistema para la función Tráfico sospechoso de NSX](#) para obtener detalles.
- Asegúrese de que tiene una función de NSX-T que esté autorizada para utilizar Tráfico sospechoso de NSX.

Para acceder a todas las funcionalidades de Tráfico sospechoso de NSX durante una sesión de NSX Manager, a la cuenta de usuario de NSX-T que utiliza se le debe asignar una de las siguientes funciones integradas de NSX-T Data Center. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.

- Usuario admin de organización
- Usuario admin de seguridad

Requisitos del sistema para la función Tráfico sospechoso de NSX

Antes de poder empezar a utilizar la función Tráfico sospechoso de NSX, el entorno de NSX-T Data Center y la función NSX Intelligence deben cumplir requisitos específicos de licencia y software.

Requisitos de licencia

Debe tener una de las siguientes licencias vigentes durante la sesión de NSX Manager. A continuación se enumeran las diversas licencias de NSX Data Center que admiten la función Tráfico sospechoso de NSX.

- NSX Data Center Evaluation
- NSX-T Evaluation
- NSX Advanced Threat Prevention (solo se aplica a clientes que hayan adquirido la licencia previamente).
- Complemento de NSX Advanced Threat Prevention para NSX Distributed Firewall con Threat Prevention
- Complemento de NSX Advanced Threat Prevention para NSX Distributed Firewall o NSX Advanced o NSX Enterprise Plus
- NSX Distributed Firewall con Advanced Threat Prevention
- NSX Gateway Firewall con Advanced Threat Prevention
- Complemento de NSX Advanced Threat Prevention para NSX Gateway Firewall
- Complemento de NSX-T Advanced con NSX Advanced Threat Prevention para NSX Distributed Firewall o NSX Advanced o NSX Enterprise Plus
- Complemento de NSX-T Enterprise Plus con NSX Advanced Threat Prevention para NSX Distributed Firewall o NSX Advanced o NSX Enterprise Plus

Requisitos de software

Debe cumplir los siguientes requisitos de software para poder empezar a utilizar la función Tráfico sospechoso de NSX.

- Instale NSX-T Data Center 3.2 o una versión posterior.
- Implemente VMware NSX® Application Platform mediante un formato avanzado.

- Active la aplicación NSX Intelligence 3.2 o versiones posteriores en NSX Application Platform.
- Configure la función NSX Intelligence 3.2 o versiones posteriores para recopilar solo los datos de tráfico de red de los clústeres o los hosts independientes específicos de los hosts que desea supervisar. La función Tráfico sospechoso de NSX solo se admite en hosts independientes o clústeres de hosts que tienen activada la recopilación de datos de tráfico. Para obtener más información sobre cómo configurar los ajustes de la función NSX Intelligence 3.2 o una versión posterior, consulte el documento *Activar y actualizar VMware NSX Intelligence*.
- Active la función NSX Network Detection and Response si va a trabajar con campañas para obtener un análisis más profundo de los eventos de tráfico sospechosos detectados mediante los servicios de nube VMware NSX® Advanced Threat Prevention. Consulte la información de activación de funciones en el documento *Guía de activación y administración de VMware NSX Network Detection and Response* que se proporciona con la función NSX Intelligence 3.2 o posterior en <https://docs.vmware.com/es/VMware-NSX-Intelligence/index.html>.

Nota Para proporcionar funcionalidades para un análisis más profundo de los eventos malintencionados o anómalos detectados, la función NSX Network Detection and Response requiere que el entorno de NSX-T Data Center 3.2 o versiones posteriores esté conectado a Internet.

Descripción general de la función Tráfico sospechoso de NSX

El objetivo de la función Tráfico sospechoso de NSX es detectar comportamientos de tráfico de red sospechosos o anómalos en el entorno de NSX-T Data Center.

Cómo funciona

Después de cumplir los requisitos previos, la función Tráfico sospechoso de NSX puede comenzar a generar análisis de amenazas de red en los datos de flujo de tráfico de red este-oeste que la aplicación NSX Intelligence ha recopilado a partir de las cargas de trabajo de NSX-T aptas (hosts o clústeres de hosts). La aplicación NSX Intelligence almacena los datos recopilados y los conserva durante 30 días. La función Tráfico sospechoso de NSX analiza los datos y marca las actividades sospechosas mediante los detectores compatibles. Puede ver la información sobre los eventos de amenazas detectados mediante la pestaña **Eventos de detección** de la página de la interfaz de usuario de Tráfico sospechoso de NSX.

Si se activa, la función NSX Network Detection and Response enviará los eventos sospechosos al servicio de nube de VMware NSX® Advanced Threat Prevention para un análisis más profundo. Si el servicio de NSX Advanced Threat Prevention determina que ciertos eventos sospechosos están relacionados, correlacionará esos eventos sospechosos en una campaña. A continuación, el servicio organizará los eventos de esa campaña en una escala de tiempo y los visualizará en la interfaz de usuario de NSX Network Detection and Response. Todos los eventos de amenazas se visualizan en la interfaz de usuario de NSX Network Detection and Response. El equipo de

seguridad de red puede investigar los eventos y las campañas de amenazas individuales. El servicio en la nube de NSX Advanced Threat Prevention obtiene actualizaciones periódicas de las amenazas detectadas anteriormente y actualiza las pantallas de visualización de la interfaz de usuario cuando es necesario.

Detectores compatibles

En la siguiente tabla se indican los detectores compatibles que utiliza la función Tráfico sospechoso de NSX para clasificar el tráfico de red sospechoso detectado. Las detecciones generadas por estos detectores pueden asociarse a técnicas o tácticas específicas en el [marco ATT&CK® de MITRE](#).

Estos detectores están desactivados de forma predeterminada, por lo que deberá activar explícitamente cada detector que deseé utilizar en su entorno de NSX-T. Consulte [Activar los detectores de Tráfico sospechoso de NSX](#) para obtener más información sobre los requisitos previos y cómo activar los detectores.

Puede administrar las listas de exclusión y el valor de probabilidad de algunas de las definiciones de estos detectores compatibles mediante la pestaña **Definiciones de detector**. Consulte [Administrar las definiciones de detectores de Tráfico sospechoso de NSX](#) para obtener detalles.

Tabla 4-1. Categorías de detector utilizadas para detectar tráfico sospechoso

Nombre del detector	Descripción
Carga y descarga de datos	Detecta transferencias de datos inusualmente grandes (cargas/descargas) de un host.
Generador de perfiles de IP de destino	Detecta los intentos de los dispositivos internos de realizar conexiones inusuales hacia otros hosts internos.
Túnel de DNS	Detectar los intentos de un dispositivo interno de comunicarse de forma encubierta con un servidor externo si se está utilizando el tráfico DNS.
Algoritmo de generación de dominio (DGA)	Detectar anomalías en las búsquedas de DNS realizadas por un host interno que podrían deberse a malware DGA.
Exploración de puertos horizontales	Detectar si un intruso intenta escanear uno o varios puertos o servicios en varios sistemas (barrido).
Envenenamiento y retransmisión de LLMNR/NBT-NS	Permite detectar si una máquina virtual muestra un patrón de respuesta inusual para las solicitudes LLMNR/NBT-NS.
Señalización de Netflow	Detecta el comportamiento de señalización desde un host interno.
Descarte de tráfico de red	Detectar si una regla de firewall distribuido descarta una cantidad inusualmente alta de tráfico.
Generador de perfiles de puerto	Permite detectar cuándo un host de cliente interno se comunica con un host externo en un puerto inusual.
Generador de perfiles de puerto de servidor	Detecta cuándo otro host interno está conectado a un host interno en un puerto inusual.
Servicios remotos	Detecta un comportamiento sospechoso de las conexiones remotas, como telnet, SSH y VNC.

Tabla 4-1. Categorías de detector utilizadas para detectar tráfico sospechoso (continuación)

Nombre del detector	Descripción
Puerto de uso no común	Detecta que el tráfico del identificador de aplicación de capa 7 no coincide con el puerto o el protocolo asignados estándar. Por ejemplo, el tráfico SSH se ejecuta en un puerto no estándar en lugar del puerto estándar 22.
Patrón de tráfico de red inusual	Detecta anomalías en el perfil de serie temporal de un host.
Exploración de puertos verticales	Detectar si un intruso intenta atacar varios puertos o servicios abiertos de un mismo sistema (escaneado).

Terminología utilizada con la función Tráfico sospechoso de NSX

Familiarícese con la terminología que se utiliza con la función Tráfico sospechoso de NSX.

Terminología	Definición
Evento de anomalía	La terminología utilizada en la versión anterior de NSX Intelligence en la que se introdujo la función NSX Anomaly Detection (ahora Tráfico sospechoso de NSX) como una función de vista previa de tecnología. Este término ahora se reemplazará por Evento de detección.
Campaña	Un conjunto correlacionado de incidentes que afectan a uno o varios dispositivos durante un período de tiempo. Si la función NSX Network Detection and Response está activada, los vínculos a las campañas se mostrarán en la interfaz de usuario de Tráfico sospechoso de NSX, cuando corresponda.
Puntuación de confianza	La puntuación calculada para indicar la confianza del sistema en que un evento es anómalo en función de los algoritmos propietarios que utiliza la función Tráfico sospechoso de NSX.
Evento de detección	Una actividad de tráfico de red que se desvía de lo que se considera estándar o esperado. Un detector de Tráfico sospechoso de NSX genera los datos.
Detector	Un sensor diseñado para detectar eventos en el flujo de tráfico de red. Un detector se asigna a una única categoría o técnica ATT&CK de MITRE.
Puntuación de impacto	Una puntuación calculada por un algoritmo patentado que utiliza una combinación de la puntuación de confianza para el evento de detección y su gravedad, si se detecta correctamente.
Gravedad	Indica la gravedad de una amenaza. Los valores válidos son Crítico, Alto, Medio o Bajo.
Táctica	Representa el motivo por el cual un grupo está realizando una acción mediante una técnica o subtécnica de ATT&CK. Consulte https://attack.mitre.org/ para obtener información sobre el marco ATT&CK de MITRE.
Técnica	Representa el modo en que un grupo intenta alcanzar un objetivo táctico de su ataque mediante una acción. Consulte https://attack.mitre.org/ para obtener información sobre el marco ATT&CK de MITRE.

Activar los detectores de Tráfico sospechoso de NSX

Antes de que se detecten amenazas o datos sospechosos de tráfico de red en su entorno de NSX-T Data Center, debe activar manualmente los detectores de Tráfico sospechoso de NSX que

desea utilizar. Solo los detectores que estén activados se utilizarán para supervisar eventos de tráfico de red sospechosos.

Requisitos previos

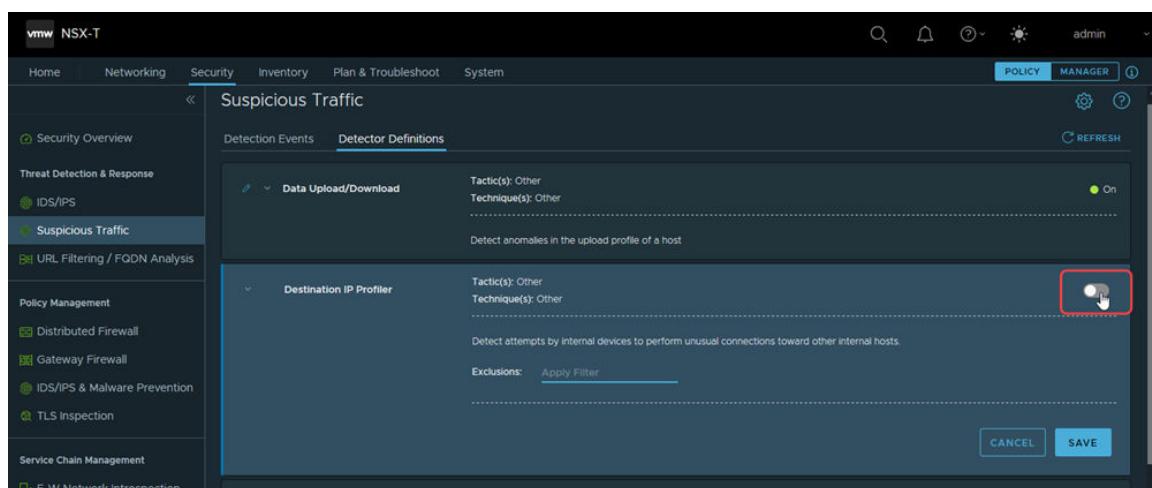
- Compruebe que se cumplen los requisitos de licencia y software especificados en [Requisitos del sistema para la función Tráfico sospechoso de NSX](#).
- Debe haber iniciado sesión en NSX Manager con una de las siguientes funciones integradas en NSX-T Data Center. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.
 - Usuario admin de organización
 - Usuario admin de seguridad

Procedimiento

- 1 En un navegador, inicie sesión con los privilegios necesarios en un dispositivo de NSX Manager desde <https://<dirección-ip-nsx-manager>>.
- 2 Utilice los siguientes pasos para activar un detector de Tráfico sospechoso de NSX compatible para realizar un análisis del tráfico de red en los datos de tráfico recopilados.

Tenga en cuenta que los siguientes pasos son para todos los detectores disponibles, excepto para los basados en DNS, que deben configurarse manualmente antes de que se puedan utilizar. Consulte el siguiente paso después de este para obtener información sobre la configuración de detectores basados en DNS.

- a Desplácese hasta la pestaña **Seguridad > Tráfico sospechoso > Definiciones de detector**.
- b Busque el detector que desea activar y haga clic en **Editar** (ícono de lápiz).
- c Busque el commutador de alternancia en el extremo derecho de la fila expandida y haga clic en el commutador de alternancia para activar el detector, como se muestra en la siguiente imagen.



- d Haga clic en **Guardar**.

- 3 Para activar detectores basados en DNS, como el algoritmo de generación de dominios (DGA) y la tunelización de DNS, realice los siguientes pasos una sola vez.
- Cree un perfil de contexto de DNS personalizado o utilice un perfil de contexto predeterminado proporcionado por el sistema.
Consulte los detalles sobre cómo agregar un perfil de contexto en la *Guía de administración de NSX-T Data Center* de la versión 3.2 o posteriores en <https://docs.vmware.com/es/VMware-NSX-T-Data-Center/index.html>.
 - Cree una regla de firewall distribuido usando **ANY** en las columnas **Orígenes** y **Destinos**; y usando el perfil de contexto de DNS, si creó uno.
Consulte los detalles sobre cómo agregar una regla de firewall distribuido en la *Guía de administración de NSX-T Data Center* de la versión 3.2 o posteriores en <https://docs.vmware.com/es/VMware-NSX-T-Data-Center/index.html>.
 - Desplácese hasta la pestaña **Seguridad > Tráfico sospechoso > Definiciones de detector**.
 - Busque el detector basado en DNS que desea activar y haga clic en **Editar** (ícono de lápiz).
 - En el extremo derecho de la fila expandida, busque el commutador de alternancia para ese detector basado en DNS. Para activar el detector, haga clic en el commutador de alternancia.
 - Haga clic en **Guardar**.

Resultados

Los commutadores de alternancia de los detectores activados se muestran activados en la pestaña **Definiciones de detector**.

Pasos siguientes

Administre los eventos de tráfico sospechoso detectados. Consulte [Análisis de los eventos de detección de Tráfico sospechoso de NSX](#) para obtener detalles.

Análisis de los eventos de detección de Tráfico sospechoso de NSX

Dado que la función Tráfico sospechoso de NSX genera análisis de amenazas de red en los datos de flujo de tráfico de red recopilados, informa sobre los eventos sospechosos detectados mediante la página **Eventos de detección**. Puede ver los eventos de detección en un gráfico de burbujas, una cuadrícula o ambos.

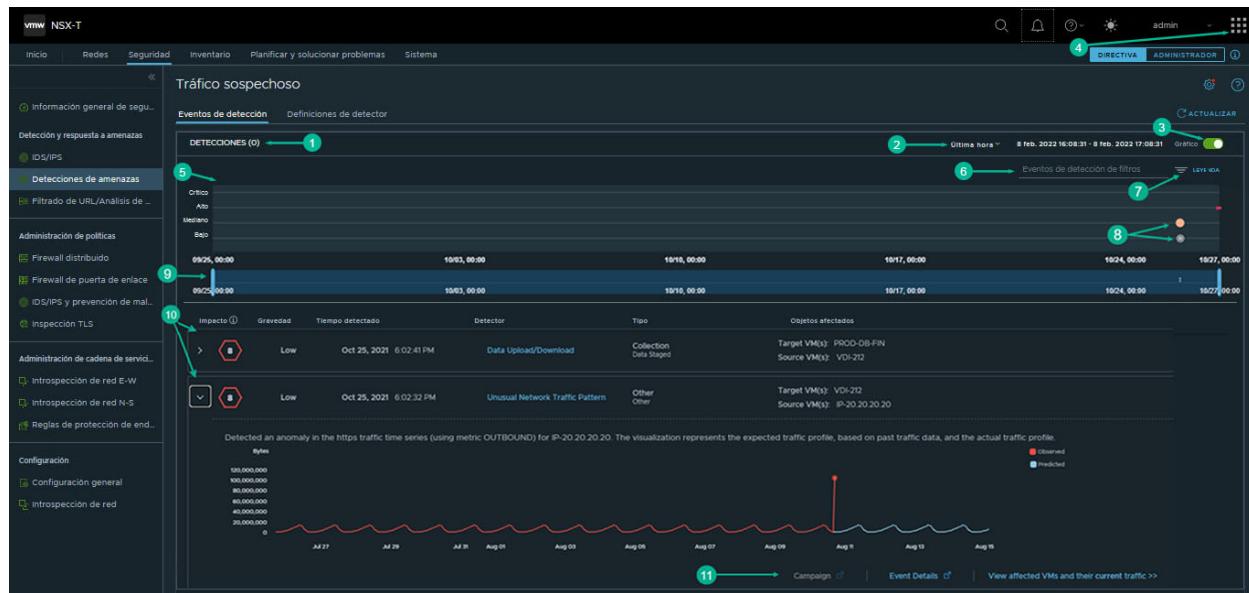
Requisitos previos

- La aplicación NSX Intelligence 3.2 o una versión posterior debe estar activada y los detectores de Tráfico sospechoso de NSX también deben estar activados. Consulte [Introducción a la detección de tráfico de red sospechoso en NSX-T Data Center](#).

- Debe haber iniciado sesión en NSX Manager con una de las siguientes funciones NSX-T.
 - Usuario admin de organización
 - Usuario admin de seguridad

Administrar eventos de detección

De forma predeterminada, cuando se desplaza hasta **Seguridad > Tráfico sospechoso > Eventos de detección**, se muestran los eventos de detección tanto en el gráfico de burbujas como en los formatos de cuadrícula, como se muestra en la siguiente imagen. La tabla que sigue a la imagen describe las secciones numeradas resaltadas en la imagen.



Sección	Descripción
1	Proporciona el número total de detecciones de eventos sospechosos que realizó la función de Tráfico sospechoso de NSX durante el período de tiempo seleccionado.
2	En esta sección, seleccione el período de tiempo que utiliza el sistema para determinar qué datos históricos sobre los eventos detectados notifica Tráfico sospechoso de NSX en esta página de la interfaz de usuario. El período de tiempo va desde la hora actual hasta un determinado período de tiempo en el pasado. El período de tiempo predeterminado es Última hora . Para cambiar el período de tiempo seleccionado, haga clic en la selección actual y seleccione otro en el menú desplegable. Las selecciones disponibles son Última hora , Últimas 12 horas , Últimas 24 horas , Última semana , Últimas 2 semanas y Último mes .
3	La opción Gráfico determina si se muestra o no el gráfico de burbujas. Cuando la opción Gráfico está desactivada, solo la cuadrícula muestra información sobre los eventos de detección. De forma predeterminada, está en la posición Activado .

Sección	Descripción
4	<p>Si la función NSX Network Detection and Response está activada, cuando esté viendo la interfaz de usuario de Tráfico sospechoso de NSX, el icono del lanzador de aplicaciones  estará visible en la esquina superior derecha de la interfaz de usuario.</p> <p>Para ver más detalles sobre los eventos anómalos detectados mediante la interfaz de usuario de NSX Network Detection and Response, haga clic en el icono  y seleccione NSX Network Detection and Response. En la interfaz de usuario NSX Network Detection and Response, vuelva a hacer clic en el icono del lanzador de aplicaciones y seleccione NSX-T para volver a la interfaz de usuario de Tráfico sospechoso de NSX.</p>
5	<p>Este gráfico de burbujas proporciona una escala de tiempo visual de cuándo se produjeron los eventos detectados durante el período de tiempo seleccionado. Cada evento se traza en función de la gravedad del evento de detección. A continuación se muestran las categorías de gravedad y sus correspondientes puntuaciones de gravedad.</p> <ul style="list-style-type: none"> ■ Crítico: 75-100 ■ Alto: 50-74 ■ Mediano: 25-49 ■ Bajo: 0-24
6	<p>El área de filtro permite delimitar los eventos de detección que se muestran para el período de tiempo seleccionado. Haga clic en Eventos de detección de filtros y seleccione en el menú desplegable los filtros que desee aplicar y los elementos específicos en el menú desplegable adicional que se muestra. Los filtros disponibles incluyen los siguientes.</p> <ul style="list-style-type: none"> ■ Puntuación de confianza: la puntuación que asigna el sistema en función de la confianza con que un evento es anómalo mediante los algoritmos propietarios que utiliza la función Tráfico sospechoso de NSX. ■ Detector: sensor diseñado para detectar eventos anómalos en el flujo de tráfico de red. Un detector se asigna a una única categoría o técnica ATT&CK de MITRE. ■ Puntuación de impacto: una puntuación calculada por un algoritmo patentado que utiliza una combinación de la puntuación de confianza para el evento de detección y su gravedad, si se detecta correctamente. ■ Tácticas: representa el motivo por el cual un grupo organizativo realizó una acción con una táctica de ATT&CK. ■ Técnicas: representa cómo un grupo organizativo intenta alcanzar un objetivo táctico de su ataque mediante técnicas o subtécnicas específicas. ■ Máquinas virtuales: las máquinas virtuales que participan en los eventos detectados que se produjeron durante el período de tiempo seleccionado.
7	<p>Haga clic en Enviar para ver una lista de los distintos tipos de globos que pueden aparecer en el gráfico de burbujas. La siguiente lista describe cada globo y el tipo de evento de detección que representa.</p> <ul style="list-style-type: none"> ■ Persistencia: el grupo está intentando mantener su retención en los sistemas de la red. ■ Acceso a credenciales: el grupo está intentando robo de nombres de cuentas y contraseñas. ■ Detección: el grupo está intentando obtener información sobre su entorno de red. ■ Comando y control: el servidor intenta comunicarse con sistemas comprometidos y controlarlos. ■ Movimiento lateral: un grupo está intentando pasar por el entorno de red. ■ Recopilación: un administrador intenta recopilar información que sería útil en su objetivo final. ■ Exfiltración: el grupo está intentando quitar datos de la red. ■ Otro: el detector no se puede asociar a una táctica específica según se define en el marco ATT&CK de MITRE. ■ Varios eventos: se produjo más de un evento de detección en el mismo segmento de tiempo. Al mover el control deslizante de la ventana de tiempo a la derecha, se cambia el alcance del tipo de burbujas que se muestran, por lo que una burbuja de varios eventos se puede dividir en varios y en otros tipos de burbujas.

Sección	Descripción
8	Cada globo del gráfico representa un evento de detección o varios eventos que se produjeron durante el período de tiempo seleccionado. El color o el tipo de burbuja representan la táctica utilizada por el enrutador durante el ataque detectado. Consulte las descripciones en Leyenda para obtener más información.
9	El control deslizante de la ventana de tiempo permite ver los eventos de detección que se produjeron dentro de un subconjunto del período de tiempo seleccionado. El área azul resaltada representa lo que se muestra en el gráfico de burbujas. Cuando deslice el control deslizante hacia la derecha o la izquierda, el gráfico de burbujas se actualizará con los eventos de detección que se produjeron durante el período resaltado en el control deslizante. Si se producen eventos de detección al mismo tiempo, una burbuja Varios eventos representará esos eventos de detección. Al mover el control deslizante hacia la derecha, observará que la burbuja Varios eventos se expande a varias burbujas que representan los diferentes eventos de detección que se produjeron en ese período de tiempo.

Sección	Descripción
10	<p>La cuadrícula muestra información acerca de cada evento de detección identificado por la función Tráfico sospechoso de NSX durante el período de tiempo seleccionado. Cuando no se expande, una fila muestra los siguientes datos de eventos clave.</p> <ul style="list-style-type: none"> ■ Impacto: la puntuación de impacto que la función Tráfico sospechoso de NSX calculó para el evento de detección ■ Gravedad: indica la gravedad del evento. Los valores posibles son Bajo, Medio, Alto y Crítico. Estos valores se corresponden con los que se utilizan en el gráfico de burbujas. ■ Hora detectada: la fecha y la hora en que se detectó el evento. ■ Detector: el nombre del detector que usó la función Tráfico sospechoso de NSX para detectar el evento. Al hacer clic en el nombre del detector, un cuadro de diálogo mostrará información adicional sobre el detector, como su objetivo, la categoría de ATT&CK y un resumen sobre el detector. La sección categoría de ATT&CK incluye un vínculo al sitio web de ATT&CK de MITRE que proporciona más detalles sobre esa categoría de ATT&CK en particular que se utiliza en el evento de detección. ■ Tipo: muestra la táctica y la técnica utilizadas en el evento de detección. ■ Objetos afectados: muestra las máquinas virtuales de origen y las máquinas virtuales de destino involucradas en el evento de detección. <p>La captura de pantalla de ejemplo también muestra una fila expandida. Cuando se expande, una fila muestra información de eventos adicional. Los detalles incluyen un resumen del evento detectado y una explicación de la visualización o de los datos de eventos adicionales que se muestran en la fila expandida. Por ejemplo, en la captura de pantalla anterior, la fila expandida muestra un resumen del evento detectado y lo que representa la visualización. No todos los eventos de detección tendrán visualización. Otros solo tienen datos detallados adicionales.</p>
11	<p>Una fila expandida también puede mostrar uno o varios vínculos en la esquina inferior derecha. Cuando se hace clic en ella, se muestra un vínculo a otra página de la interfaz de usuario en la que se proporciona más información sobre el evento detectado. A continuación se muestran los vínculos disponibles, cuando se aplican al evento de detección.</p> <p>Es posible que se habilite el siguiente vínculo, aunque la función NSX Network Detection and Response no está activada.</p> <ul style="list-style-type: none"> ■ Ver las máquinas virtuales afectadas y su tráfico actual: al hacer clic en este vínculo, el sistema mostrará el lienzo de visualización en la pestaña Planificar y solucionar problemas. Muestra las entidades informáticas involucradas en el evento de detección. Consulte Trabajar con la vista Recursos informáticos para obtener más información. <p>Si la aplicación NSX Network Detection and Response está activada, es posible que los siguientes vínculos también estén disponibles si corresponde al evento.</p> <ul style="list-style-type: none"> ■ Campaña: si el servicio de nube NSX Advanced Threat Prevention identificó que este evento de detección forma parte de una campaña, este vínculo está habilitado. Al hacer clic en el vínculo, los detalles de la campaña se muestran en la página Campañas de la interfaz de usuario de NSX Network Detection and Response. Consulte Administrar la página Campañas para obtener más información. ■ Detalles del evento: al hacer clic en este vínculo, se abrirá una nueva pestaña del navegador y se mostrarán más detalles sobre el evento de detección en la página Perfil del evento de la interfaz de usuario de NSX Network Detection and Response. Consulte Trabajar con la página Eventos para obtener más información.

Administrar las definiciones de detectores de Tráfico sospechoso de NSX

La pestaña **Definiciones de detector** en la página **Tráfico sospechoso** muestra todos los detectores compatibles actualmente con la función Tráfico sospechoso de NSX.

Un detector se desactiva de forma predeterminada. Debe activar manualmente cada detector para poder empezar a supervisar los flujos de tráfico de red en su entorno de NSX-T. Consulte [Activar los detectores de Tráfico sospechoso de NSX](#) para obtener detalles.

Cada detector de Tráfico sospechoso de NSX que aparece en la pestaña **Definiciones de detector** por lo general incluye lo siguiente.

- Nombre y descripción del detector
- Botón de alternancia Habilitar/deshabilitar
- Control deslizante de probabilidad (sensibilidad)

El control deslizante permite establecer la probabilidad de que un detector genere una alerta.

Para una detección que se encuentra por debajo del umbral de probabilidad, el sistema descartará el evento de detección. Este control deslizante no se incluye para todos los detectores.

- Exclusiones

Una exclusión de máquina virtual es una lista estática de máquinas virtuales que el detector excluye de la función Tráfico sospechoso de NSX. Para una exclusión de grupo, si el detector excluye un miembro dependerá de cuándo ejecuta el sistema el detector. Si el grupo no existe en el momento en que el sistema ejecuta el detector, es posible que el sistema genere una advertencia en los registros del sistema. Si la máquina virtual no existe en el momento en que el sistema ejecuta el detector, el detector ignorará silenciosamente la configuración de exclusión. La exclusión de grupos no es compatible con todos los detectores de Tráfico sospechoso de NSX.

Modificar algunos valores de propiedad de una definición de detector

Para modificar algunos de los valores de propiedad predeterminados para seleccionar definiciones de detector de Tráfico sospechoso de NSX, utilice la pestaña **Definiciones de detector**.

La siguiente imagen muestra un ejemplo de una definición de detector que está en modo de edición.



Requisitos previos

- Se debe activar la aplicación NSX Intelligence 3.2 o una versión posterior.
- Debe haber iniciado sesión en NSX Manager con una de las siguientes funciones NSX-T.
 - Usuario admin de organización

- Usuario admin de seguridad

Procedimiento

- 1 En un navegador, inicie sesión con los privilegios necesarios en un dispositivo de NSX Manager desde <https://<dirección-ip-nsx-manager>>.
- 2 Desplácese hasta la pestaña **Seguridad > Tráfico sospechoso > Definiciones de detector**.
- 3 Busque el detector cuya definición desea modificar y haga clic en **Editar** (ícono de lápiz).
- 4 Para activar o desactivar el detector, haga clic en el botón de alternancia.
- 5 Si se incluye un control deslizante en la definición, mueva el control deslizante al valor deseado que utiliza el detector para generar un evento de detección.
Si se establece el control deslizante en un valor menor, es más probable que ese detector genere un evento de detección.
- 6 Defina la lista de exclusión.
 - a Haga clic en Aplicar filtro y, en el menú desplegable, seleccione **Grupos o Máquinas virtuales** para el origen.
 - b Realice su selección en la lista de grupos o máquinas virtuales disponibles.
 - c Haga clic en **Aplicar**.
- 7 Haga clic en **Guardar**.

Trabajar con la aplicación NSX Network Detection and Response

5

La aplicación VMware NSX® Network Detection and Response™ ofrece un conjunto perfectamente integrado de capacidades de detección y respuesta de red para la seguridad norte-sur y este-oeste dentro de su entorno de NSX-T Data Center. Esta función está disponible a partir de NSX Intelligence versión 3.2 y NSX-T Data Center versión 3.2.

Este capítulo incluye los siguientes temas:

- Requisitos previos para usar la aplicación NSX Network Detection and Response
- Terminología utilizada con la función NSX Network Detection and Response
- Introducción a la interfaz de usuario de NSX Network Detection and Response
- Explorar la página del panel de control
- Administrar la página Campañas
- Trabajar con la página Hosts
- Trabajar con la página Eventos
- Administrar la página Incidentes
- Trabajar con la página de archivos descargados
- Uso de la página de administración de alertas
- Uso del informe Análisis

Requisitos previos para usar la aplicación NSX Network Detection and Response

Debe cumplir los siguientes requisitos previos antes de comenzar a utilizar todas las funcionalidades de la aplicación NSX Network Detection and Response.

- Familiarícese con el objetivo principal de la aplicación NSX Network Detection and Response y comprenda su flujo de trabajo de activación y uso.

Consulte la información de introducción en la *Guía de activación y administración de VMware NSX Network Detection and Response* que se ofrece con el conjunto de documentación de NSX Intelligence para la versión 3.2 o posterior en <https://docs.vmware.com/es/VMware-NSX-Intelligence/index.html>.

- Active la aplicación NSX Network Detection and Response en NSX Application Platform. Consulte la información sobre los requisitos del sistema y la activación de aplicaciones en el documento *Guía de activación y administración de VMware NSX Network Detection and Response* incluido en la documentación de NSX Intelligence para la versión 3.2 o posterior en <https://docs.vmware.com/es/VMware-NSX-Intelligence/index.html>.
- Asegúrese de que tiene una función de NSX-T que esté autorizada para utilizar la aplicación NSX Network Detection and Response. Para acceder a todas las funcionalidades de NSX Network Detection and Response, la cuenta de usuario que utilice durante la sesión de NSX Manager debe tener asignada una de las siguientes funciones integradas de NSX-T. Consulte [Control de acceso basado en funciones en NSX Intelligence](#) para obtener más información.
 - Usuario admin de organización
 - Usuario admin de seguridad
 - Operador de seguridad
 - Auditor (acceso de solo lectura)

Terminología utilizada con la función NSX Network Detection and Response

Familiarícese con la siguiente terminología clave que se utiliza con la función NSX Network Detection and Response.

Terminología	Definición
Campaña	Un conjunto correlacionado de incidentes que afectan a una o varias cargas de trabajo durante un período de tiempo.
Evento	Representa una actividad relevante para la seguridad que se ha producido en la red supervisada. Un evento puede incluir varios flujos de datos (por ejemplo, conexiones TCP), pero representa un solo tipo de actividad que se produce entre un par específico de direcciones IP durante un breve período de tiempo. Varios eventos se agregan automáticamente en incidentes.
Incidente	Representa una actividad relevante para la seguridad que se ha producido en la red supervisada. Un incidente puede constar de un solo evento o de varios eventos que se agregaron automáticamente a un incidente.
Infección	Un incidente que se determinó como crítico. El asunto debe ser un asunto que se debe incluir sin demora.
Molestia	Un incidente de bajo riesgo. Por lo general, esto corresponde a una actividad potencialmente no deseada/peligrosa que no necesariamente implica un riesgo o una vulneración en la red supervisada. Se realiza un seguimiento de las molestias, ya que contribuyen a proporcionar una concienciación situacional de red más completa.

Terminología	Definición
Puntuación del impacto del evento	<p>La puntuación de impacto general calculada para un evento detectado por la función NSX Network Detection and Response. La puntuación oscila entre 0 y 100, siendo 100 la detección más peligrosa. Se utilizan los siguientes niveles de impacto de eventos.</p> <ul style="list-style-type: none"> ■ Bajo: impacto entre 1 y 29 ■ Mediano: impacto entre 30 y 69 ■ Alto: impacto entre 70 y 100
Lista de inspección	<p>Un incidente que se determinó como de riesgo medio. Estos incidentes, aunque indican un riesgo potencial, no requieren una atención inmediata. Se mantienen bajo una estrecha inspección en caso de que aparezca una nueva evidencia que modifique su estado.</p> <p>Por ejemplo, un incidente relacionado con un comando no operativo y una infraestructura de control se clasifica como una lista de supervisión.</p>

Introducción a la interfaz de usuario de NSX Network Detection and Response

La interfaz de usuario (IU) de NSX Network Detection and Response proporciona un único punto de control para administrar los eventos de amenazas y las campañas correlacionadas detectadas en su entorno NSX-T, así como para ver los informes generados sobre dichas amenazas.

Importante Para acceder a la interfaz de usuario de NSX Network Detection and Response, primero debe activar la aplicación NSX Network Detection and Response en NSX Application Platform. También debe activar una o varias de las funciones de NSX cuyos eventos de detección consume la aplicación NSX Network Detection and Response. Consulte la *Guía de activación y administración de VMware NSX Network Detection and Response* para obtener una descripción general de una aplicación y los detalles sobre cómo activarla.

Algunos elementos de la interfaz de usuario de NSX Network Detection and Response solo están visibles si activa la función o la aplicación correspondientes del elemento que proporciona los eventos que consume la aplicación NSX Network Detection and Response.

Acceder a la interfaz de usuario de

Si hay informes de eventos o campañas generadas, puede acceder a la interfaz de usuario (IU) de NSX Network Detection and Response mediante uno de los siguientes métodos.

- Haga clic en el icono del programa de inicio de la aplicación  en la esquina superior derecha de la interfaz de usuario de NSX Manager y seleccione **NSX Network Detection and Response**.
- Desplácese hasta **Seguridad > Información general de seguridad** en la interfaz de usuario de NSX Manager y en la pestaña **Threat Detection & Response > Campañas**, haga clic en **Ir a Campañas**.

- Si activó NSX Intelligence, desplácese hasta **Seguridad > Tráfico sospechoso** en la interfaz de usuario de NSX Manager. Expanda la fila de un evento sospechoso detectado, haga clic en **Campañas** o **Detalles del evento**, si está disponible. Estos vínculos solo aparecen si hay campañas o informes de eventos disponibles para la actividad sospechosa detectada.
- Si activó la aplicación VMware Prevención de malware de NSX®, desplácese hasta **Seguridad > Prevención de malware** en la interfaz de usuario de NSX Manager, expanda la fila de un malware notificado y haga clic en **Campañas** o **Detalles del evento**, si están disponibles. Estos vínculos solo aparecen si hay campañas o informes de eventos disponibles para el malware detectado.

En las siguientes secciones se describen las áreas comunes que se ven al desplazarse por la interfaz de usuario de NSX Network Detection and Response. En el lado izquierdo de la interfaz se encuentra el menú de navegación principal. En la parte superior de casi todas las páginas se encuentran los widgets de configuración de pantalla. Los datos presentados en las páginas de la interfaz de usuario se muestran con la configuración de pantalla que seleccionó.

Navegar por la interfaz de

Puede utilizar el menú de navegación principal de la parte izquierda de la página del navegador para acceder a las páginas de nivel superior correspondientes de la interfaz de usuario de NSX Network Detection and Response. Para contraer temporalmente este menú de navegación, haga clic en  en la esquina superior derecha del panel de menú. Al acceder por primera vez a la interfaz de usuario de NSX Network Detection and Response, la página **Panel de control** estará seleccionada de forma predeterminada. La página **Panel de control** contiene widgets que proporcionan una descripción general de varios elementos que se supervisan. Estos widgets se describen más detalladamente en [Explorar la página del panel de control](#).

Para acceder a otra página de interfaz de NSX Network Detection and Response, haga clic en su pestaña correspondiente en el menú de navegación principal de la izquierda. Cada página con pestañas consta de varios widgets que proporcionan más información sobre las áreas supervisadas. Los temas disponibles más adelante en esta guía proporcionan detalles sobre cada una de estas páginas de la interfaz de usuario de NSX Network Detection and Response.

Configurar el tema de visualización

Establezca el tema de visualización utilizado en la sesión de NSX Network Detection and Response actual mediante el ícono del modo de tema para mostrar en la sección superior derecha de la interfaz. El ícono que se muestra depende del tema de visualización que se esté utilizando en ese momento. Para cambiar a un modo de tema claro, haga clic en . Para cambiar a un modo de tema oscuro, haga clic en .

Obtener asistencia

Para acceder a los temas de NSX Network Detection and Response disponibles incluidos el documento *Usar y administrar VMware NSX Intelligence*, haga clic en  y, a continuación, en **Ayuda**.

Para ver el estado de la conexión con conector de nube de NSX Network Detection and Response, haga clic en **Comprobar estado de conectividad**. El conector de nube proporciona un túnel seguro de comunicación entre la sesión de NSX Manager y los servicios de nube de NSX Advanced Threat Prevention.

Si encuentra algún problema de conectividad que no pueda resolver con la información de la sección Solución de problemas de esta documentación, haga clic en **ticket de soporte** e informe del problema.

Acceder a la interfaz de usuario principal de NSX-T

Para volver a la interfaz de usuario principal de NSX Manager, haga clic en  situado en la esquina superior derecha y seleccione **NSX-T**.

Configurar el intervalo de tiempo

Para especificar el número de días de datos que se mostrarán en los widgets de NSX Network

Detection and Response, utilice el botón **Intervalo de tiempo** .

Para desplazarse hacia atrás y hacia adelante con la selección de fecha mientras se mantiene constante el rango de fechas seleccionado, haga clic en  o  situado a ambos lados del botón **INTERVALO DE TIEMPO: ÚLTIMOS 7 DÍAS**. Por ejemplo, suponiendo que el intervalo de tiempo predeterminado es de 7 días, al hacer clic en el botón de flecha hacia la izquierda una vez, se seleccionará un intervalo con la fecha de finalización 7 días atrás.

Puede definir un intervalo de tiempo más detallado mediante la ventana emergente **Intervalo de tiempo**. Haga clic en el botón **INTERVALO DE TIEMPO: ÚLTIMOS 7 DÍAS** y seleccione **Relativo** (valor predeterminado) o **Absoluto** en el menú desplegable. En el modo Relativo, seleccione el número de días transcurridos desde la fecha actual para los que desea que se muestren los datos. El valor predeterminado es 7 días, el mínimo es 1 día y el máximo es 31 días. En el modo Absoluto, introduzca las fechas en **Desde** y **Hasta** seleccionando las fechas de la ventana emergente del calendario. Para guardar los cambios, haga clic en **Aplicar**.

Usar el botón Ver opciones

Todos los datos de fecha y hora que se muestran en la interfaz de NSX Network Detection and Response utilizan la zona horaria UTC predeterminada hasta que la cambie.

Para cambiar la zona horaria utilizada para los datos mostrados, haga clic en situado en la parte superior derecha de la interfaz y seleccione la zona horaria seleccionada actualmente. En la ventana emergente **Zona horaria**, haga clic en el menú desplegable y seleccione una zona horaria diferente. Para limitar la selección del menú, comience a introducir el nombre de una zona horaria en el cuadro de búsqueda. Después de seleccionar la zona horaria deseada, haga clic en **Aplicar**.

Administrar los widgets

Cada una de las páginas de la interfaz de usuario de NSX Network Detection and Response consta de varios widgets que muestran detalles sobre las amenazas detectadas y los informes generados a partir del análisis de dichas amenazas.

Puede administrar los widgets con la siguiente información.

- Para volver a cargar los datos mostrados en un widget, haga clic en en la esquina superior derecha del widget.
- Puede minimizar un widget haciendo clic en o maximizarlo haciendo clic en junto al título del widget.
- Para centrarse más en los datos que se muestran en algunos widgets, haga clic en el ícono .
- Para ver los datos en formato XML/JSON que están disponibles en algunos de los widgets, haga clic en .
- Algunos widgets tienen ayuda contextual que se muestra en una ventana emergente. Para acceder a la información de ayuda, haga clic en . En algunas ventanas emergentes de ayuda contextual, puede hacer clic en el vínculo **aquí** para consultar más documentación sobre los datos que se muestran en el widget.

Explorar la página del panel de control

La página **Panel de control** es donde se empieza cuando se accede a la interfaz de usuario de NSX Network Detection and Response.

La página proporciona una descripción general de las campañas activas en la red, los incidentes y amenazas detectados y los eventos de amenazas observados más recientes en su entorno NSX-T Data Center.

La página consta de varios widgets que se pueden administrar mediante la información incluida en [Introducción a la interfaz de usuario de NSX Network Detection and Response](#).

Puede profundizar en los detalles de aspectos individuales de la interfaz y ver información detallada. Parte de esta información detallada se presenta directamente en el widget. Se muestra otra información en las páginas vinculadas de otro lugar de la interfaz de usuario de NSX Network Detection and Response.

Campañas activas en mi red

El widget **Campañas activas en mi red** proporciona una descripción general de las campañas identificadas por la aplicación NSX Network Detection and Response y que actualmente están activas en la red, y muestra las campañas que requieren su acción inmediata de una forma más crítica.

El widget muestra las estadísticas Todas las campañas activas, Campañas abiertas de alto impacto, Campañas de alto impacto en curso y Hosts afectados.

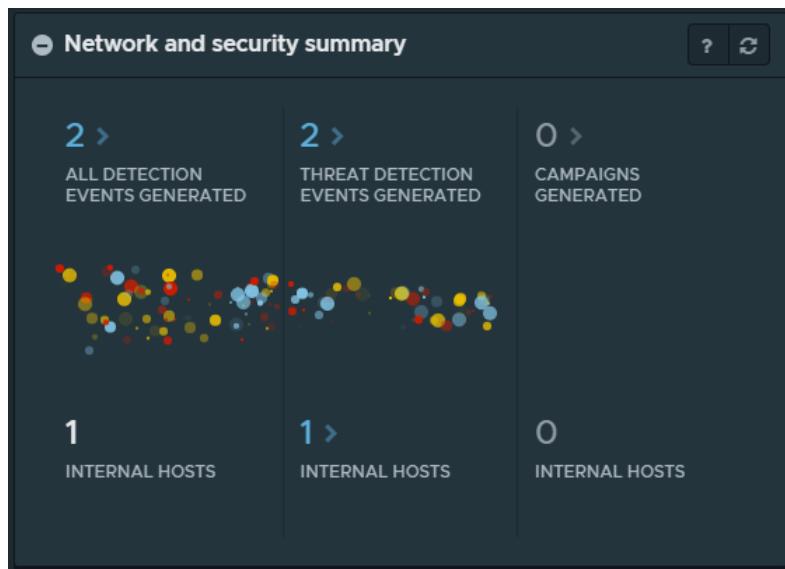
Para ver más detalles sobre estas campañas, haga clic en **Ir a campañas**, en la esquina inferior izquierda del widget, y accederá a la página **Campañas**. Consulte [Administrar la página Campañas](#) para obtener detalles.

Resumen de redes y seguridad

El widget **Resumen de redes y seguridad** muestra cómo NSX Network Detection and Response procesa y analiza los datos de flujo de tráfico de red.

El widget muestra la canalización de procesamiento utilizada para analizar todos los eventos (incluidos los eventos informativos), detectar eventos de amenazas (solo eventos importantes) y generar campañas.

El widget tiene segmentos que indican las diferentes etapas del procesamiento que realiza el sistema en los datos entrantes. Como se muestra en la siguiente imagen, el procesamiento comienza con Todos los eventos de detección generados y continúa hasta llegar a Campañas generadas.



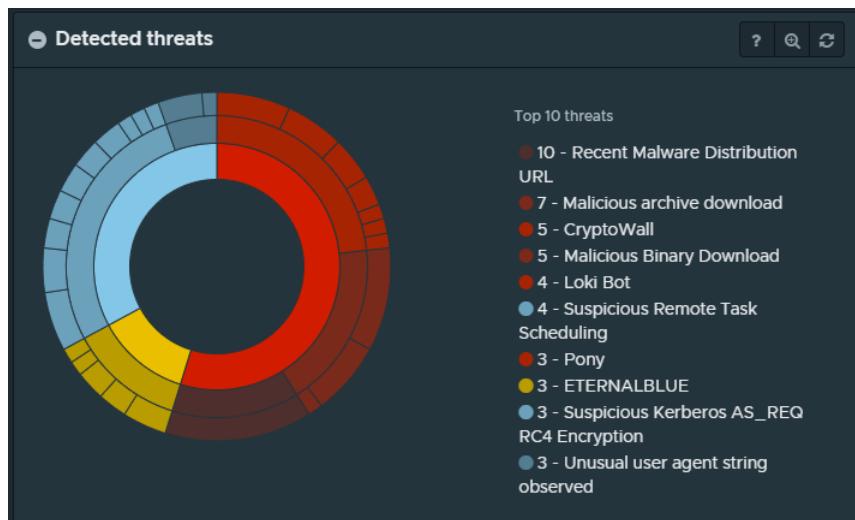
- Al hacer clic en el vínculo de recuento del segmento Todos los eventos de detección generados, se le redirigirá a la página **Eventos**, que estará filtrada para mostrar todos los eventos de detección, incluidos los eventos de detección de información no importantes. Consulte [Trabajar con la página Eventos](#) para obtener detalles.

- Al hacer clic en el vínculo de recuento del segmento Eventos de detección de amenazas generados, se le redirige a la página **Eventos** filtrada para mostrar solo la lista de eventos de detección de amenazas. Al hacer clic en el vínculo de recuento debajo del segmento Eventos de detección de amenazas generados, accederá a la página **Hosts**. Consulte [Trabajar con la página Hosts](#).
- Al hacer clic en el vínculo de recuento del segmento Campañas generadas, se le dirigirá a la página **Campañas**, que mostrará las tarjetas de las campañas detectadas. Consulte [Administrar la página Campañas](#) para obtener detalles.

Amenazas detectadas

El widget **Amenazas detectadas** proporciona una descripción gráfica de los distintos tipos de amenazas que ha detectado la aplicación NSX Network Detection and Response en la red.

La información de la amenaza se muestra en un círculo en capas, similar a la siguiente imagen.



Las divisiones de los círculos representan el número de hosts afectados por los tipos de incidentes mostrados. Al avanzar hacia los círculos externos, se proporciona una granularidad más precisa y una información más específica.

- El anillo más interno muestra los tres tipos diferentes de incidentes.

Tipo de incidente	Descripción
Infecciones	Estos son incidentes que la aplicación NSX Network Detection and Response determinó que son críticos. Estos incidentes tienen una puntuación de impacto de 70 o más y se muestran en color rojo.
Lista de inspección	Estos son incidentes que la aplicación NSX Network Detection and Response determinó como de riesgo medio. Estos incidentes, aunque indican un riesgo potencial, puede que no requieran una atención inmediata. Se mantienen bajo una estrecha inspección en caso de que una nueva evidencia modifique su estado. A estos incidentes se les asigna una puntuación de impacto entre 30 y 69 y se muestran en color amarillo.
Molestias	Se trata de incidentes que se consideran de riesgo bajo o nulo. Por lo general, esto corresponde a una actividad potencialmente no deseada/peligrosa que no necesariamente implica un riesgo o una vulneración en la red supervisada. Estos incidentes tienen una puntuación de impacto inferior a 30 y se muestran en azul.

- El anillo intermedio muestra la clase de amenaza junto con el número de incidentes relevantes para cada tipo de incidente. Las clases de amenazas incluyen servidores de comandos y control, descargas de archivos malintencionados, criptomineros y muchos más.
- El anillo externo representa las familias de amenazas individuales detectadas en la red. Las familias de amenazas incluyen ransomware, archivos binarios malintencionados, etc.

Al señalar el gráfico, el widget muestra el nombre de la amenaza y un recuento de hosts en los que la aplicación NSX Network Detection and Response observó la amenaza.

Al hacer clic en un elemento del gráfico, la vista se acerca y se muestran más detalles sobre el tipo de información seleccionado. Al hacer clic de nuevo en el elemento, se vuelve a alejar la vista.

Si hace clic en un tipo de incidente en el anillo interno, la vista de gráfico amplía y muestra los incidentes coincidentes en el anillo central y externo. Si hace clic en una clase de amenaza en el anillo central, la vista de gráfico se acerca y muestra las familias de amenazas coincidentes. Si hace clic en el anillo externo, la vista de gráfico se acerca y muestra detalles sobre la amenaza seleccionada.

La leyenda en el lado derecho del widget muestra un recuento de las ocurrencias de las amenazas más frecuentes detectadas. Al señalar un elemento de la leyenda, una ventana emergente proporciona más información sobre la clase de amenaza, el número de incidentes y el número de hosts afectados. Al hacer clic en el elemento, se amplía la vista de gráfico del tipo de amenaza seleccionado y se proporciona más información contextual.

Mapa de eventos global

El widget **Mapa de eventos global** proporciona una descripción general visual de las geolocalizaciones de los eventos agregados.

Marca la ubicación aproximada de los otros hosts implicados en el evento detectado por la aplicación NSX Network Detection and Response. El color del marcador representa el impacto del evento. El tamaño del marcador representa el número de hosts afectados.

Los eventos sin ubicación específica se excluyen de este mapa.

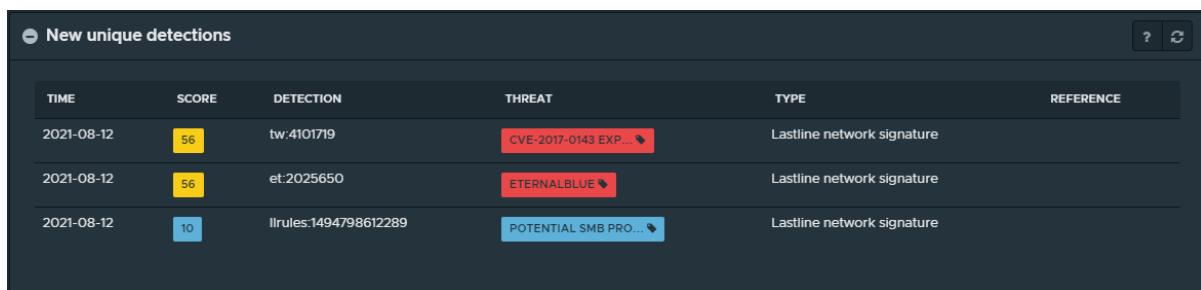
Para obtener más información sobre las amenazas y los hosts representados en esa ubicación en particular, haga clic en un marcador en el mapa.

En la ventana emergente **Detalles de ubicación** que se muestra, puede ver la ubicación aproximada, las amenazas y los hosts de destino del evento seleccionado. Haga clic en el icono  junto a cada entrada para aplicar filtros a la lista que se muestra en la página **Eventos**.

Nuevas detecciones únicas

El widget **Nueva detección única** muestra una lista de eventos que la aplicación NSX Network Detection and Response identificó por primera vez en su red.

La siguiente imagen muestra un ejemplo de la lista.



TIME	SCORE	DETECTION	THREAT	TYPE	REFERENCE
2021-08-12	56	tw:4101719	CVE-2017-0143 EXP...	Lastline network signature	
2021-08-12	56	et:2025650	ETERNALBLUE	Lastline network signature	
2021-08-12	10	llrules:1494798612289	POTENTIAL SMB PRO...	Lastline network signature	

La lista contiene la hora del evento, su puntuación de impacto, la firma de detección (que puede ser una URL con reputación malintencionada o una regla específica), la amenaza, el tipo de evento y una referencia de vínculo permanente al evento asociado.

Cuando se coloca el puntero sobre cualquiera de las filas de la lista, se mostrarán más detalles sobre el evento de detección. Al hacer clic en el nombre de la amenaza, se mostrará una ventana emergente con información sobre el tipo de amenaza, la gravedad y los detalles sobre la amenaza detectada.

Importante Controle e investigue estos eventos, ya que la aplicación NSX Network Detection and Response detectó estas amenazas en su entorno de NSX-T Data Center por primera vez.

Lista de archivos descargados

El widget **Lista de archivos descargados** muestra una lista de archivos distintos y únicos que los hosts de la red detectaron como descargados por la aplicación NSX Network Detection and Response. Este widget solo puede mostrar datos si la aplicación Prevención de malware de NSX está activada.

La siguiente imagen muestra un ejemplo del widget **Lista de archivos descargados** con datos.

Downloaded files list							
Quick search							
MD5	TYPE	SIZE	DOWNLOADS	AV CLASS	MALWARE	SCORE	≡
⊕895006de3c22c2e907...	Executable	740.500 KB	3 ↗	PWD-STEALER	LOKI BOT, PONY	100	
⊕936e73lb8be167a396e...	Executable	480.133 KB	2 ↗	TROJAN	EMOTET	100	
⊕2e61ed247b60ef7fa77c...	Java	470.109 KB	1 ↗	PWD-STEALER, TROJAN	ORAT	100	
⊕c3138c2c7dd16daa812c...	Archive	108.817 KB	2 ↗	TROJAN	EMOTET	100	
⊕2773e3dc59472296cb...	Executable	283.500 KB	2 ↗	RANSOMWARE	JIGSAW	100	
⊕72d2bbafa257441c968...	Executable	12.354 KB	3 ↗	No tags	No tags	0	
⊕69dcca2c07d75aa7ba8...	Executable	19.386 KB	3 ↗	No tags	No tags	0	

El cuadro de texto **Búsqueda rápida** en la esquina superior izquierda de la lista proporciona una capacidad de búsqueda rápida mientras introduce texto. Filtra las filas de la lista y muestra solo aquellas filas de cualquier columna que incluyan texto que coincida con la cadena de consulta que introdujo en el cuadro de texto de búsqueda.

Para personalizar las columnas que se muestran en la lista, haga clic en el **≡** situado en la esquina superior derecha de la lista.

Puede personalizar el número de filas que se mostrarán. El valor predeterminado es 20 entradas. Utilice los iconos **◀** y **▶** para desplazarse por varias páginas.

Cada fila es un resumen de un archivo descargado. Haga clic en el ícono **⊕** o en cualquier lugar de una fila de entrada para acceder a una vista detallada del archivo descargado.

La lista se ordena por puntuación e incluye las siguientes columnas.

Nombre de la columna	Descripción
MD5	El hash MD5 del archivo descargado.
Tipo	El tipo de archivo de alto nivel del archivo descargado. Los tipos admitidos actualmente son: <ul style="list-style-type: none"> ■ Archivo: formatos de archivo como ZIP o RAR ■ Documento: incluye otros tipos de documentos de Office ■ Ejecutable: formatos de aplicación binarios, como ejecutable portátil de Windows. ■ Java: aplicación Java o applet ■ Medios: archivo Flash de Macromedia (Adobe) ■ Otro: otro formato de archivo reconocido ■ PDF: archivos con formato de documento portátil ■ Script: un script ejecutable, como JavaScript, Python y otros. ■ Desconocido: tipo de archivo desconocido
Tamaño	Tamaño en bytes del archivo descargado.
Descargas	Número de veces que los hosts de la red descargaron el archivo. El número mostrado y ⊕ proporcionan un vínculo a la página de descargas detallada. El vínculo pasa un filtro UUID de Analista que restringe la vista a las descargas de este archivo específico.

Nombre de la columna	Descripción
Clase AV	Etiqueta que define la clase de antivirus del archivo descargado. Si la etiqueta tiene un icono  , puede hacer clic en ese icono para obtener una descripción en una ventana emergente.
Malware	Una etiqueta que define el tipo de malware del archivo descargado. Si la etiqueta tiene un icono  , puede hacer clic en ese icono para obtener una descripción en una ventana emergente.
Puntuación	<p>La puntuación asignada al archivo descargado por el análisis indica el nivel crítico de la amenaza detectada y oscila entre 0 y 100:</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas que se encuentran entre 1 y 29 se consideran benignas. <p>Para obtener más información sobre el núcleo de la malintencionaldad y la estimación de riesgo, consulte Informe de análisis: pestaña Descripción general.</p> <p>Si aparece el icono , significa que el artefacto se bloqueó. La lista se ordena en orden descendente (las amenazas más críticas en la parte superior). Haga clic en  para ordenar la lista en orden creciente (las amenazas menos críticas en la parte superior), y haga clic en  para volver al orden predeterminado.</p>

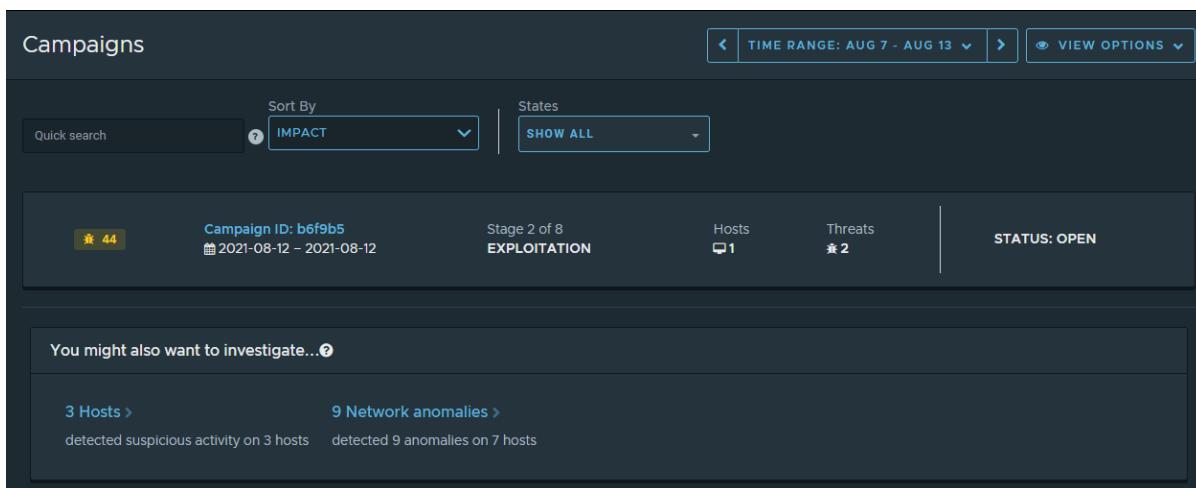
Administrar la página Campañas

La página **Campañas** proporciona una interfaz para supervisar las campañas que la aplicación NSX Network Detection and Response detectó en la red.

La página consta de varios widgets que se pueden administrar mediante la información incluida en [Introducción a la interfaz de usuario de NSX Network Detection and Response](#).

Si no se detectan campañas, se mostrará el mensaje Ninguna campaña encontrada.

Si se detectan campañas, la página mostrará las tarjetas de campaña correspondientes. La siguiente imagen muestra una página **Campañas** de ejemplo con una tarjeta para la campaña detectada durante el intervalo de tiempo seleccionado. Consulte [Trabajar con tarjetas de campaña](#).



The screenshot shows the 'Campaigns' page with the following details:

- Header:** Campaigns, TIME RANGE: AUG 7 - AUG 13, VIEW OPTIONS.
- Search and Filter:** Quick search, Sort By (IMPACT selected), States (SHOW ALL).
- Campaign Card:**
 - Header:** Campaign ID: b6f9b5, Date: 2021-08-12 – 2021-08-12, Stage: Stage 2 of 8 EXPLOITATION, Status: STATUS: OPEN.
 - Metrics:** Hosts: 1, Threats: 2.
 - Callout:** You might also want to investigate... (with a question mark icon).
 - Details:** 3 Hosts > (detected suspicious activity on 3 hosts) and 9 Network anomalies > (detected 9 anomalies on 7 hosts).

En la parte inferior de la página, se muestra el widget **Es posible que también desee investigar**. Consulte [Acerca del widget Investigar](#) para obtener detalles.

Trabajar con tarjetas de campaña

La página **Campañas** muestra tarjetas de campaña para cualquier campaña detectada. Una tarjeta de campaña muestra la puntuación calculada de la amenaza, el nombre de la campaña (identificador de campaña), la etapa de ataque más reciente que detectó la aplicación NSX Network Detection and Response, el número de hosts afectados, el número de amenazas diferentes y el estado de la campaña.

Administrar tarjetas de campaña

Para ordenar las tarjetas de campaña, haga clic en el menú desplegable **Ordenar por** y seleccione en la lista de criterios: **Impacto** (valor predeterminado), **Etapa**, **Hosts**, **Amenazas**, **Primera** o **Última actividad**.

Para seleccionar las tarjetas de campaña que desea que se muestren, haga clic en el menú desplegable **Estados** y seleccione entre **Mostrar todo** (valor predeterminado), **Abierto**, **En curso**, **Finalizado** o **Actualizado**. Puede seleccionar más de una opción. Para borrar una selección, vuelva a hacer clic en la opción.

Para ver todos los detalles disponibles sobre una campaña, haga clic en el vínculo **ID de campaña** y se mostrarán los detalles de la campaña. Consulte [Página Detalles de la campaña](#).

Haga clic en cualquier lugar de una tarjeta de campaña y la barra lateral **Resumen de campaña** aparecerá en el lado derecho.

Información sobre la barra lateral de resumen de campañas

La barra lateral **Resumen de campaña** se muestra en el lado derecho de la página **Campañas** al hacer clic en cualquier lugar de una tarjeta de campaña.

A continuación se describe lo que se ve en la barra lateral resumen **Campaña**.

Sección principal

En la parte superior de la barra lateral se encuentran los siguientes elementos:

- La puntuación de la amenaza calculada y el nombre/ID de la campaña (en formato hash largo) se muestran en la parte superior.
- Al hacer clic en el botón **Ver detalles**, podrá acceder a la página **Detalles de la campaña**. Consulte [Página Detalles de la campaña](#) para obtener más información.
- Se muestra el número de hosts afectados por la campaña.
- Se muestra el número de tipos de amenazas involucrados en la campaña.

Acciones

La siguiente sección del panel incluye la siguiente información.

- **Nombre de la campaña/ID de campaña:** puede hacer clic en el icono de lápiz y, opcionalmente, editar el nombre o el identificador de la campaña.
- **Estado:** seleccione el estado de la selección de la campaña en el menú desplegable. Seleccione entre **Abrir**, **En curso**, **Actualizado** o **Finalizado**.
- Primera detección y Última detección: muestra un gráfico lineal con la marca de tiempo de la primera y última detección de la evidencia. La duración se muestra después del gráfico.

Etapas de ataque vistas

La sección **Etapas de ataque vistas** muestra las etapas de ataque, resaltando las etapas actuales de ataques de campaña. Apunte a una actividad resaltada (por ejemplo, **Explotación**) para ver una ventana emergente con más información sobre la etapa. Consulte [Acerca de las etapas de ataque](#) para obtener información detallada.

Host afectado

La sección **Hosts afectados** muestra los hosts que participan en la campaña seleccionada. Para ver la página **Perfil de host**, haga clic en el vínculo dirección IP. Consulte [Página de perfil de host](#).

Para ver los detalles de los hosts en la pestaña **Hosts**, haga clic en **Ver hosts**. Consulte [Detalles de la campaña: pestaña Hosts](#) para obtener más información.

Amenazas

La sección **Amenazas** muestra las amenazas actuales detectadas en la campaña seleccionada. El código de color indica la gravedad de la amenaza: rojo para gravedad alta, amarillo para media y azul para baja.

Para ver información detallada sobre la campaña en la pestaña **Cronología de la campaña**, haga clic en **Ver amenazas**. Consulte [Detalles de la campaña: pestaña Escala de tiempo](#) para obtener más información.

Acerca del widget Investigar

El widget **Investigar** muestra el mensaje **Es posible que también desee investigar...** y una lista de hechos y destinos personalizados preparados por la aplicación NSX Network Detection and Response en función de la actividad de su red.

Para explorar información de seguridad interesante, siga los vínculos proporcionados en la lista. El widget muestra cualquiera de los siguientes datos en función de lo que haya detectado la aplicación NSX Network Detection and Response.

Nombre de detalle	Descripción
Hosts	Informa sobre actividad sospechosa en los hosts de la red. Haga clic en el vínculo para ir a la página Hosts .
Descargas de archivos sospechosos	Informa sobre descargas de archivos sospechosos. Haga clic en el vínculo para ir a la pestaña Todos de la página Archivos descargados .
Anomalías de red	Notifica eventos INFO que podrían necesitar investigación. Haga clic en el vínculo para ir a la página Eventos .

Página Detalles de la campaña

La página **Detalles de la campaña** de la interfaz de usuario de NSX Network Detection and Response muestra todos los detalles disponibles para la campaña seleccionada actualmente en la página **Campañas**.

Para acceder a esta página, haga clic en el ID de una campaña en la página **Campañas**.

Esta página se divide en varias pestañas, como se muestra en la siguiente imagen.

The screenshot displays the 'Overview' tab of the 'Campaign Details' page. At the top, it shows the Campaign ID: e7ff58, the date range 2021-08-16 – 2021-08-26, and key metrics: Latest stage: Exploitation, Affected hosts: 1, Threats: 2, and State: Open. Below this, the 'Threats and hosts' section shows 2 threats (CVE-2017-0143 and ETERNALBLUE) and 1 host affected. The 'Attack stages' section lists the progression from delivery to exfiltration. The 'Campaign blueprint' section contains a network diagram showing the flow of the exploit between hosts.

- **Descripción general:** proporciona un resumen y un modelo gráfico de la campaña que ha generado la aplicación NSX Network Detection and Response.
- **Hosts:** proporciona una lista de los hosts afectados por la campaña.
- **Escala de tiempo:** muestra los eventos incluidos en la campaña en orden cronológico.
- **Historial:** proporciona un historial textual de la campaña.

- **Prueba:** muestra una lista de la evidencia detectada para la campaña seleccionada actualmente.

En la parte superior de la página de detalles de la campaña se muestran los datos de la tarjeta de campaña seleccionada. Muestra la puntuación de la amenaza calculada, el nombre de la campaña (identificador de campaña), la etapa de ataque más reciente, el número de hosts afectados, el número de amenazas diferentes y el estado de la campaña.

Para volver a la página **Campañas**, haga clic en el icono en la esquina superior izquierda de la página, junto a la puntuación de la amenaza de la campaña y el identificador de campaña.

Detalles de la campaña: pestaña Descripción general

La pestaña **Descripción general** de la página **Detalles de la campaña** muestra un resumen de la campaña y un gráfico Blueprint interactivo.

La siguiente información describe las tres secciones de esta pestaña.

Amenazas y hosts de campaña

La sección **Amenazas y hosts** muestra los widgets **Amenazas y Hosts**.

El widget **Amenazas** muestra las amenazas actuales que detectó la aplicación NSX Network Detection and Response en la campaña seleccionada. La gravedad de la amenaza se indica con el código de color: rojo para alto, amarillo para medio y azul para bajo. Coloque el puntero sobre el nombre de las amenazas enumeradas y aparecerá una ventana emergente con las direcciones IP de los hosts afectados. Haga clic en **Ver detalles de amenazas** y la pestaña **Cronología** mostrará información detallada sobre la campaña.

El widget **Hosts** muestra los hosts afectados por la campaña seleccionada. La gravedad de la amenaza se indica con el código de color: rojo para alto, amarillo para medio y azul para bajo.

Apunte a la dirección IP de un host afectado y una ventana emergente mostrará los nombres de las amenazas que afectan al host. Haga clic en **Ver detalles de hosts** y la pestaña **Hosts** mostrará información detallada sobre los hosts.

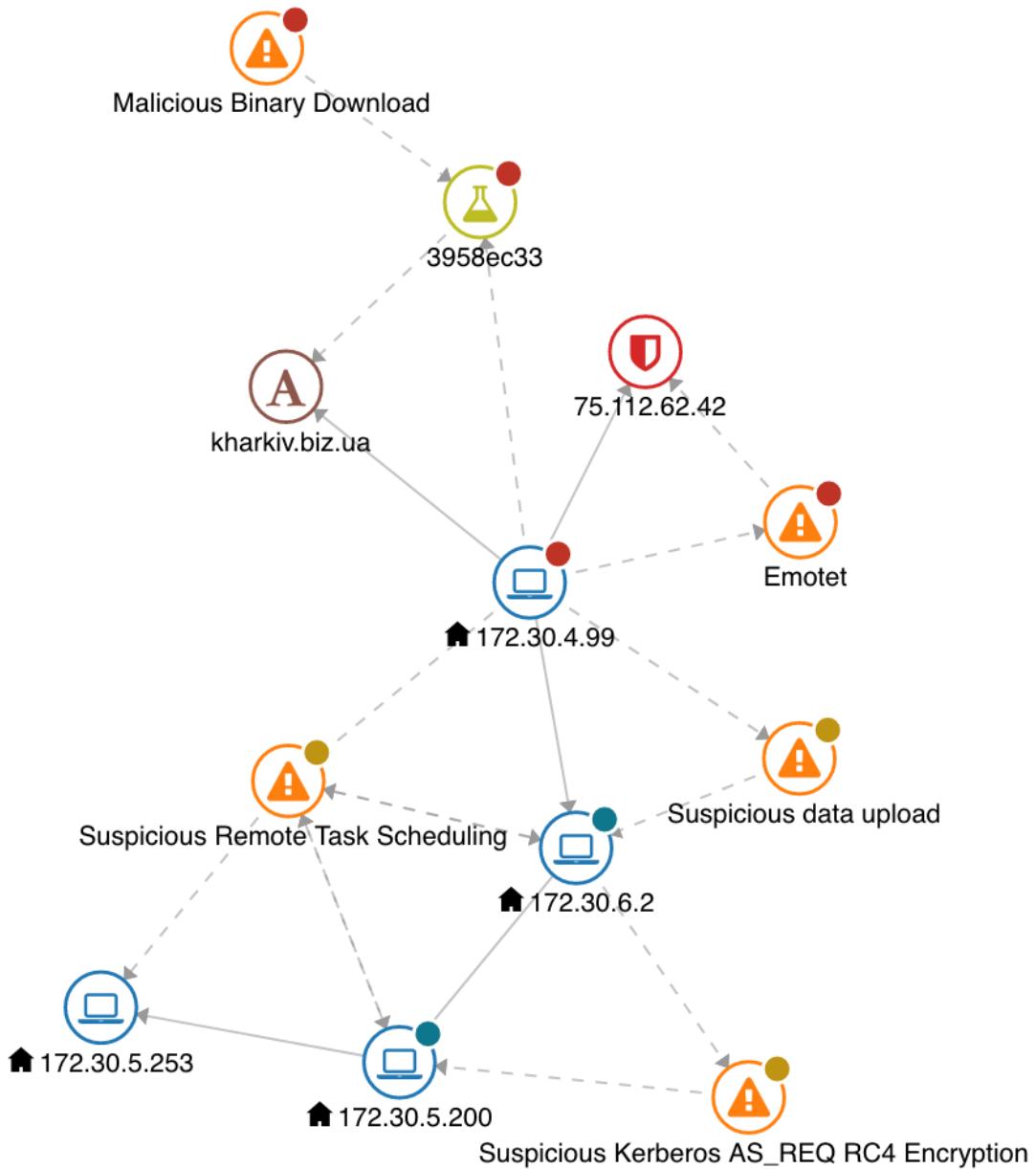
Etapas de ataques de campaña

El widget **Etapas de ataque** muestra las etapas de ataque y resalta las etapas actuales de los ataques de campaña. Coloque el puntero sobre una actividad resaltada y aparecerá una ventana emergente con más información sobre la etapa de ataque. Consulte [Propiedades de la campaña](#) para obtener más información sobre las etapas de ataque.

Blueprint de campaña

El widget **Blueprint de campaña** proporciona una representación gráfica interactiva de la campaña. Muestra los hosts involucrados en la campaña (tanto internos como externos a la red), las amenazas que los afectaron e información adicional que completa la descripción de la campaña.

A continuación se muestra un ejemplo de un gráfico de blueprint.



Este gráfico de blueprint muestra las siguientes actividades.

- Se descarga un archivo binario malintencionado en el nodo de host con la etiqueta 172.30.4.99. Esta actividad puede corresponder a un usuario de ese host que abre un correo electrónico (por ejemplo, visitar una URL o abrir un archivo adjunto incluido en ese correo electrónico).
- El nodo de host con la etiqueta 172.30.4.99 se conecta al nodo de nombre de host con la etiqueta kharkiv.biz.ua. El informe de análisis 3958ec33 muestra que se realizó una descarga desde la URL <http://kharkiv.biz.ua/hPpD/>. El informe de análisis también muestra que lo que se descarga es un archivo ejecutable de PE, 32 bits, Intel i386.

- El nodo de host con la etiqueta 172.30.4.99 está conectado a Emotet command and control. El servidor es la entrada bloqueada 75.112.62.42.
- El nodo de host con la etiqueta 172.30.4.99 está conectado al nodo de host con la etiqueta 172.30.6.2 con una carga de datos sospechosa y a los nodos de host con las etiquetas 172.30.5.200 y 172.30.5.200 con una programación de tareas remotas sospechosa, todas las actividades asociadas con el movimiento lateral.
- El nodo de host con la etiqueta 172.30.6.2 está conectado al nodo de host con la etiqueta 172.30.5.200 con un cifrado de Kerberos sospechoso, una actividad que se corresponde con la exfiltración de datos.

Clave de nodo

Los siguientes tipos de nodo pueden aparecer en el gráfico Blueprint.

Ico	no	Tipo de nodo	Descripción
	Informe de análisis		<p>Este tipo de nodo representa los resultados de la detonación de una muestra (archivo o URL) en el espacio aislado NSX Network Detection and Response.</p> <ul style="list-style-type: none"> ■ Los nodos del informe de análisis se etiquetan con una versión abreviada del UUID de la tarea de análisis correspondiente. ■ El rango de puntuación de la ejecución del análisis se expresa mediante la etiqueta codificada por colores en la parte superior derecha del nodo.
	Archivo descargado		<p>Este tipo de nodo representa un archivo que se descargó en la red.</p> <ul style="list-style-type: none"> ■ Los nodos de archivos descargados se etiquetan con una versión abreviada del hash SHA1 del archivo correspondiente.
	Host		<p>Este tipo de nodo representa un dispositivo de red.</p> <ul style="list-style-type: none"> ■ Los nodos del host se etiquetan con la dirección IP del host correspondiente. ■ El nodo de host indica si un host es interno o externo. Los hosts internos muestran el icono junto a su dirección IP. La determinación de si un host es interno se basa en la configuración de rangos de IP privadas. ■ El impacto máximo de los incidentes que afectan al host correspondiente se expresa mediante la etiqueta codificada por colores en la parte superior derecha del nodo.
	Información		<p>Este tipo de nodo representa una detección de una actividad de nivel de información. Este nodo solo aparece en el gráfico de Blueprint Análisis de red.</p> <ul style="list-style-type: none"> ■ Se crea un evento de información en presencia de actividades o comportamientos que no son necesariamente malintencionados, sino que proporcionan información adicional y útil. ■ El impacto máximo de los eventos detectados para la amenaza correspondiente se expresa mediante la etiqueta codificada por colores en la parte superior derecha del nodo.
	Amenaza		<p>Este tipo de nodo representa una detección.</p> <ul style="list-style-type: none"> ■ Los nodos de amenaza se etiquetan con el nombre de la amenaza asociado al evento detectado. ■ El impacto máximo de los eventos detectados para la amenaza correspondiente se expresa mediante la etiqueta codificada por colores en la parte superior derecha del nodo.

Acerca de las instancias de Edge

Las líneas que conectan los nodos de se denominan instancias de Edge.

Un nodo de host está conectado a nodos de informes de amenazas o análisis con una línea de puntos para indicar que el host correspondiente al nodo de host ha estado expuesto a la amenaza representada por el nodo de informe de amenazas o análisis.

Otras conexiones se representan con una línea continua para expresar que alguna actividad (por ejemplo, una conexión de red, una búsqueda de DNS o una solicitud web) pone en relación las entidades correspondientes a dos nodos.

Interacción de blueprint

El gráfico de Blueprint es interactivo: admite la selección de elementos, mueve nodos y acerca y reduce el zoom.

Para seleccionar el nodo y las instancias de Edge, haga clic en ellos. Encontrará información adicional sobre el elemento seleccionado en la barra lateral.

Al pasar el mouse sobre un nodo, se coloreará la conexión de las instancias de Edge y se resaltarán la interacción de ese nodo.

Los nodos individuales se pueden arrastrar a nuevas posiciones en el gráfico. Todo el gráfico puede desplazarse, lo que cambia de forma efectiva el punto de vista.

Para acercar y alejar el gráfico, desplácese por la rueda del mouse. Se muestran más detalles en niveles de zoom superiores. En particular, la etiqueta utilizada con varios tipos de nodos para transmitir la información de impacto se enriquece con la puntuación de impacto real.

Barra lateral Campaña

La barra lateral **Campaña** se utiliza para mostrar información relativa a uno o varios elementos del gráfico de proyecto. Está minimizada de forma predeterminada.

- Haga clic en el icono  para ver información del nodo o de la instancia de Edge.
- Haga clic en el icono  para ver herramientas de terceros.

Para minimizar la barra lateral, haga clic en el icono .

Información de nodo o Edge

La pestaña información de nodo/instancia de Edge proporciona información adicional sobre un nodo o una instancia de Edge seleccionados en el gráfico de Blueprint. Para seleccionar un nodo, haga clic en su ícono en el gráfico.

Tipo de nodo	Información
Informe de análisis	<p>Información adicional sobre un informe de análisis.</p> <p>Detalles del informe:</p> <ul style="list-style-type: none"> ■ Informes de análisis: muestra el UUID y la puntuación de la tarea. Haga clic en el icono  para ver el informe de análisis en una nueva pestaña del navegador. ■ MD5: valor hash de archivo. ■ SHA1: valor hash de archivo. ■ Tamaño : tamaño de archivo en bytes. ■ Categoría: la categoría a la que pertenece el archivo analizado. ■ Tipo: información más detallada sobre el archivo. <p>Detalles de los avistamientos de la muestra analizada:</p> <ul style="list-style-type: none"> ■ Número de descargas: número de veces que se ha observado que se ha descargado el archivo analizado. ■ Hosts: dirección IP de los hosts que descargaron el archivo analizado. ■ URL: la dirección URL completa del archivo descargado.
Archivo descargado	<p>Información adicional sobre un archivo descargado</p> <p>Detalles del archivo:</p> <ul style="list-style-type: none"> ■ MD5: valor hash de archivo. ■ SHA1: valor hash de archivo. ■ Tamaño : tamaño de archivo en bytes. ■ Categoría: la categoría a la que pertenece el archivo analizado. ■ Tipo: información más detallada sobre el archivo. <p>Detalles de avistamientos:</p> <ul style="list-style-type: none"> ■ Número de descargas: número de veces que se ha observado que se ha descargado el archivo analizado. ■ Hosts de descarga: dirección IP de los hosts que descargaron el archivo analizado. ■ URL: la dirección URL completa del archivo descargado. ■ Informes: muestra el estado del informe, el UUID de la tarea y la puntuación. Haga clic en el icono  para ver el informe de análisis en una nueva pestaña del navegador.
Host	<p>Información adicional sobre un host.</p> <p>Detalles de nivel de host:</p> <ul style="list-style-type: none"> ■ Dirección IP: ícono de asignación geográfica o red local. ■ Nombres de host: nombre de dominio del host. ■ Servicios: todos los servicios detectados en el host. <p>Incidentes relacionados con el host:</p> <ul style="list-style-type: none"> ■ Número de incidentes: recuento de todos los incidentes. ■ Impacto máximo: indica el impacto máximo de todos los incidentes. ■ Amenazas: una lista de los eventos detectados. <p>Una nota indica si el host es interno o externo a la red supervisada.</p>

Tipo de nodo	Información
Solicitud HTTP	<p>Información adicional sobre una solicitud HTTP.</p> <p>Detalles de URL:</p> <ul style="list-style-type: none"> ■ Descargar URL: las URL observadas en la solicitud HTTP. ■ Descargar direcciones IP: las direcciones IP resueltas para la solicitud HTTP. Haga clic en el icono  para ver la dirección IP de la solicitud en Análisis de red. <p>Detalles de la solicitud</p> <ul style="list-style-type: none"> ■ Número de solicitudes: número de veces que se observó la solicitud HTTP. ■ Hosts: dirección IP de los hosts que emiten la solicitud HTTP. ■ Referencias: los valores del encabezado "referer" observados en la solicitud HTTP. ■ Agentes de usuario: valores de usuario-agente observados en la solicitud HTTP.
Amenaza	<p>Información adicional sobre una amenaza</p> <p>Detalles de la amenaza:</p> <ul style="list-style-type: none"> ■ Clase de amenaza: el nombre de la clase de amenaza detectada. Por ejemplo, comando y control. ■ Amenaza: el nombre de la amenaza detectada. Por ejemplo, Loki Bot. ■ Gravedad: la puntuación de amenaza calculada. ■ Información: una descripción de la amenaza detectada

Al hacer clic en una instancia de Edge, se muestra la siguiente información sobre la conexión:

- Nodo de origen: el origen de la conexión. Puede ser un nombre de nodo, una dirección IP, un nombre de dominio, etc.
- Nodo de destino: el destino de la conexión. Puede ser un nombre de nodo, una dirección IP, un nombre de dominio, etc.

En Nodo de origen y Nodo de destino se muestran el origen o el destino real de la conexión. Haga clic en el icono  para expandir el origen o el destino.

Herramientas de terceros

La pestaña herramientas de terceros se vincula a herramientas externas que pueden proporcionar información adicional sobre una entidad seleccionada en el gráfico. Actualmente, las herramientas compatibles son [DomainTools](#) y [VirusTotal](#).

Se admiten las siguientes búsquedas:

- Al seleccionar un nodo de host, puede buscar la dirección IP correspondiente en DomainTools y VirusTotal.
- Al seleccionar un nodo de nombre de host, puede buscar el nombre de dominio correspondiente en DomainTools y VirusTotal.
- Si selecciona un nodo de archivo descargado, podrá buscar el hash correspondiente en VirusTotal.
- Al seleccionar un nodo de solicitud HTTP, puede buscar el nombre de host de la solicitud en DomainTools y VirusTotal.

Detalles de la campaña: pestaña Hosts

La pestaña **Hosts** de la página **Detalles de la campaña** muestra una lista de los hosts a los que afectó la campaña.

Las columnas proporcionan la siguiente información.

Nombre de la columna	Descripción
Hosts	La dirección IP del host afectado por la campaña. Haga clic en el vínculo de la dirección IP y se mostrará la barra lateral Resumen del host en el lado derecho.
Amenazas	Una lista de todas las amenazas que detectó NSX Network Detection and Response en el host.
Etapas de ataque	Las etapas de ataque observadas durante la actividad de amenaza que afecta a ese host específico.
Última actividad	La marca de tiempo de la última vez que se detectó una actividad para ese host.

Detalles de la campaña: pestaña Escala de tiempo

En la pestaña **Cronología** de la campaña en la página **detalles de Detalles de campaña**, las amenazas detectadas por NSX Network Detection and Response se representarán mediante tarjetas de amenazas.

Una tarjeta de amenaza muestra el host que está conectado a esta amenaza, la puntuación de la amenaza calculada, el nombre y la clase de la amenaza, el resultado de detección (si está disponible), el estado de la amenaza y otras acciones. Para ver su evidencia relacionada, expanda la tarjeta haciendo clic en el icono **>**, como se muestra en la siguiente imagen. Haga clic en el icono **▼** para contraer la sección Evidencia.

The screenshot shows the 'Timeline' tab of the campaign details page. At the top, it displays 'Campaign ID: b6f9b5' and the date range '2021-08-12 – 2021-08-12'. It also shows 'Latest stage: Exploitation', 'Affected hosts: 1', 'Threats: 2', and a dropdown for 'State: Open'. Below this, there are two threat cards:

- ETERNALBLUE**: Occurred on Aug 12, 12:48:57 - Aug 12, 12:48:57. It has a confidence of 75 and a signature type. Evidence summary: 1 type: Signature. Supporting data: 1 detection events. Actions: OPEN, NEXT STEPS.
- CVE-2017-0143 EXPLOIT**: Occurred on Aug 12, 12:48:50 - Aug 12, 12:48:50. It has a confidence of 75 and a signature type. Evidence summary: 1 type: Signature. Supporting data: 1 detection events. Actions: OPEN, NEXT STEPS.

Ordene las tarjetas de amenazas con el menú desplegable **Ordenar por**. Seleccione entre **Más reciente** (valor predeterminado), **Anterior**, **Mayor impacto** y **Menor impacto**.

El cuadro de texto **Buscar amenazas** sobre la lista permite hacer una búsqueda rápida mientras introduce la búsqueda. Filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier campo, que coincida con la cadena de consulta. Su consulta se compara con los valores de las siguientes categorías: impacto, dirección IP, amenaza/malware, fase de la última campaña, visto por primera vez, evidencia y otros hosts, y, para los mensajes de correo, información del mensaje.

Para filtrar las tarjetas de amenazas mostradas por estado de amenaza, use el botón de alternancia **Mostrar amenazas cerradas**. El valor predeterminado es mostrar todas las amenazas.

Tarjetas de amenazas

Las tarjetas de amenazas muestran todas las amenazas asociadas con la campaña seleccionada y sus niveles de amenaza correspondientes.

Cada tarjeta muestra el impacto calculado de la amenaza, el nombre de la amenaza, la clase de amenaza y, si está disponible, el resultado de detección. También muestra el estado de la amenaza: **OPEN** o **CLOSED**.

Puede hacer clic en **Pasos siguientes** y seleccionar una acción en el menú desplegable.

Seleccione **Cerrar** para cerrar la amenaza, **Abrir** para volver a abrir una amenaza cerrada o **Administrar alerta** para crear una regla de administración de alertas a partir de la amenaza.

La sección **Resumen de evidencia** contiene una descripción general de la evidencia y otros datos detectados para la amenaza. Haga clic en el ícono ▾ (o casi en cualquier otro lugar de la tarjeta) para expandir la sección Detalles de la evidencia.

Detalles de la evidencia

La columna **Evidencia** muestra las descargas de archivos, las firmas y otras categorías junto con una marca de tiempo de cuándo se vio la evidencia.

La columna **Interacciones de red e IoC de red** muestra la dirección IP o el nombre de dominio de los hosts externos. Haga clic en el vínculo dirección IP para expandir la barra lateral **Interacción de red**.

La columna **Datos de soporte** proporciona un vínculo a los eventos detectados, un vínculo a los datos capturados y un vínculo a los detalles de la amenaza.

Detalles de la campaña: pestaña Historial

La pestaña **Historial** de la página **Detalles de campaña** de la interfaz de usuario de NSX Network Detection and Response muestra un historial textual descriptivo de cómo se creó la campaña.

Cada entrada proporciona un Aviso y una Descripción de las fases de campaña registradas, junto con la marca de tiempo de aviso.

Detalles de la campaña: pestaña Evidencia

La pestaña **Evidencia** de la página **Detalles de la campaña** de la interfaz de usuario de NSX Network Detection and Response muestra una lista de la evidencia detectada para la campaña seleccionada actualmente.

Cada fila es un resumen de la evidencia de la campaña. Haga clic en  (o en cualquier lugar de una fila de entrada) para expandir la fila y ver la información de la evidencia de firma.

La lista de evidencias incluye las siguientes columnas.

Columnas de evidencia	Descripción
Dirección IP	La dirección IP del host que es el origen de la amenaza.
Primera detección	Marca de tiempo que muestra la hora de inicio de la campaña.
Última detección	Marca de tiempo que muestra la actividad más reciente de la campaña.
Amenaza	Nombre del riesgo de seguridad detectado.
Clase de amenaza	Nombre de la clase de riesgo de seguridad detectada.
Impacto	<p>El valor del impacto indica el nivel crítico de la amenaza detectada y oscila entre 1 y 100:</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas entre 1 y 29 se consideran benignas. <p>Si aparece el  [ícono de bloqueo], significa que el artefacto se bloqueó.</p>
Evidencia	El valor derivado de la evidencia de la campaña. Consulte Acerca de la evidencia para obtener detalles.
Asunto	Información adicional de la campaña. Puede ser una dirección IP, un código de respuesta HTTP o algún otro dato.
Referencia	Haga clic en el vínculo para acceder a la página Detalles del evento de red . El enlace se abre en una nueva pestaña del navegador. Consulte Página de perfil del evento para obtener detalles.
Identificador de incidente	Vínculo permanente a un incidente correlacionado. El enlace se abrirá en una nueva pestaña del navegador. Consulte Administrar la página Incidentes .

Haga clic en el  para cambiar las columnas que desea mostrar. El valor predeterminado es mostrar todas las columnas disponibles.

Al hacer clic en  (o en cualquier lugar de una fila de evidencia), se mostrará la siguiente información.

Nombre de la información	Descripción
Amenaza	Nombre del riesgo de seguridad detectado.
Clase de amenaza	Nombre de la clase de riesgo de seguridad detectada.
Impacto	La puntuación de impacto de la campaña.
Detector	Si aparece, mostrará el módulo de NSX Network Detection and Response que identificó la amenaza. Haga clic en el vínculo para ver la ventana emergente Detector .
Ver detección de red	Si aparece, mostrará el módulo de NSX Network Detection and Response que identificó la amenaza. Haga clic en el vínculo para ver la ventana emergente Detector.
Ver incidente	Haga clic en el vínculo para acceder a la página Detalles del evento de red. El enlace se abre en una nueva pestaña del navegador. Consulte Página de perfil del evento .
Primera detección	Marca de tiempo que muestra la hora de inicio de la campaña.

Nombre de la información	Descripción
Última detección	Marca de tiempo que muestra la actividad más reciente de la campaña.
Gravedad	Estimación del nivel de gravedad de la amenaza detectada. Por ejemplo, una conexión a un comando y un servidor de control se suele considerar una gravedad alta, ya que la conexión podría resultar dañada.
Confianza	Indica la probabilidad de que la amenaza individual detectada sea malintencionada. Dado que el sistema utiliza heurísticas avanzadas para detectar amenazas desconocidas, en algunos casos, la amenaza detectada puede tener un valor de confianza menor si el volumen de información disponible para esa amenaza específica es limitado.

Propiedades de la campaña

Una campaña detectada por la aplicación NSX Network Detection and Response se caracteriza por varias propiedades.

A continuación se detallan las propiedades de la campaña y sus definiciones.

Nombre de propiedad	Descripción
Nombre	Un identificador de campaña que identifica de forma exclusiva la campaña.
Hosts	Los hosts que se ven afectados por la campaña.
Amenaza	Las amenazas detectadas de la campaña.
Etapas de ataque	Las fases del ciclo de vida del almacén correspondientes a las actividades detectadas. Consulte Acerca de las etapas de ataque para obtener detalles.
Duración	El intervalo de tiempo durante el cual se han observado las actividades asociadas con una campaña.

Acerca de las etapas de ataque

Las etapas de ataque son las fases del ciclo de vida de un adversario que corresponden a las actividades detectadas por la aplicación NSX Network Detection and Response.

Un modelo de adversario describe las acciones que puede realizar un adversario para comprometer y operar dentro de una red empresarial. La aplicación NSX Network Detection and Response utiliza el modelo [Tácticas, técnicas y conocimientos comunes de adversario](#) (ATT&CK™) de MITRE para describir los comportamientos de estos. En este modelo, las técnicas que podría utilizar un adversario se agrupan en una serie de categorías tácticas, que corresponden a diferentes etapas del ciclo de vida del ataque.

En el sistema, la actividad asociada con cada evento detectado puede asociarse a una etapa de ataque específica y podría proporcionar una indicación del progreso de la campaña a lo largo de su ciclo de vida. (Es posible que las actividades detectadas en diferentes fases de ataque no estén asociadas a una etapa de ataque específica). Actualmente, se utilizan las siguientes etapas de ataque.

Nombre de la etapa de ataque	Descripción
Distribución	La etapa en la que los atacantes envían la carga útil al destino. Entre los mecanismos de distribución más comunes se encuentran las vulnerabilidades remotas, las páginas web de descargas drive-by y las unidades USB u otras unidades extraíbles malintencionadas.
Explotación	La etapa en la que se implementa la carga útil del atacante en la red de destino. En consecuencia, uno o varios dispositivos de la red de destino están comprometidos y bajo el control del atacante.
Comando y control	La etapa en la que los atacantes se comunican con los sistemas que controlan dentro de la red de destino, lo que permite obtener acceso remoto "práctico al teclado" a estos sistemas.
Acceso de credenciales	La etapa en la que los atacantes obtienen acceso o control sobre las credenciales de sistema, dominio o servicio utilizadas en el entorno de destino. Por lo general, los atacantes intentan obtener credenciales legítimas de las cuentas de los usuarios y administradores para suplantarlos o crear nuevas cuentas.
Detección	La etapa en la que los atacantes intentan encontrar más información sobre el entorno de destino. Los atacantes suelen intentar identificar dispositivos adicionales en la red que puedan utilizar para sus objetivos.
Movimiento lateral	La etapa en la que los atacantes pasan por la red de destino al obtener acceso y control sobre los sistemas remotos.
Recopilación	La etapa en la que los atacantes identifican y recopilan información de una red de destino antes de la exfiltración.
Exfiltración	La etapa en la que los atacantes eliminan archivos e información de una red de destino.

Acerca de las reglas de correlación

En general, los incidentes se agrupan en una campaña cuando hay evidencia que indica que las actividades malintencionadas o los ataques correspondientes están relacionados.

Dado que estas reglas de correlación se ejecutan en el servicio de nube NSX Advanced Threat Prevention, pueden mejorarse o extenderse independientemente de los ciclos de versión de NSX-T. Además, la lista de reglas de correlación o el comportamiento específico de una regla pueden cambiar con el tiempo.

Las siguientes son las reglas de correlación admitidas actualmente.

Evento de anomalía

Esta regla correlaciona los eventos de detección de la función Tráfico sospechoso de NSX con eventos de tipo infección de impacto más alto. Por ejemplo, un evento de anomalía de la función Tráfico sospechoso de NSX coincide con un evento de red de alto impacto para los mismos hosts.

Exfiltración

Esta regla correlaciona los eventos de exfiltración que van precedidos por eventos de tipo infección. Por ejemplo, un evento de red de comando y control va seguido de un evento de red que sabemos que está exfiltrando datos.

Transferencia de archivos (basada en hash)

Esta regla correlaciona las transferencias de archivos malintencionadas. Por ejemplo, si se descarga el mismo archivo malintencionado en varios hosts de la red, la regla correlacionará todas estas transferencias en una intrusión. La similitud de las transferencias de archivos malintencionadas se determina en función del hash SHA-1 del archivo transferido.

Transferencia de archivos (basada en etiquetas de análisis)

Esta regla correlaciona las transferencias de archivos malintencionadas. Por ejemplo, si se descarga el mismo archivo malintencionado en varios hosts de la red, la regla correlacionará todas estas transferencias en una intrusión. La similitud de las transferencias de archivos malintencionadas se determina en función de las etiquetas asociadas a las tareas de análisis de los archivos.

Análisis de vulnerabilidad

Esta regla correlaciona diferentes tipos de eventos de red que potencialmente indican un análisis de vulnerabilidad. Por ejemplo, se observan varios eventos de tipo NTA o de tipo infección saliente desde un único host hacia uno o varios hosts de destino internos.

Olas

Este grupo de reglas identifica las "olas" de ataque, en las que se observa el mismo ataque (es decir, incidentes para la misma amenaza) en varios hosts de la red dentro de un período de tiempo determinado.

Este grupo de reglas es útil para identificar los hosts de la red que han pasado a formar parte de la misma infraestructura de comando y control o que han estado expuestos al mismo vector de ataque (por ejemplo, un ataque de tipo drive-by o un ataque de distribución de malware). Como resultado, estas reglas están restringidas a las amenazas de clase comando y control, drive-by, distribución de malware, sinkhole, falso AV y minería de criptomonedas.

Las reglas de este grupo se activan en los siguientes casos.

- Existen eventos de firma de red en los que la clase de amenaza es comando y control, lo que afecta a varios hosts.
- Existen eventos de firma de red en los que la clase de amenaza es distribución de malware, lo que afecta a varios hosts.
- Hay eventos de firma de red en los que la clase de amenaza es drive-by y la entrada (dirección IP o nombre de host) donde se produjeron las detecciones son la misma, lo que afecta a varios hosts.
- Hay eventos de reputación malintencionados para la misma entrada (dirección IP o nombre de host) y la clase de amenaza es comando y control, lo que afecta a varios hosts.
- Hay eventos de reputación malintencionados para la misma entrada (dirección IP o nombre de host) y la clase de amenaza es distribución de malware, lo que afecta a varios hosts.

En este caso, la ventana de correlación se establece en tres días. Por lo tanto, se consideran relacionados dos incidentes por la misma amenaza que afectan a diferentes hosts si se producen dentro de este intervalo de tiempo limitado.

Nota Estas reglas pueden crear campañas que incluyan solo un host y un incidente.

Drive-by confirmado

Este grupo de reglas identifica las campañas en las que un host interno está expuesto a un ataque de tipo drive-by con éxito. Se considera que un ataque drive-by a un host tiene éxito si va seguido de una actividad de comando y control, descarga de malware, sinkhole o falso AV. Las reglas de este grupo se activan en los siguientes casos.

- Un ataque drive-by seguido de cerca por actividad de descarga de malware: en este caso, la ventana de correlación es de 10 minutos, ya que esperamos que la descarga esté causada inmediatamente por una vulnerabilidad del navegador con éxito.
- Un ataque drive-by seguido de cerca por actividad de un falso AV: en este caso, la ventana de correlación es de 10 minutos, ya que esperamos que la actividad del falso AV siga inmediatamente a una vulnerabilidad drive-by.
- Un ataque drive-by seguido de actividad de comando y control: en este caso, la ventana de correlación es de cuatro horas, ya que el canal de comando y control puede tardar en configurarse.
- Un ataque drive-by seguido de actividad sinkhole: en este caso, la ventana de correlación es de cuatro horas, ya que la actividad hacia un servidor malintencionado con un sinkhole a través de un canal de comando y control puede tardar en configurarse. Esta regla correlaciona la actividad de movimiento lateral saliente de un host de la red de inicio y las infecciones en ese host que se produjeron antes de las detecciones de movimiento lateral (pero dentro de la ventana de correlación).

Nota Estas reglas pueden crear campañas que incluyan solo un host.

Descarga de archivo confirmada

Este grupo de reglas identifica las campañas en las que se descarga y ejecuta correctamente un archivo malintencionado en un host. Se considera que un archivo descargado se ejecutó correctamente en un host si, poco después de la descarga, hay eventos de red para las actividades que coinciden con la actividad observada durante el análisis del archivo.

En particular, el análisis de archivos puede proporcionar dos partes más de información para caracterizar la actividad observada durante el análisis.

Información de malware

Si el comportamiento del archivo coincide con el comportamiento de una amenaza conocida, el nombre del malware pasará a estar disponible.

Información de IoC de red

Si durante el análisis la muestra genera un tráfico de red que coincide con las firmas de red o la inteligencia de amenazas, se pondrán a disposición los indicadores del tráfico. Es decir, se proporcionará información sobre reputación malintencionada y coincidencias de firma de red.

Las reglas de este grupo se activan en los siguientes dos casos, según el tipo de información derivada del análisis de archivos.

- Caso basado en malware
 - Se descarga un archivo en un host.
 - El análisis del archivo atribuye una amenaza específica al archivo (por ejemplo, el malware Emotet).
 - Más tarde, se detecta un evento de red para la misma amenaza (es decir, Emotet) para el host que descargó el archivo.
- Caso basado en IoC de red
 - Se descarga un archivo en un host.
 - El análisis del archivo identifica IoC de red para el archivo.
 - Más tarde, el host que descargó el archivo intenta contactar con una dirección IP o un nombre de host incluidos en el IoC de reputación malintencionada extraído para el archivo y este tráfico coincide con una firma de red.

La aplicación NSX Network Detection and Response establece la ventana de correlación en este caso en tres días.

Nota Esta regla puede crear campañas que incluyan solo un host.

Movimiento lateral

Este grupo de reglas identifica campañas en las que los atacantes han establecido una "cabeza de playa" en la red comprometiendo algunos hosts y luego intentan moverse lateralmente dentro de la red para comprometer hosts adicionales.

Este grupo consta de dos reglas, cada una de las cuales detecta un paso independiente de la campaña de movimiento lateral.

Movimiento lateral saliente

Esta regla correlaciona la actividad de movimiento lateral saliente de un host de la red local y las infecciones en ese host que se produjeron antes de las detecciones de movimiento laterales (pero dentro de la ventana de correlación).

Movimiento lateral entrante

Esta regla correlaciona la actividad de movimiento lateral entrante con un host de la red de inicio configurada y la actividad comúnmente observada después de un compromiso inicial (comando y control, sondeo y recopilación de credenciales) que ocurrió en el mismo host después de las detecciones de movimiento lateral. Por ejemplo, el uso del protocolo de escritorio remoto (RDP) puede ser normal en un entorno en el que esta herramienta se utiliza para fines administrativos legítimos, pero en otras situaciones puede ser un indicio muy sospechoso de que un atacante podría estar intentando controlar de forma remota un host.

Tenga en cuenta que estas reglas solo se activarán para los hosts dentro de la red de inicio, es decir, que la campaña se crea solo si los hosts de origen y destino de las actividades de movimiento lateral pertenecen a la red de inicio. Si la red de inicio no está configurada, el sistema utilizará [rangos de RFC1918](#) de forma predeterminada.

Promoción de eventos INFO

La aplicación NSX Network Detection and Response detecta varias actividades en una red protegida que podrían ser interesantes para un analista, pero que probablemente no sean malintencionadas. Estas detecciones generan eventos INFO, que se pueden ver estableciendo un valor adecuado para el filtro "resultado de evento".

La aplicación NSX Network Detection and Response no tiene en cuenta los eventos INFO para fines de correlación.

Un desafío con estas detecciones es que la misma actividad de evento INFO puede ser normal o altamente sospechosa, en función de la red en la que la detectó la aplicación NSX Network Detection and Response. Por ejemplo, el uso del protocolo de escritorio remoto (RDP) puede ser normal en un entorno en el que esta herramienta se utiliza para fines administrativos legítimos, pero puede ser un indicio muy sospechoso de que un atacante podría estar intentando controlar de forma remota un host.

La lógica de detección de anomalías es capaz de determinar cuándo ciertos tipos de detecciones de INFO son inusuales para la red supervisada y para los hosts de origen y destino específicos involucrados. Cuando el sistema determina que una detección de INFO es inusual, el evento pasa al modo de "detección" y, como consecuencia, se muestra entre los eventos normales. Este escenario es relevante en el contexto de las reglas de correlación para el movimiento lateral, ya que la detección de la actividad de movimiento lateral a menudo provoca la creación de eventos INFO.

Red de inicio

La configuración de red de inicio tiene el siguiente efecto en las reglas de correlación de campañas.

- Todas las reglas de correlación de campañas ignoran los eventos que se produjeron en hosts fuera de la red de inicio.
- Si no hay ninguna red de inicio configurada, el sistema establecerá de forma predeterminada los [rangos de RFC1918](#).

La red de inicio se configura en **Seguridad > Configuración general > Rangos de IP privados**.

Silenciamiento de hosts

La configuración de silenciamiento de hosts tiene el siguiente efecto en las reglas de correlación de campañas.

- Si se configura el silenciamiento de hosts, todas las reglas de correlación de campañas ignorarán los eventos que se produjeron en los hosts silenciados.
- Si no se configura ningún silenciamiento de hosts, todos los hosts de origen detectados en un evento se considerarán válidos para la correlación.

Para asegurarse de que el silenciamiento de hosts no incluya por error hosts cuya actividad debe incluirse en campañas, debe comprobar esta configuración.

Acerca de la evidencia

La aplicación NSX Network Detection and Response informa sobre las acciones observadas al analizar un evento, un incidente o una campaña.

La evidencia contiene la siguiente información.

Evidencia de detección básica: red

Tipo de evidencia REPUTATION

Indica que se detectó tráfico de red a una IP o un dominio que están asociados a una amenaza conocida.

Se mostrará un campo SUBJECT y una dirección IP o un dominio. Por ejemplo: reputation: evil.com (evento de referencia), 6.6.6.6 (evento de referencia) o bad.org (evento de referencia).

Por lo general, estos dominios y direcciones IP malintencionados se bloquean. Si está disponible, se mostrará información de reputación adicional.

Las direcciones IP pueden anotarse con una ubicación (marca de país).

Tipo de evidencia SIGNATURE

Indica que se detectó tráfico de red que coincide con una firma de red para una amenaza conocida.

Se muestra un campo Detector que es el nombre/identificador único de la firma con la que se encontró una coincidencia. Por ejemplo, Detector: et:2014612 O Detector: llrules:1490720342088.

Tipo de evidencia ANOMALY

Similar a SIGNATURE, con la diferencia de que la detección se basa en una heurística que detecta algo anómalo. Por ejemplo, Anomaly: anomaly:download_smb.

Tipo de evidencia FILE DOWNLOAD

Se descargó un archivo sospechoso o malintencionado.

Se muestra `task_uuid`, el identificador de un análisis (detonación en espacio aislado) y `severity`, la puntuación de dicho análisis. Por ejemplo, `File download: a7ed621`.

A continuación se muestra información opcional adicional del evento de referencia.

- La URL desde la que se descargó el archivo
- El tipo de archivo (normalmente ejecutable)
- El nombre del archivo

Tipo de evidencia UNUSUAL_PORT

Indica que se está utilizando un puerto TCP o UDP poco común y que corresponde a lo que se espera de esta amenaza específica.

La dirección IP o el dominio implicados en el tráfico que utilizó el puerto inusual se muestran en el campo SUBJECT.

Tipo de evidencia URL_PATH_MATCH

Similar a UNUSUAL_PORT, con la diferencia de que la detección se basa en una ruta de URL. Por ejemplo, `http://evil.com/evil/path?evil=threat`, la detección se activa con la parte `/evil/path` de la URL.

Tipo de evidencia DGA

DGA hace referencia a "algoritmo de generación de dominios", un enfoque utilizado por algunos tipos de malware, donde en lugar de utilizar una pequeña cantidad de dominios para comando y control, el malware incluye un algoritmo que genera miles de nuevos dominios aleatorios cada día. A continuación, intenta ponerse en contacto con cada uno de ellos. Para controlar su malware, el grupo solo registra uno o varios de estos dominios. El uso de DGA es muy visible en la red debido a los intentos de resolución de muchos de estos dominios.

La evidencia DGA se utiliza actualmente, además de la evidencia de reputación regular, cuando se detectan varios dominios malintencionados de un algoritmo DGA que se está resolviendo.

Evidencia de la correlación de varios eventos

Evidencia de la correlación de varios eventos

Los siguientes tipos de evidencia se crean en los casos en los que la combinación de varios eventos de red en un host aumenta la confianza en que se detectó una amenaza correctamente. Los tipos de evidencias pueden ser, por ejemplo, que se contacte con la misma entrada de reputación maliciosa o que se active la misma firma de red.

En cada uno de estos casos, la amenaza puede etiquetarse de la siguiente manera.

- `Repeated`: la amenaza específica se ha detectado tres o más veces.
- `Periodic`: también se detectó que la amenaza específica se producía a intervalos regulares.

Se muestra una etiqueta en la evidencia de REPUTATION/SIGNATURE correspondiente.

En el ejemplo de la evidencia REPUTATION, si se detectan evidencias repetidas y periódicas de bad.org, se mostrará una etiqueta REPEATED o PERIODIC.

Tipo de evidencia CONFIRMED_EXECUTION

Está asociada a amenazas como MALICIOUS FILE DOWNLOAD. Significa que se detecta un comportamiento en la red desde el host que descargó el archivo que confirma que el archivo descargado se ejecutó realmente.

Por ejemplo:

- Se descargó un archivo malintencionado en el host 1.2.3.4.
- Cuando se ejecuta en un espacio aislado, este archivo se pone en contacto con el host evil.com.
- Poco después, se observa el tráfico de comando y control desde el host 1.2.3.4 hacia evil.com, lo que confirma que se ejecutó el archivo malintencionado.

El evento de referencia vinculado es donde se descargó el archivo.

La evidencia adicional puede proporcionar confirmación de la amenaza, como la siguiente información sobre el archivo.

- UUID de tarea
- Puntuación
- Nombre de archivo
- URL desde la que se descargó

Tipo de evidencia CONFIRMED_C&C

De forma similar a CONFIRMED_EXECUTION, esta evidencia se agrega a la detección de comando y control para la amenaza especificada debido a que el host descargó previamente un archivo para esa amenaza.

Tipo de evidencia CONFIRMED_DRIVE_BY

Se agrega en situaciones en las que se detectó un ataque de tipo drive-by seguido de una indicación de que el ataque se realizó con éxito. Por ejemplo:

- El host 1.2.3.4 parece ser víctima de un ataque de tipo drive-by.
- Poco después, el host 1.2.3.4:
 - Descargó un archivo malintencionado
 - Generó tráfico de comando y control

Esta evidencia se agrega a un evento de referencia del evento drive-by inicial.

Tipo de evidencia DRIVEBY_CONFIRMATION

De forma similar a la evidencia CONFIRMED_DRIVEBY, esta evidencia se agrega como evento de referencia a las detecciones de descarga de archivos malintencionados o comando y control que se produjeron poco después de un ataque drive-by.

Trabajar con la página Hosts

La página **Hosts** muestra una lista de los hosts supervisados en la red de NSX-T Data Center.

La página consta de varios widgets que se pueden administrar mediante la información incluida en [Introducción a la interfaz de usuario de NSX Network Detection and Response](#).

Puede personalizar rápidamente la selección de hosts mediante los accesos directos de filtro. También puede seleccionar sus propios filtros. Utilice estos filtros para personalizar la lista hosts que se muestra en la página **Hosts**.

La siguiente imagen muestra una página **Hosts** de ejemplo.

The screenshot shows the 'Hosts' page interface. At the top, there are buttons for 'TIME RANGE: LAST 7 DAYS' and 'VIEW OPTIONS'. Below that is a search bar with 'Search IP address or range' and a 'GO' button. A 'Filters' section includes a 'Quick search' input and a 'SELECT' dropdown. The main table displays 5 hosts with columns: IMPACT, HOST IP, THREATS, THREAT ACTIVITY, and CAMPAIGNS. Each host row has a checkbox in the first column.

	IMPACT	HOST IP	THREATS	THREAT ACTIVITY	CAMPAIGNS
<input checked="" type="checkbox"/>	! 92	35.199.17.54	TeslaCrypt	2021-08-24 14:36:56 - 2021-08-26 09:...	-
<input checked="" type="checkbox"/>	! 60	15.16.104	ETERNALBLUE, CVE-2017-0143 Expl...	2021-08-24 14:36:55 - 2021-08-26 15:...	! 1
<input checked="" type="checkbox"/>	! 60	1.2.238.177	ETERNALBLUE	2021-08-24 14:36:31 - 2021-08-26 15:4...	-
<input checked="" type="checkbox"/>	! 60	1.2.19.3	CVE-2017-0143 Exploit	2021-08-24 14:36:25 - 2021-08-26 15:...	-
<input checked="" type="checkbox"/>	! 1	52.4.181.42	Lastline sensor rule test	2021-08-24 14:38:22 - 2021-08-25 11:4...	-

Filtrar accesos directos

Para limitar los datos de la lista de hosts que se muestran en la página **Hosts** de la interfaz de usuario de NSX Network Detection and Response, utilice los accesos directos de filtro.

Para seleccionar uno de los siguientes accesos directos de filtro, haga clic en el botón correspondiente que aparece en la interfaz de usuario.

Nombre de acceso directo	Descripción
Hosts con amenazas	Enumera todos los hosts de la red de inicio con amenazas detectadas.
Abrir amenazas de alto impacto	Enumera todos los hosts de la red de inicio con amenazas de alto impacto abiertas.
Amenazas que no son de campaña	Enumera todos los hosts de la red de inicio con amenazas que no forman parte de una campaña.

Como alternativa, también puede limitar los datos mostrados introduciendo una dirección IP IPV4 válida, un rango de direcciones IP o un bloque CIDR en el cuadro de texto de búsqueda situado en el lado derecho del widget **Filtrar accesos directos** y haciendo clic en **IR**.

Usar filtros en la página Host

La aplicación NSX Network Detection and Response proporciona un mecanismo de filtrado que le permitirá centrarse en la información específica del host que le interese. El uso de filtros es opcional.

Procedimiento

- 1 En la página **Hosts**, haga clic en  para expandir el widget **Filtros**.
- 2 Haga clic en cualquier lugar del cuadro de texto **Filtra en** y seleccione un elemento en el menú desplegable.

Puede seleccionar entre los siguientes filtros disponibles. Para delimitar aún más el foco de la información que se muestra, puede combinar varios filtros.

Nombre de filtro	Descripción
UUID de campaña	Restrinja las entradas mostradas por el UUID de campaña. Se trata de una cadena hexadecimal de 32 caracteres, por ejemplo, <code>7dabc0fc9b3f478a850e1089a923df3a</code> . Como alternativa, introduzca la cadena <code>null</code> para seleccionar registros que no pertenezcan a ninguna campaña.
Red de inicio	Restrinja las entradas mostradas por la configuración de la red de inicio. Seleccione Solo red de inicio o Solo redes sin identificar en el menú desplegable.
IP de host	Restrinja las entradas mostradas a una dirección IP de origen, un rango de direcciones IP o un bloque CIDR específicos. Escriba el valor en el cuadro de texto.
Hosts con amenazas	Restrinja las entradas mostradas por los hosts con el estado de amenazas. Seleccione Solo hosts con amenazas o Todos los hosts en el menú desplegable.
Prioridad	Restrinja las entradas mostradas según el estado de Prioridad. Seleccione Infecciones , Lista de inspección o Molestias en el menú desplegable.
Lectura	Restrinja las entradas mostradas por su estado de lectura. Seleccione Leído o Sin leer en el menú desplegable.
Estado	Restrinja las entradas mostradas por su estado. Seleccione Cerrado o Abierto en el menú desplegable.

Nombre de filtro	Descripción
Amenaza	<p>Restrinja las entradas mostradas por una amenaza específica. Seleccione una amenaza en el menú desplegable. El menú se rellena automáticamente con una lista de amenazas catalogadas.</p> <p>Utilice la función de búsqueda en la parte superior del menú para encontrar rápidamente un nombre de amenaza.</p>
Clase de amenaza	<p>Restrinja las entradas mostradas a una clase específica de amenazas. Seleccione la clase de amenaza en el menú desplegable. El menú se rellena automáticamente con un catálogo de clases, algunos de los cuales se enumeran a continuación. Utilice la función de búsqueda en la parte superior del menú para encontrar rápidamente un nombre de clase.</p> <ul style="list-style-type: none"> ■ adware: malware que muestra o descarga anuncios en un equipo infectado. ■ fraude de clics: el fraude de clics se centra en la publicidad en línea de pago por clic. ■ comando y control: una máquina infectada pertenece a un botnet y un atacante puede controlar la máquina de forma remota. ■ drive-by: un atacante intentó explotar una vulnerabilidad en la máquina para instalar malware adicional en el sistema de destino. ■ kit de herramientas de explotación: detección de un kit de herramientas de explotación que intentó un ataque de descarga drive-by ■ falso av: software antivirus falso u otro tipo de software de seguridad no autorizado diseñado para simular o malinformar a los usuarios. ■ C&C inactivo: el servidor de comando y control de este botnet específico está inactivo. ■ Descarga de archivos malintencionados, distribución de malware y descarga de malware: la dirección IP o el dominio alojan ejecutables malintencionados. ■ sinkhole: una organización legítima opera un agujero de recepción, por lo que no representa una amenaza. Sin embargo, los hosts que intenten ponerse en contacto con ese host pueden verse afectados. ■ spyware: malware que intenta el robo de información confidencial. ■ dns sospechoso: los dominios DNS sospechosos son dominios a los que se contacta mediante malware que se ejecuta en máquinas infectadas. Nuestras técnicas patentadas pudieron identificar de forma proactiva estos dominios como malintencionados. ■ desconocido: se detectó un riesgo de seguridad desconocido.

- 3 Para aplicar los filtros seleccionados, haga clic en **Aplicar**.
- 4 (opcional) Para eliminar un filtro individual, haga clic en el botón **Eliminar** – junto a su entrada. Para eliminar todos los filtros seleccionados, haga clic en el icono  situado en el lado derecho del widget **Filtros**.

El widget **Filtros** se contrae al eliminar todos los filtros seleccionados.

Listado de hosts

La parte inferior de la página **Hosts** de la interfaz de usuario de NSX Network Detection and Response muestra una lista de hosts que cumplen los criterios de los filtros seleccionados. Si no se seleccionó ningún filtro, se mostrarán todos los hosts de la red.

Buscar

El cuadro de texto **Búsqueda rápida** situado en la parte superior izquierda del widget de lista proporciona una función de búsqueda rápida mientras introduce texto. El sistema filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier columna, que coincida con la cadena de consulta.

Nota Si la lista es larga, la **búsqueda rápida** solo examina las primeras 1000 entradas y puede devolver resultados incompletos. El número total de resultados de búsqueda devueltos se muestra en la esquina superior derecha del widget de lista.

Selección

Utilice el menú desplegable **SELECCIONAR** para realizar una selección afinada. Las opciones de selección disponibles son **Todos los visibles**, **Todas las páginas** o **Borrar selección**. Para seleccionar todos los hosts visibles, también puede hacer clic en en la fila de los nombres de columna.

Lista de hosts

Puede personalizar el número de filas que se muestran en la lista de hosts. El valor predeterminado es 20 entradas. Para desplazarse por varias páginas, utilice los iconos  y .

Cada fila proporciona un resumen de información para un host. Para seleccionar una fila de host, haga clic en el ícono . Para acceder a más información sobre un host, haga clic en cualquier lugar de una fila de entrada y se mostrará el panel **Resumen del host** de la barra lateral. Consulte [Barra lateral de resumen del host](#) para obtener información detallada.

La lista incluye las siguientes columnas.

Nombre de la columna	Descripción
IMPACTO	Las amenazas activas en el host se indican con el ícono  . El valor del impacto indica el nivel crítico de la amenaza detectada y oscila entre 1 y 100: <ul style="list-style-type: none"> ■ Un valor de amenaza igual o superior a 70 se considera crítico. El número se mostrará en rojo. ■ Un valor de amenaza entre 30 y 69 se considera de riesgo intermedio. El número se mostrará en amarillo. ■ Un valor de amenaza entre 1 y 29 se considera benigno. El número se mostrará en azul.
IP DE HOST	La dirección IP del host. Haga clic en el vínculo dirección IP para mostrar la página Perfil de host del host.
AMENAZAS	Muestra el nombre del mayor riesgo de seguridad detectado y el número de amenazas detectadas en el host. Si el nombre tiene un ícono  , haga clic en él y una ventana emergente mostrará la descripción de la amenaza.
ACTIVIDAD DE AMENAZA	Marcas de tiempo desde el primer evento y el último evento que componen este incidente.
CAMPAÑAS	El ícono  indica el número de campañas a las que pertenece el host.

Barra lateral de resumen del host

Haga clic en cualquier lugar de una fila de entrada de un host de la lista Host y la barra lateral **Resumen del host** aparecerá en el lado derecho de la página **Hosts**.

A continuación se describe lo que se ve en la barra lateral Resumen del host.

Sección principal

Los siguientes elementos se muestran en la parte superior del panel.

- Para cerrar la barra lateral, haga clic en el icono .
- Se muestran el valor de impacto y la dirección IP del host seleccionado.
- Apunte al valor de impacto y se mostrará el estado de la amenaza.
- Para ir a la página **Perfil de host**, haga clic en **Ver perfil**.
- Se muestra el número de campañas, amenazas, aplicaciones y servicios.

Sección Detalles

Se muestran los siguientes detalles sobre el host:

- La sección Nombre de host enumera todos los nombres conocidos del host.
- La sección Etiqueta de host muestra las etiquetas asignadas al host. Puede editar la etiqueta.

Campañas activas

La sección Campañas activas enumera las campañas asociadas con este host durante el período de tiempo actual, si las hubiera. Cada entrada es un resumen de una campaña e incluye la siguiente información.

- Impacto de la campaña.
- Identificador de campaña, que es un vínculo a la página **Detalles de la campaña**. Consulte [Página Detalles de la campaña](#).
- La cantidad de hosts que forman parte de la campaña.

Amenazas

La sección Amenazas enumera los incidentes de amenazas asociados con el host seleccionado durante el período de tiempo actual. Cada entrada es un resumen de una amenaza:

- Valor de impacto de la amenaza.
- El nombre de la amenaza. Al pasar el cursor sobre el nombre, se muestra una ventana emergente con más información sobre la amenaza.
- El intervalo de tiempo de actividad de amenazas.

Haga clic en el vínculo **Ver amenazas** para ver los detalles de la pestaña **Perfil de host > Amenazas**.

Página de perfil de host

La página **Perfil de host** proporciona una descripción general y detalles sobre el host seleccionado en la lista de hosts de la página NSX Network Detection and Response **Hosts**.

La página **Perfil de host** consta de las siguientes pestañas.

Nombre de la pestaña	Descripción
Descripción general	Proporciona un resumen del host y es la vista predeterminada.
Amenazas	Muestra los incidentes detectados, con su evidencia asociada, interacciones de red e IoC.
Eventos	Muestra información de eventos de detección e información.
Descargas de archivos	Muestra los archivos que se han descargado.

Hay controles y botones en la parte superior de la página **Perfil de host** que son comunes a todas las pestañas.

- Haga clic en  para volver a la lista **Hosts**.

Junto al elemento de navegación se encuentra el indicador de nivel de amenaza para el host seguido de su dirección IP. Si el host se encuentra dentro de la red de inicio, se mostrará el icono .

- Para iniciar la barra lateral **Administrar alerta**, haga clic en **Acciones de host** en la parte superior derecha de la interfaz de usuario y seleccione **Administrar alerta** en el menú desplegable. La barra lateral **Administrar alerta: filtros** aparecerá en el lado derecho.

Utilice la barra lateral **Administrar alerta** para suprimir o degradar las alertas producidas por eventos inofensivos del host, como los eventos de prueba o bloqueo del sistema, o bien para asignar valores de impacto personalizados a los eventos. Consulte [Trabajar con la barra lateral Administrar alerta](#) para obtener información detallada.

Perfil de host: pestaña Descripción general

La pestaña **Descripción general** de la página **Perfil de host** de la interfaz de usuario de NSX Network Detection and Response proporciona un resumen sobre el host seleccionado.

Resumen del host

La sección **Resumen del host** contiene el widget **Amenazas**, que proporciona una descripción general rápida de las amenazas detectadas en el host.

Campañas relacionadas

La sección **Campañas relacionadas** enumera las campañas que afectan al host seleccionado. Haga clic en el vínculo ID de campaña y la barra lateral Resumen de campaña mostrará una descripción general de la campaña.

Identidad de host

La sección Identidad de host contiene los siguientes detalles.

- IP del host: la dirección IP del host.
- Nombre de host: el nombre detectado del host.
- Etiqueta de host: la etiqueta del host. Para editar la etiqueta, haga clic en el icono.

Configuración de hosts

La sección Configuración del host contiene las siguientes propiedades.

- En Red de inicio: para agregar el host, establezca el botón de alternancia en **SÍ**. De lo contrario, establézcalo en **NO**.
- Silenciado: para agregar el host, establezca el botón de alternancia en **SÍ**. De lo contrario, establézcalo en **NO**.

Propiedades del host

La sección Propiedades del host contiene los siguientes detalles.

- Primera detección: marca de tiempo que indica cuándo se detectó el host por primera vez.
- Última detección: marca de tiempo que indica cuándo se detectó el host por última vez.

Perfil de host: pestaña Amenazas

Las amenazas detectadas por NSX Network Detection and Response se representan mediante tarjetas de amenazas en la pestaña **Amenazas** de la página **Perfil de host**.

Una tarjeta de amenaza muestra la puntuación de la amenaza calculada, el nombre y la clase de la amenaza, el resultado de detección (si está disponible), el estado de la amenaza y otras acciones. Si está disponible, se mostrará la campaña a la que está conectada esta amenaza. Expanda la tarjeta para ver su evidencia relacionada.

Utilice el menú desplegable **Ordenar por** para ordenar las tarjetas de amenazas. Puede seleccionar entre **Más reciente**, **Anterior**, **Mayor impacto** (valor predeterminado) y **Menor impacto**.

El cuadro de texto **Buscar amenazas** permite hacer una búsqueda rápida mientras introduce la búsqueda. Filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier campo, que coincida con la cadena de consulta que especificó.

Active el botón **Mostrar amenazas cerradas** para filtrar las tarjetas de amenazas mostradas por estado de amenaza. El valor predeterminado es mostrar todas las amenazas.

Gestión de las tarjetas de amenazas

Las tarjetas de amenazas muestran todas las amenazas asociadas con el host seleccionado y sus niveles de amenaza correspondientes. Cada tarjeta muestra el impacto calculado de la amenaza, el nombre de la amenaza, la clase de amenaza y, si está disponible, el resultado de detección. También muestra el estado de la amenaza: Abierta o Cerrada.

Haga clic en **Próximos pasos** y seleccione una acción en el menú desplegable.

- Seleccione **Cerrar** para cerrar la amenaza. Seleccione **Abrir** para volver a abrir una amenaza cerrada.
- Seleccione **Administrar alerta** para crear una regla de administración de alertas a partir de la amenaza.

La sección **Resumen de evidencia** contiene una descripción general de la evidencia y otros datos detectados para la amenaza. Haga clic en la **>** o casi en cualquier otro lugar de la tarjeta para expandir los detalles de la evidencia.

Si los datos de campaña conectados a esta amenaza están disponibles, se mostrará **Campaña** con un vínculo a la **barra lateral de resumen Campaña**.

Detalles de la evidencia

La columna **Evidencia** muestra las descargas de archivos, las firmas y otras categorías de tipo de evidencia junto con una marca de tiempo de cuándo se vio la evidencia. Al hacer clic en el vínculo de tipo de evidencia, se mostrará la barra lateral **Resumen de evidencia** correspondiente a ese tipo en el lado derecho de la página. La barra lateral **Resumen de evidencia** está disponible para los siguientes tipos de evidencia.

- Anomalía
- Descarga de archivos
- Firma

La columna **Interacciones de red e IoC de red** muestra la dirección IP o el nombre de dominio de los hosts externos. Al hacer clic en el vínculo, se expandirá la barra lateral **Interacción de red**.

La columna **Datos de soporte** proporciona un vínculo a los eventos de detección, así como un vínculo a los detalles de la amenaza.

Resultados de detección

Los resultados de los eventos de detección de amenazas tienen los siguientes posibles valores, enumerados en orden de gravedad.

Resultado de detección	Descripción
Correcto	Se verificó que la amenaza alcanzó su objetivo. Esto podría ser que completó su intento de verificación al servidor C&C y se recibieron datos del endpoint malintencionado.
Error	La amenaza no pudo alcanzar su objetivo. Esto puede deberse a que el servidor C&C está sin conexión, el atacante generó errores de codificación, etc.
Bloqueado	La amenaza fue bloqueada por la aplicación NSX Network Detection and Response o por una aplicación de terceros.

Si el resultado del evento es desconocido, no se muestra este campo.

Barra lateral interacción de red

Para expandir la barra lateral **Interacción de red**, haga clic en el vínculo de la dirección IP o el nombre de dominio de un host específico en la columna **Interacciones de red e IoC de red** de la pestaña **Amenazas**.

El impacto y la dirección IP del host seleccionado se muestran en la parte superior de la barra lateral.

Resumen de WHOIS

La sección **WHOIS** muestra los campos clave del registro WHOIS correspondientes a la dirección IP o el nombre de dominio seleccionados. Haga clic en el ícono  para acceder a la ventana emergente **WHOIS** y obtener más información sobre la dirección IP o el dominio. Consulte [Ventana emergente WHOIS](#) para obtener información detallada.

Abrir en

La sección **Abrir en...** contiene enlaces a proveedores de terceros, como [DomainTools](#), [VirusTotal](#) y [Google](#), entre otros. Si hay más proveedores de los que caben en la vista, puede hacer clic en

Expandir para ver más ▾ .

Barra lateral de resumen de evidencia de anomalías

La barra lateral **Resumen de evidencia** para un tipo de evidencia de anomalía aparece hacer clic en un vínculo de evidencia de anomalía en la columna **Evidencia** de la pestaña **Amenazas**.

Haga clic en **Evento de referencia** ▾ para acceder a la página **Perfil de eventos** y a todos los detalles del evento asociado.

Se proporciona una breve descripción de la evidencia.

Detalles de la amenaza

Se proporcionan los siguientes detalles sobre la amenaza.

- Amenaza: nombre del riesgo de seguridad detectado.
- Clase de amenaza: nombre de la clase de riesgo de seguridad detectada.
- Primera detección ↔ Última detección: un gráfico con la marca de tiempo de la primera y la última detección de la evidencia. La duración se muestra debajo del gráfico.

Resumen del detector

Se muestra un resumen del detector. Para obtener más información, haga clic en el vínculo

Más detalles ▾ para ver la ventana emergente **Detector**. Consulte [Ventana emergente de documentación del detector](#) para obtener información detallada.

- Nombre del detector: el nombre del detector.
- Objetivo: breve descripción del objetivo del detector.
- Categorización de ATT&CK: si corresponde, se proporciona un vínculo a la técnica ATT&CK de MITRE. De lo contrario, se mostrará N/A.

Detalles de anomalías

Se proporcionan detalles sobre la anomalía.

Detalle	Descripción
Descripción	Una breve descripción de la anomalía que detalla cómo se desvía del comportamiento de la línea base o por qué debe considerarse sospechoso.
Tipo de estado	El tipo de anomalía. Por ejemplo, Atípico.
Anomalía	El elemento anómalo detectado en el host. Por ejemplo, acceso a un puerto inusual.
Elementos de línea base	Los elementos que se suelen ver en este host.
Perfil creado:	Marca de tiempo de la creación de la línea base.
Perfil actualizado:	Marca de tiempo para el momento en que se detectó la anomalía.
Diagrama de valores atípicos	<p>El diagrama muestra la carga/descarga de datos normal del host para compararla con la transferencia de datos que se marcó como anómala. Es posible que se muestren los siguientes datos, según el detector</p> <ul style="list-style-type: none"> ■ El tamaño de carga/descarga que provocó que se activara la alerta de anomalía. ■ El tamaño máximo de carga/descarga antes de que se activara la alerta de anomalía. ■ El tamaño promedio de carga/descarga del host.

Barra lateral de resumen de la evidencia de descarga de archivos

La barra lateral **Resumen de evidencia** para un tipo de evidencia de descarga de archivos aparece al hacer clic en un vínculo de evidencia Descarga de archivos en la columna Evidencia de la pestaña **Amenazas**.

Haga clic en **Evento de referencia** > para acceder a la página **Perfil de eventos** y a todos los detalles del evento asociado.

Se proporciona una breve descripción de la evidencia.

Detalles del archivo

Se proporcionan los siguientes detalles sobre el archivo.

- **Tipo de archivo:** el tipo de alto nivel del archivo descargado. Consulte [Pestaña Único](#) para obtener la lista de tipos de archivo.
- **Confianza:** indica la probabilidad de que el archivo descargado sea malintencionado. Dado que el sistema utiliza heurísticas avanzadas para detectar amenazas desconocidas, en algunos casos, la amenaza detectada puede tener un valor de confianza menor si el volumen de información disponible para esa amenaza específica es limitado.
- **SHA1:** el hash SHA1 del archivo.

Identificación de malware

Se muestra un resumen del malware detectado. Para obtener más información, haga clic en el vínculo [Informe de análisis](#) para ver el informe Análisis. Consulte [Uso del informe Análisis](#) para obtener más información.

- **Clase de antivirus:** etiqueta que define la clase de antivirus del archivo descargado.

- Familia de antivirus: etiqueta que define la familia de antivirus del archivo descargado.
- Malware: etiqueta que define el tipo de malware del archivo descargado. Si la etiqueta tiene el icono , haga clic en el icono para ver la descripción en una ventana emergente.
- Descripción general del comportamiento: los comportamientos detectados del archivo descargado. Si hay muchos datos, se mostrará una lista parcial de forma predeterminada. Haga clic en **Expandir para ver más ▼** para ver más. Para contraer la vista de nuevo, haga clic en **Contraer para ver menos ^**.

Abrir en ...

Para abrir el archivo descargado en un servicio específico, haga clic en uno de los iconos de los proveedores. De forma predeterminada, muestra una lista parcial de proveedores.

Detalles de la descarga

Se mostrarán los detalles del archivo descargado. Para obtener más información, haga clic en el vínculo **Informe de análisis** para ver el informe Análisis. Consulte [Uso del informe Análisis](#) para obtener más información.

Información	Descripción
Nombre de archivo	La ruta del recurso al archivo descargado.
Dirección URL	La dirección URL completa del archivo descargado.
Primera detección	La marca de tiempo desde la primera vez que se detectó el archivo descargado. Si se han producido varias instancias de este archivo, este será un rango de marcas de tiempo.
Descargado de	La dirección IP del servidor de origen.
Protocolo	El protocolo que se utilizó para transferir el archivo descargado del servidor de origen.
Agente de usuario	Si está disponible, se mostrará la cadena del agente de usuario para la solicitud de descarga.

Barra lateral de resumen de evidencia de firma

La barra lateral **Resumen de evidencia** para un tipo de evidencia de firma aparece al hacer clic en un vínculo de evidencia de firma en la columna Evidencia de la pestaña **Amenazas**.

Haga clic en **Evento de referencia >** para acceder a la página **Perfil de eventos** y a todos los detalles del evento asociado.

Se proporciona una breve descripción de la evidencia.

Detalles de la amenaza

Se proporcionan los siguientes detalles sobre la amenaza.

Detalle	Descripción
Amenaza	Nombre del riesgo de seguridad detectado.
Clase de amenaza	Nombre de la clase de riesgo de seguridad detectada.
Actividad	Si está disponible, muestra la actividad actual detectada de la amenaza.

Detalle	Descripción
Confianza	Indica la probabilidad de que la amenaza detectada sea malintencionada. Para los eventos que muestran resultados de análisis, como una descarga de archivos, se muestra una puntuación.
Primera detección  Última detección	Un gráfico con la marca de tiempo de la primera y la última detección de la evidencia. La duración se muestra debajo del gráfico.

Detalles del tráfico

El widget **Tráfico de eventos de referencia** proporciona una descripción general del tráfico observado entre los hosts implicados en el evento de referencia. Al menos un host implicado en el evento es un host supervisado. El host que se comunica puede ser un host supervisado o un sistema externo.

La flecha indica la dirección del tráfico entre los hosts.

Para cada host, se muestra la dirección IP. Si el host es local, la dirección será un vínculo en el que puede hacer clic para ver la página Perfil de host. Es posible que se muestre una marca de ubicación geográfica,  o . Se pueden mostrar varios. Si está disponible, se mostrará un nombre de host. Se mostrarán todas las etiquetas de host aplicadas al host. Si está disponible, haga clic en el ícono  para ver los detalles del host en la ventana emergente **WHOIS**. Consulte [Ventana emergente WHOIS](#) para obtener detalles.

Resumen del detector

Se muestra un resumen del detector. Para obtener más información, haga clic en el vínculo

[Más detalles >](#) para ver la ventana emergente **Detector**. Consulte [Ventana emergente de documentación del detector](#) para obtener detalles.

- Nombre del detector: el nombre del detector.
- Objetivo: breve descripción del objetivo del detector.
- Regla de IDS: haga clic en el vínculo **Ver regla (si está disponible)** para abrir la ventana emergente **Detector**. Consulte [Ventana emergente de documentación del detector](#) para obtener detalles. Puede contener una regla de IDS.

Perfil de host: pestaña Eventos

La pestaña **Eventos** de la página **Perfil de host** muestra información de eventos y detección.

Eventos de detección

La lista Eventos de detección muestra los eventos que la aplicación NSX Network Detection and Response encontró asociada al host seleccionado. Estos eventos conforman algunos de los incidentes que también aparecen en la lista del host.

Personalice el número de filas que se muestran. El valor predeterminado es de 30 entradas. Utilice los iconos  y  para desplazarse por varias páginas.

Las columnas que se muestran en la lista se pueden personalizar haciendo clic en el icono .

Cada fila muestra un resumen de un evento. Haga clic en cualquier lugar de una fila de entrada para acceder a la barra lateral **Resumen de eventos**.

La lista Eventos de detección contiene las siguientes columnas.

Nombre de la columna	Descripción
Marca de tiempo	Indica la hora de inicio del evento. La hora se muestra en la zona horaria seleccionada actualmente. La lista se ordena por marca de tiempo, de forma predeterminada en orden descendente (evento más reciente en la parte superior). Puede utilizar los iconos para ordenar la lista en orden ascendente (evento más antiguo en la parte superior) o cambiar de nuevo al orden predeterminado.
Host	El host de la red supervisada que participa en este evento. Esta columna mostrará la dirección IP, el nombre de host o la etiqueta del host, según el valor actual de Ajustes de visualización.
Otra IP	Dirección IP y puerto del host que está relacionado con este evento. Por ejemplo, 203.0.113.115:80 indica que se contactó con la dirección IP 203.0.113.115 en el puerto 80. El sistema intenta localizar geográficamente la dirección IP. Si se realiza correctamente, un ícono de marca pequeña indica el país que posiblemente aloja esa dirección IP. Se utiliza un ícono Red local para los hosts locales.
Otro host	El nombre de host o la dirección IP de la entrada malintencionada o sospechosa.
Amenaza	Nombre de la clase de amenaza detectada.
Clase de amenaza	Nombre de la clase de amenaza detectada.
Impacto	El valor del impacto indica el nivel crítico de la amenaza detectada y oscila entre 1 y 100: <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas entre 1 y 29 se consideran benignas. Si aparece el ícono , significa que el artefacto se bloqueó. Haga clic en el ícono para ordenar la lista por impacto.

Eventos de detección de información

La lista Eventos de detección de información muestra eventos asociados con el host seleccionado. Esta lista contiene las mismas columnas que la lista Eventos de detección.

Perfil de host: pestaña Descargas de archivos

La pestaña **Descargas de archivos** de la página **Perfil de host** de la interfaz de usuario de NSX Network Detection and Response muestra los archivos malintencionados descargados por el host con detalles sobre su contenido y los niveles de amenaza correspondientes

El cuadro de texto **Búsqueda rápida** sobre la lista permite hacer una búsqueda rápida mientras introduce la búsqueda. Filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier campo, que coincide con la cadena de consulta.

Las columnas que se muestran en la lista se pueden personalizar haciendo clic en el icono .

Cada fila es un resumen de un archivo descargado. Haga clic en el icono  (o en cualquier lugar de una fila de entrada) para ver detalles del archivo descargado.

La lista se ordena por puntuación e incluye las siguientes columnas.

Nombre de la columna	Descripción
Marca de tiempo	La marca de tiempo de la detección de la descarga del archivo
Host	El host que descargó el archivo.
Sensor	El sensor que detectó la descarga del archivo.
IP contactada	La dirección IP del host contactado.
Ubicación	Para una descarga, esta es la dirección URL del archivo en el formato admitido. Por ejemplo, <code>\\"127.0.0.2\share\\1128dedb.exe</code> para una descarga de SMB o <code>http://www.example.com/download/example.zip</code> para una descarga HTTP. Para una carga, se muestra "Carga".
Nombre de archivo	El nombre del archivo descargado.
MD5	El hash MD5 del archivo descargado.
Tipo	El tipo de archivo de alto nivel del archivo descargado. Consulte en Pestaña Único la lista de tipos compatibles actualmente.
Clase AV	Etiqueta que define la clase de antivirus del archivo descargado. Si la etiqueta tiene un icono  , puede hacer clic en ese icono para obtener una descripción en una ventana emergente.
Malware	Una etiqueta que define el tipo de malware del archivo descargado. Si la etiqueta tiene un icono  , puede hacer clic en ese icono para obtener una descripción en una ventana emergente.
Puntuación	<p>La puntuación asignada al archivo descargado por el análisis indica el nivel crítico de la amenaza detectada y oscila entre 0 y 100:</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas entre 1 y 29 se consideran benignas. <p>Para obtener más información sobre el núcleo de la malintencionaldad y la estimación de riesgo, consulte Informe de análisis: pestaña Descripción general.</p> <p>Si aparece el icono , significa que el artefacto se bloqueó. La lista se ordena en orden descendente (las amenazas más críticas en la parte superior). Haga clic en  para ordenar la lista en orden creciente (las amenazas menos críticas en la parte superior), y haga clic en  para volver al orden predeterminado.</p>

Trabajar con la página Eventos

La página **Eventos** proporciona información sobre eventos individuales detectados por la aplicación NSX Network Detection and Response en la red de NSX-T Data Center.

La página consta de varios widgets que se pueden administrar mediante la información incluida en [Introducción a la interfaz de usuario de NSX Network Detection and Response](#).

La pestaña **Red** de la página **Eventos** consta de widgets que le permiten inspeccionar, administrar y priorizar los eventos de detección de red notificados por la aplicación NSX Network Detection and Response.

Mapa de eventos global

El widget **Mapa de eventos global** proporciona una descripción general visual de las geolocalizaciones de los eventos agregados.

Marca la ubicación aproximada de los otros hosts implicados en el evento detectado por la aplicación NSX Network Detection and Response. El color del marcador representa el impacto del evento. El tamaño del marcador representa el número de hosts afectados.

Los eventos sin ubicación específica se excluyen de este mapa.

Para obtener más información sobre las amenazas y los hosts representados en esa ubicación en particular, haga clic en un marcador en el mapa.

En la ventana emergente **Detalles de ubicación** que se muestra, puede ver la ubicación aproximada, las amenazas y los hosts de destino del evento seleccionado. Haga clic en el icono  junto a cada entrada para aplicar filtros a la lista que se muestra en la página **Eventos**.

Amenazas detectadas en la página Eventos

El widget **Amenazas detectadas** de la página **Eventos** permite ver todos los tipos de amenazas y clases de amenazas que la aplicación NSX Network Detection and Response detectó en su red.

Al hacer clic en el rectángulo de una clase de amenaza específica, puede examinar en mayor detalle las amenazas que contiene dentro de la misma visualización. Cuando selecciona una amenaza específica, el sistema muestra detalles sobre esa amenaza en particular y su actividad en su red.

Nota Sus selecciones, a medida que acceda a las amenazas individuales, recortarán la lista **Eventos de detección**. Por el contrario, cuando se utilizan los filtros para delimitar la lista de eventos que se muestra, también se filtran las amenazas que se presentan en el widget **Amenazas detectadas**.

Clase de amenaza

La vista inicial muestra las clases de amenazas detectadas en la red, similares a la siguiente imagen.



Los rectángulos representan las clases de amenazas que se detectaron en la red. El tamaño de cada rectángulo se escala en función de la cantidad de eventos para cada clase de amenaza detectada. Los colores de los bloques indican la gravedad de la amenaza.

La lista en el lado derecho del widget muestra la lista de las principales amenazas detectadas. Al señalar un elemento de la lista, una ventana emergente proporciona más información sobre la amenaza, su clase y el número de eventos y hosts afectados.

Al señalar un rectángulo específico de una clase de amenaza, aparecerá una ventana emergente. Muestra la clase de amenazas, el número de amenazas únicas y un desglose del número de eventos y hosts participantes. Al hacer clic en la ventana emergente o el rectángulo, puede profundizar en las amenazas únicas que conforman la clase de amenaza seleccionada.

Amenazas únicas

La vista posterior muestra las amenazas que conforman la clase de amenaza seleccionada. Los rectángulos se escalan en función del número de eventos de cada amenaza detectada y los colores indican la gravedad de la amenaza.

Al pasar el cursor sobre una amenaza específica, se muestra una ventana emergente. Muestra la amenaza y un desglose del número de eventos y hosts participantes. Al hacer clic en la ventana emergente o en el rectángulo para seleccionar la amenaza, se mostrará **Detalles de la amenaza** en el lado derecho del widget.

Detalles de la amenaza

La sección Detalles de la amenaza muestra la siguiente información:

- **AMENAZA:** el nombre de la amenaza.
- **CLASE:** el nombre de la clase de amenaza.
- **IMPACTO MÁXIMO:** el impacto máximo de los eventos detectados para la amenaza.
- **EVENTOS:** el número de eventos detectados.
- **HOSTS:** la cantidad de hosts de destino. Para ver la lista hosts, haga clic en el vínculo numérico. Consulte [Lista de hosts](#) para obtener detalles.
- **PRIMERA DETECCIÓN/ÚLTIMA DETECCIÓN:** un gráfico de barras que muestra las marcas de tiempo vistas para la amenaza. La duración se muestra debajo.

Usar filtros en la página Eventos

La aplicación NSX Network Detection and Response proporciona un mecanismo de filtrado que le permitirá centrarse en la información específica de eventos que le interese. El uso de filtros es opcional.

Procedimiento

- 1 En la página **Eventos**, haga clic en  para expandir el widget **Filtros**.
- 2 Haga clic en cualquier lugar del cuadro de texto **Filtra en** y seleccione un elemento en el menú desplegable.

Puede seleccionar entre los siguientes filtros disponibles. Para delimitar aún más el foco de la información que se muestra, puede combinar varios filtros.

Nombre de filtro	Descripción
Resultado del evento	Seleccione Todo o Información en el menú desplegable. La configuración predeterminada es mostrar los eventos que se han determinado que están relacionados con una amenaza. Al seleccionar Info solo se incluirán los eventos informativos. Al realizar un seguimiento de estos eventos, puede obtener más información sobre la actividad de la red.
Red de inicio	Restrinja los eventos mostrados por la configuración de red de inicio mediante el menú desplegable. Seleccione Solo red de inicio para los eventos dentro de la red de inicio definida. Seleccione Solo redes sin identificar para los eventos de hosts desconocidos.
IP de host	Restrinja los eventos mostrados a una dirección IP de origen, un rango de direcciones IP o un bloque CIDR específicos. Escriba un valor válido en el cuadro de texto IP de host .
Nombre del host	Restrinja los eventos mostrados a un nombre de host de origen específico. Se debe proporcionar la etiqueta o el nombre de host completos.
Identificador de incidente	Muestra los eventos que pertenecen al incidente especificado. Un identificador de incidente es una entrada numérica, por ejemplo, 73142. Se debe proporcionar un identificador de incidente válido.
Impacto mínimo	Muestra los eventos que han marcado el nivel de impacto mínimo. El rango es 1-100.
Otro host	Restrinja los eventos mostrados a un nombre de host específico.
IP de otro host	Restrinja los eventos mostrados a una dirección IP de host específica. La dirección IP se puede introducir como una o varias direcciones IP, bloques CIDR (como 192.168.0.0/24) o rangos de direcciones IP (como 1.1.1.5-1.1.1.9).
Puerto	Muestre los eventos mediante un puerto TCP/UDP específico. Para filtrar aún más los eventos mostrados, puede combinarlos con el filtro Transporte .
Prioridad	Restrinja los eventos mostrados por el estado Prioridad. Seleccione Infecciones , Lista de inspección o Molestias en el menú desplegable. Consulte Infecciones a lo largo del tiempo para obtener detalles.
Amenaza	Restrinja los incidentes mostrados por una amenaza específica. Seleccione una amenaza en el menú desplegable. El menú se rellena automáticamente con una lista de amenazas catalogadas. Utilice la función de búsqueda en la parte superior del menú para encontrar rápidamente un nombre de amenaza.

Nombre de filtro	Descripción
Clase de amenaza	Restrinja la visualización a una clase específica de eventos. Seleccione la clase de amenaza en el menú desplegable. El menú se rellena automáticamente con un catálogo de clases.
Transporte	Muestre los eventos mediante un protocolo de capa de transporte específico. Seleccione TCP o UDP en el menú desplegable.

- 3 Para aplicar los filtros seleccionados, haga clic en **Aplicar**.

El sistema aplicará los filtros seleccionados y actualizará la lista eventos.

- 4 (opcional) Para eliminar un filtro individual, haga clic en el botón **ELIMINAR**– junto a su entrada. Para eliminar todos los filtros seleccionados, haga clic en el icono **X** situado en el lado derecho del widget **Filtros**.

El widget **Filtros** se contrae al eliminar todos los filtros seleccionados.

Eventos de detección

El widget **Eventos de detección** proporciona una descripción general de los eventos individuales detectados por la aplicación NSX Network Detection and Response.

Un evento representa una actividad relevante para la seguridad que se ha producido en la red supervisada. Un evento puede incluir varios flujos de datos (por ejemplo, conexiones TCP), pero representa un solo tipo de actividad que se produce durante un breve período de tiempo (como máximo, una hora).

Si el intervalo de tiempo seleccionado incluye hoy (el predeterminado), el widget actualizará su lista de eventos cada 5 minutos. Los eventos nuevos se resaltan en color verde; el color se atenúa después de unos segundos.

El campo **Búsqueda rápida** sobre la lista permite hacer una búsqueda rápida mientras introduce la búsqueda. Filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier campo, que coincida con la cadena de consulta.

Actualice manualmente la lista de eventos haciendo clic en el botón **Actualizar ahora**.

Personalice el número de filas que se muestran. De forma predeterminada, se muestran 30 entradas. Se pueden mostrar hasta 1000 eventos; sin embargo, es posible que haya un retraso considerable para que el sistema recupere un gran número de eventos. Utilice los iconos de **<** y **>** para desplazarse por varias páginas.

Cada fila muestra un resumen de un evento. Haga clic en cualquier lugar de una fila de entrada para acceder a la barra lateral **Resumen de eventos**.

La lista de eventos contiene las siguientes columnas.

Nombre de la columna	Descripción
Marca de tiempo	<p>Indica la hora de inicio del evento. La hora se muestra en la zona horaria seleccionada actualmente.</p> <p>La lista se ordena por marca de tiempo, de forma predeterminada en orden descendente (evento más reciente en la parte superior). Puede utilizar los iconos para ordenar la lista en orden ascendente (evento más antiguo en la parte superior) o cambiar de nuevo al orden predeterminado.</p> <p>Haga clic en el ícono  para ordenar la lista por marca de tiempo.</p>
Host	<p>El host de la red supervisada que participa en este evento. Esta columna mostrará la dirección IP, el nombre de host o la etiqueta del host, según el valor actual de Ajustes de visualización. Haga clic en el ícono Editar junto al host para abrir la ventana emergente Etiquetar/Silenciar host.</p>
Otra IP	<p>Dirección IP y puerto del host que está relacionado con este evento. Por ejemplo, 203.0.113.115:80 indica que se contactó con la dirección IP 203.0.113.115 en el puerto 80.</p> <p>El sistema intenta localizar geográficamente la dirección IP. Si se realiza correctamente, un ícono de marca pequeña indica el país que posiblemente aloja esa dirección IP. Se utiliza un ícono Red local para los hosts locales.</p>
Otro host	<p>El nombre de host o la dirección IP de la entrada malintencionada o sospechosa.</p>
Amenaza	<p>Nombre de la amenaza o el riesgo de seguridad detectados.</p>
Clase de amenaza	<p>Nombre de la clase de amenaza detectada.</p>
Impacto	<p>El valor del impacto indica el nivel crítico de la amenaza detectada y oscila entre 1 y 100:</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas entre 1 y 29 se consideran benignas. <p>Si aparece el ícono , significa que el artefacto se bloqueó.</p> <p>Haga clic en el ícono  para ordenar la lista por impacto.</p>

Barra lateral de resumen de eventos

Puede acceder a la barra lateral **Resumen de eventos** al hacer clic en una fila de entrada en el widget **Eventos de detección** de la página NSX Network Detection and Response**Eventos**.

En la siguiente sección se describe lo que se ve en esta barra lateral. Después de la sección superior, las secciones posteriores muestran los datos de soporte. Algunas secciones solo se muestran si hay datos relevantes disponibles.

Sección principal

La parte superior de la barra lateral incluye lo siguiente:

- Para cerrar la barra lateral, haga clic en el ícono .
- Para ver el evento en la página **Perfil del evento**, haga clic en **Detalles**  . Consulte [Página de perfil del evento](#) para obtener más información.

- Si está disponible, se proporciona una breve descripción del evento. Incluye una explicación del motivo por el que el sistema marcó este evento, identifica la amenaza o el malware asociado a este evento y describe brevemente la actividad detectada.

Detalles de la amenaza

Esta sección incluye la siguiente información.

Nombre de detalle de la amenaza	Descripción
Amenaza	Nombre del riesgo de seguridad detectado.
Clase de amenaza	Nombre de la clase de riesgo de seguridad detectada.
Detector de eventos	<p>El nombre del detector de eventos. Haga clic en el vínculo para ver la ventana emergente Detector. Consulte Ventana emergente de documentación del detector para obtener detalles.</p> <p>Si no hay ningún detector para el evento, no se muestra esta sección.</p>
Impacto	<p>El valor del impacto indica el nivel crítico de la amenaza detectada y oscila entre 1 y 100</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas entre 1 y 29 se consideran benignas.
Acción	Una lista de acciones realizadas por el sensor (por ejemplo, cualquier actividad de bloqueo, si el evento se registra, si se capturó tráfico o se extrajo una descarga de malware).
Resultado	<p>El resultado del evento. En la mayoría de los casos, se trata de Detección.</p> <p>Para los eventos Info y los eventos que se promocionaron desde el estado Info, una etiqueta adicional proporciona el motivo de su cambio de estado. Al pasar el cursor sobre la etiqueta, se muestra una ventana emergente que proporciona detalles adicionales sobre el motivo.</p>
Primera detección - Última detección	<p>Un gráfico con la marca de tiempo de la primera y la última detección de la evidencia.</p> <p>La información sobre duración se muestra debajo del gráfico.</p>

Tráfico de eventos

El widget **Tráfico de eventos** proporciona una descripción general del tráfico observado entre los hosts implicados en el evento. Al menos un host implicado en el evento es un host supervisado. El host que se comunica puede ser un host supervisado o un sistema externo. Si los datos están disponibles, se mostrará un vínculo para ver el tráfico capturado.

La flecha indica la dirección del tráfico entre los hosts.

Para cada host, se muestra la dirección IP. Si el host es local, la dirección será un vínculo en el que puede hacer clic para ver la página **Perfil de host**. Es posible que se muestre una marca de ubicación geográfica, o . Es posible que se muestre más de uno. Si está disponible, se mostrará un nombre de host. Si está disponible en la supervisión del tráfico DHCP, se mostrará la dirección MAC del host. Se mostrarán todas las etiquetas de host aplicadas al host. Si está disponible, haga clic en para ver los detalles del host en la ventana emergente **WHOIS**.

Evidencia de evento

La sección Evidencia de evento enumera varias acciones observadas al analizar el evento. Para obtener más detalles, haga clic en el vínculo **Detalles del evento** para ver la evidencia del evento.

Las acciones incluyen Firma, Reputación, Comportamiento inusual, Descarga de archivos, Coincidencia de ruta de URL, Verificación, Anomalía, etc. Si se proporciona, haga clic en el vínculo para ver la ventana emergente **Detector** correspondiente. Se muestra un valor de confianza para cada acción.

Identificación de malware

Si se activa la aplicación Prevención de malware de NSX, se mostrará un resumen del malware detectado. Para obtener más información, haga clic en el vínculo **Informe de análisis** para ver el informe Análisis. Consulte [Uso del informe Análisis](#) para obtener más información.

Nombre de detalle	Descripción
Clase de antivirus	Etiqueta que define la clase de antivirus del archivo descargado.
Familia antivirus	Etiqueta que define la familia de antivirus del archivo descargado.
Malware	Una etiqueta que define el tipo de malware del archivo descargado. Si la etiqueta tiene un icono , puede hacer clic en él para obtener una descripción emergente.
Descripción general del comportamiento	Los comportamientos detectados del archivo descargado. Si hay muchos datos, se mostrará una lista parcial de forma predeterminada. Haga clic en Expandir para ver más para ver más. Para contraer la vista de nuevo, haga clic en Contraer para ver menos .

URL de eventos

La sección URL de eventos muestra todas las URL detectadas en el evento. Esta sección aparece solo si el evento está asociado a una URL.

Metadatos de eventos

La sección Metadatos de eventos muestra los siguientes datos.

Nombre de datos	Descripción
Incidente relacionado	Haga clic en  para ver el incidente relacionado, si hay alguno disponible.
Conexiones	Número de conexiones incluidas en el evento.
Campaña relacionada	Haga clic en  para ver la campaña relacionada, si hay alguna disponible.

Ventana emergente WHOIS

La ventana emergente **WHOIS** muestra información de registro y otros detalles sobre la dirección IP o el nombre de host del host que está examinando.

Tiene las siguientes dos pestañas.

Resumen

La pestaña **RESUMEN** muestra la siguiente información sobre la dirección IP o el nombre de host.

- Información de fecha: la fecha de registro del dominio, la fecha en la que se actualizó el registro del dominio y, si está disponible, la fecha de caducidad del dominio.
- Organización: el nombre de la organización, las direcciones de correo electrónico de la organización, el país de la organización (código de país), los números de teléfono de la organización, el nombre del registrador y la lista de contactos.
- Red: el nombre de red, el rango de direcciones IP, la lista de AS, los servidores de nombres autoritativos y las redes principales.

Registro sin formato

La pestaña **REGISTRO SIN FORMATO** muestra los datos de WHOIS sin formato.

Información no disponible

Si la ventana emergente **WHOIS** muestra una advertencia de que la información de la dirección IP o el nombre de host especificados no está disponible, puede intentar usar un tercero. Para buscar el host, haga clic en **Ver en herramienta externa** en la parte inferior derecha de la ventana emergente.

Nota El botón para el proveedor de terceros siempre está disponible.

Ventana emergente de documentación del detector

La ventana emergente **Documentación del detector** proporciona información detallada sobre el detector de NSX Network Detection and Response que proporcionó la evidencia del evento. El objetivo es ayudarle a determinar la confianza que puede depositar en este detector.

La documentación muestra al menos algunos de los siguientes detalles.

Nombre de detalle	Descripción
Objetivo	Breve descripción del objetivo del detector.
Categorización ATT&CK	Si corresponde, se proporcionará un vínculo a la técnica ATT&CK de MITRE.
Resumen del detector	Una descripción técnica detallada del detector y su operación.
Regla de IDS	Una representación de alto nivel de la lógica de detección utilizada por una firma de red de NSX Network Detection and Response. La sintaxis de la regla está relacionada en general con el lenguaje de firma Suricata definido en https://suricata.readthedocs.io/en/latest/rules/index.html . Una regla consta de uno o varios conjuntos de cláusulas, normalmente una única cláusula, y cada una contiene pares de clave/valor. Si hay más de una cláusula en una regla, cada una estará numerada, la primera precedida por "IF:" y cada una de las posteriores por "AND THEN IF:". Los distintos conjuntos de cláusulas se evaluarán secuencialmente en los datos que pertenecen al mismo flujo. Apunte a cualquier par clave/valor para ver una ventana emergente de ayuda relevante.
Falsos positivos	Una descripción de la posibilidad de que el detector genere falsos positivos.
Falsos negativos	Los supuestos que pueden provocar que el detector cause falsos negativos.

Página de perfil del evento

Se accede a la página **Perfil del evento** desde el botón **Detalles** ➤ situado en la parte superior de la barra lateral **Resumen de eventos**.

Hay una serie de controles y botones en la parte superior de la vista:

- Haga clic en **Eventos similares** para ver una lista desplegable de funciones similares. Haga clic en el ícono de junto a cada uno para seleccionar **Destino**, **Puerto de destino**, **IP de origen**, **Protocolo de transporte**, **Clase de amenaza** y **Tipo de amenaza**. A continuación, haga clic **Ver eventos** 🔍 para ver los eventos seleccionados en una pestaña nueva.
- Haga clic en **Administrar alerta** para iniciar la barra lateral **Administrar alerta**. Utilice esta función para suprimir o degradar eventos inofensivos, como los eventos de prueba o bloqueo del sistema, o para aplicar puntuaciones personalizadas a eventos específicos. Consulte [Trabajar con la barra lateral Administrar alerta](#) para obtener detalles.
- Haga clic en el ícono  para contraer todos los campos o en el ícono  para expandirlos todos.

Descripción general de eventos

La sección superior proporciona una descripción general visual de la amenaza o el malware que ha detectado la aplicación NSX Network Detection and Response y muestra la clase de amenaza y la puntuación de impacto de la amenaza.

Resumen de eventos

La sección **Resumen de eventos** proporciona una explicación del motivo por el que la aplicación NSX Network Detection and Response marcó este evento, identifica la amenaza o el malware asociado a este evento, describe brevemente la actividad detectada y muestra los datos de respaldo.

Si está disponible en el servicio de nube NSX Advanced Threat Prevention, se mostrará una explicación detallada del evento y el motivo por el que se considera malintencionado en la parte superior de la sección **Resumen de eventos**.

Bloque de servidores

El bloque de servidores muestra los siguientes datos.

Datos	Descripción
Nombre del host	Si está disponible, el FQDN del servidor.
Dirección IP	<p>La dirección IP del servidor de. Es posible que se muestre una marca de ubicación geográfica. Si se muestra el icono , haga clic en el vínculo para ver más detalles en la página Perfil de host.</p> <p>Si está disponible, haga clic en el icono  para ver las etiquetas de reputación del cliente.</p> <p>Si está disponible, haga clic en el icono  para ver la información de registro y otros datos sobre el host en la ventana emergente WHOIS.</p>
Dirección MAC	Si está disponible, la dirección MAC del servidor. Esta dirección se obtiene de la supervisión del tráfico DHCP y es uno de los puntos de datos que utiliza el sistema para generar una entrada de HostID única que se asigna a un host específico de la red, independientemente de su dirección IP.

Bloque de clientes

El bloque de clientes muestra los siguientes datos.

Datos	Descripción
Nombre del host	Si está disponible, el FQDN del cliente.
Dirección IP	<p>La dirección IP del cliente. Es posible que se muestre una marca de ubicación geográfica. Si está disponible, haga clic en la dirección o en el icono  para ver la página Perfil de host.</p> <p>Si está disponible, haga clic en el icono  para ver las etiquetas de reputación del cliente.</p> <p>Si está disponible, haga clic en el icono  para ver la información de registro y otros datos sobre el host en la ventana emergente WHOIS.</p>
Dirección MAC	Si está disponible, la dirección MAC del cliente. Esta dirección se obtiene de la supervisión del tráfico DHCP y es uno de los puntos de datos que utiliza el sistema para generar una entrada de HostID única que se asigna a un host específico de la red, independientemente de su dirección IP.

Metadatos de eventos

La sección Metadatos de eventos muestra los siguientes datos.

Datos	Descripción
Resultado de verificación	Indica el resultado del evento. Estos son los valores posibles: <ul style="list-style-type: none"> ■ Bloqueado: la amenaza fue bloqueada por la aplicación NSX Network Detection and Response o por una aplicación de terceros. ■ Error: la amenaza no pudo alcanzar su objetivo. Esto puede deberse a que el servidor C&C está sin conexión, el atacante generó errores de codificación, etc. ■ Correcto: se verificó que la amenaza alcanzó su objetivo. Este podría ser que completó su intento de verificación al servidor C&C y se recibieron datos del endpoint malintencionado. Si el resultado del evento es desconocido, no se muestra este campo.
Nombre del verificador	El nombre del verificador de eventos. Haga clic en el vínculo para acceder a la ventana emergente Documentación del verificador .
Mensaje del verificador	Un mensaje del verificador que proporciona más información sobre el resultado, por ejemplo, qué aplicación de terceros bloqueó la amenaza.
Sensor	El sensor que detectó el evento.
Conexiones	Número de conexiones incluidas en el evento.
Acción	Una lista de acciones realizadas por el sensor (por ejemplo, cualquier actividad de bloqueo, si el evento se registra, si se capturó tráfico o se extrajo una descarga de malware).
Usuarios que iniciaron sesión	Una lista de los usuarios detectados en los registros registrados.
Resultado	El resultado del evento. En la mayoría de los casos, el resultado es DETECCIÓN . Para los eventos INFO y los eventos que se promocionaron desde el estado INFO, una etiqueta adicional proporciona el motivo de su cambio de estado. Al pasar el cursor sobre la etiqueta, se muestra una ventana emergente que proporciona detalles adicionales sobre el motivo.
Incidente relacionado	Vínculo permanente a un incidente correlacionado. Al hacer clic en el enlace  , se abre la página Perfil del incidente en una nueva pestaña del navegador. Este evento puede ser uno de varios eventos estrechamente relacionados que se correlacionan automáticamente con un incidente.
Identificador de evento	Consulte el evento en la página Detalles del evento de red . El enlace se abre en una nueva pestaña del navegador.
Hora de inicio	Una marca de tiempo para el comienzo del evento.
Hora de finalización	Una marca de tiempo para el final del evento.

Malware capturado

La sección Malware capturado proporciona información del análisis dinámico que se realizó en la instancia de software malintencionado que está relacionada con el evento.

Puede acceder a información técnica detallada sobre qué hace el malware, cómo funciona y qué tipo de riesgo supone. Para obtener más información sobre la información mostrada, consulte [Uso del informe Análisis](#).

Nota Si no se detectó ningún software malintencionado para el evento, esta sección no aparecerá.

Evidencia de evento

La sección Evidencia de evento proporciona detalles de las acciones observadas al analizar el evento.

Las acciones pueden incluir la descarga de archivos malintencionados, el tráfico de red que coincide con la firma de red de las amenazas conocidas, la resolución de nombres de dominio de un dominio de malware bloqueado, una ruta de URL incorrecta conocida, etc.

Si está disponible, haga clic en el vínculo Detector para ver la ventana emergente [Ventana emergente de documentación del detector](#). Consulte también [Acerca de la evidencia](#) para obtener más información.

Reputación del host

La sección Reputación del host proporciona información sobre entradas de reputación de URL o hosts malintencionados conocidos que aparecen en el evento.

Nota Si el host no tiene historial conocido, esta sección no aparecerá.

Datos de anomalías

Esta sección muestra los registros de DNS pasivos o de netflow que provocaron el evento de anomalía.

Se denominará **Datos de anomalías de DNS** o **Datos de anomalías de Netflow**, según la anomalía vista.

Se puede proporcionar información adicional, como las direcciones IP o los puertos que se clasificaron como anómalos. Si hay un gran número de elementos involucrados, puede hacer clic en el **+#** para exponer todos los elementos.

Nota Si no se ha detectado ninguna anomalía para el evento, esta sección no aparecerá.

Descripción de la amenaza

La sección Descripción de la amenaza proporciona una descripción detallada de la amenaza asociada con el evento.

Mitigación

La sección Mitigación proporciona instrucciones detalladas para eliminar cualquier software malintencionado y otros procesos recomendados para limpiar después del evento.

Nota Si no hay ningún proceso de mitigación conocido para el evento, esta sección no aparecerá.

Administrar la página Incidentes

La página **Incidentes** muestra los incidentes y sus diferentes calificaciones de amenazas. Puede utilizar los widgets de la página para inspeccionar, administrar y priorizar los incidentes notificados por la aplicación NSX Network Detection and Response.

La página consta de varios widgets que se pueden administrar mediante la información incluida en [Introducción a la interfaz de usuario de NSX Network Detection and Response](#).

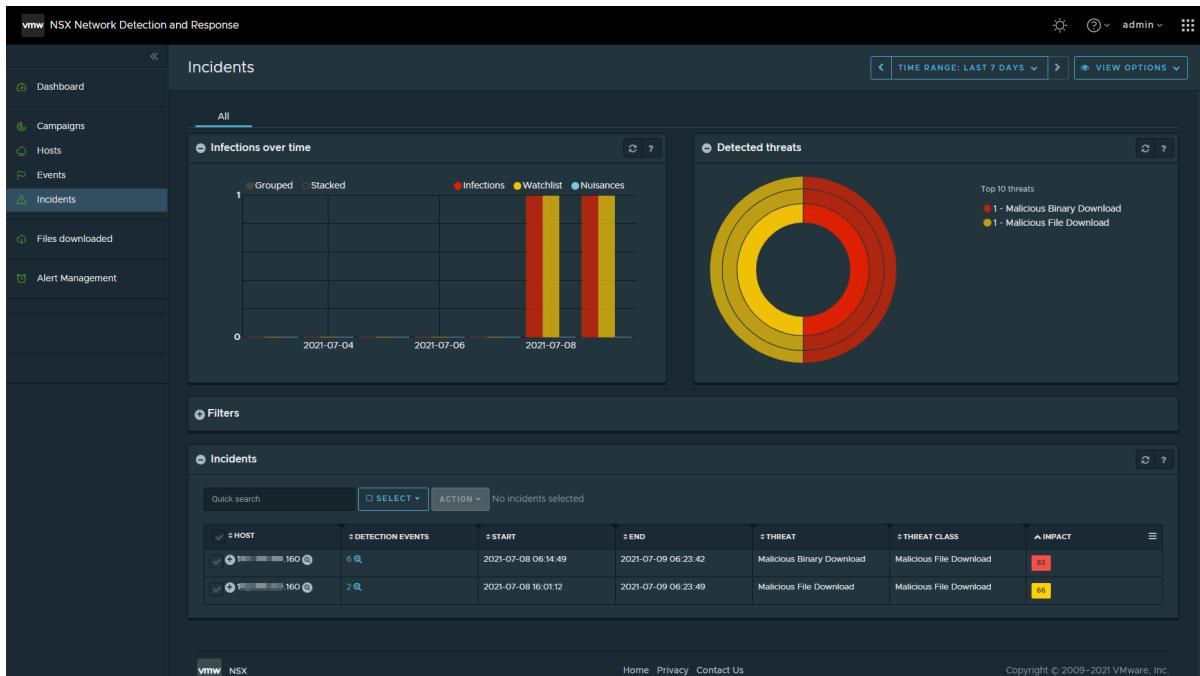
En la aplicación NSX Network Detection and Response, un incidente es un agregado de eventos de detección de una sola amenaza detectada en una sola carga de trabajo de la red supervisada.

La aplicación NSX Network Detection and Response no solo informa de los eventos de seguridad. Un incidente puede constar de un solo evento o de muchos eventos que se han correlacionado automáticamente y se ha determinado que están estrechamente relacionados con el motor de amenazas del sistema. Por ejemplo, la página **Incidentes** puede informar de todas las conexiones salientes al canal de comando y control del malware y de todas las búsquedas de DNS sospechosas (por ejemplo, solicitudes de dominios de malware relacionados generados automáticamente), y ofrecer descripciones detalladas de cada evento de seguridad registrado.

La página **Incidentes** permite realizar las siguientes tareas.

- Realizar un seguimiento eficiente de todos los incidentes que están ocurriendo.
- Vea rápidamente una lista de los hosts afectados.
- Priorizar las amenazas en función de su impacto y niveles de gravedad mediante diferentes vistas.
- Obtener información detallada sobre los eventos que se registraron para cada incidente y acceder a las descripciones de amenazas y mitigaciones.
- Cerrar o abrir incidentes.
- Marcar o borrar los hosts afectados como limpiados.
- Filtrar las amenazas notificadas para hosts específicos.

La siguiente imagen es un ejemplo de la página **Incidentes**, mostrando la pestaña **Todo**.



Infecciones a lo largo del tiempo

El widget **Infecciones a lo largo del tiempo** proporciona una descripción gráfica de los distintos tipos de incidentes detectados en la red. El eje X muestra la hora y el eje Y el número de hosts afectados por incidentes de un tipo determinado.

Existen tres tipos diferentes de incidentes.

Tipo de incidente	Descripción
Infecciones	Estos son incidentes que se determinaron como críticos. Estos incidentes tienen una puntuación de impacto de 70 o más y se muestran en color rojo.
Lista de inspección	Estos son incidentes que se determinaron como de riesgo medio. Es posible que estos incidentes, a la vez que indican un riesgo potencial, no necesiten atención inmediata; Se mantienen bajo una estrecha inspección en caso de que aparezca una nueva evidencia que modifique su estado. Estos incidentes tienen una puntuación de impacto entre 30 y 69 y se muestran en color naranja.
Molestias	Se trata de incidentes que se consideran de riesgo bajo o nulo. Por lo general, esto corresponde a una actividad potencialmente no deseada/peligrosa que no necesariamente implica un riesgo o una vulneración en la red supervisada. Estos incidentes tienen una puntuación de impacto inferior a 30 y se muestran en azul.

Para mostrar u ocultar los distintos tipos de incidentes, haga clic en sus nombres correspondientes en la leyenda situada en la parte superior del gráfico.

Al apuntar a una barra del gráfico, una ventana emergente mostrará el número de hosts de la red que se ven afectados por los incidentes correspondientes.

Al hacer clic en una barra, el intervalo de tiempo y el tipo de incidente se actualizan según corresponda. El panel de control solo muestra información de ese tipo de incidente en el día seleccionado.

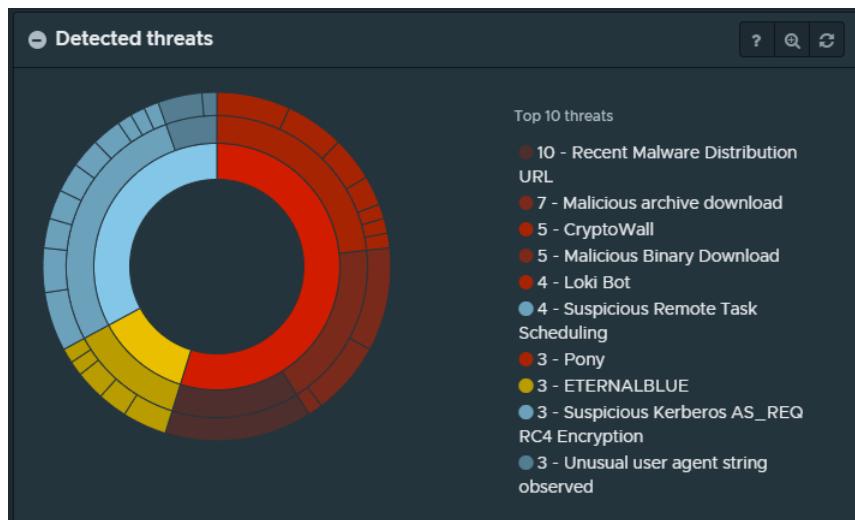
Para deshacer el zoom, restablezca el intervalo de tiempo. Tenga en cuenta que esto dejará seleccionado el tipo de incidente. Para restablecer el panel de control, utilice el botón Atrás del navegador.

La vista predeterminada muestra los incidentes en la pantalla agrupada. Haga clic en **Apilados** para ver los incidentes en una pantalla apilada. Haga clic en el **Agrupados** para volver a la pantalla agrupada.

Amenazas detectadas

El widget **Amenazas detectadas** proporciona una descripción gráfica de los distintos tipos de amenazas que ha detectado la aplicación NSX Network Detection and Response en la red.

La información de la amenaza se muestra en un círculo en capas, similar a la siguiente imagen.



Las divisiones de los círculos representan el número de hosts afectados por los tipos de incidentes mostrados. Al avanzar hacia los círculos externos, se proporciona una granularidad más precisa y una información más específica.

- El anillo más interno muestra los tres tipos diferentes de incidentes.

Tipo de incidente	Descripción
Infecciones	Estos son incidentes que la aplicación NSX Network Detection and Response determinó que son críticos. Estos incidentes tienen una puntuación de impacto de 70 o más y se muestran en color rojo.
Lista de inspección	Estos son incidentes que la aplicación NSX Network Detection and Response determinó como de riesgo medio. Estos incidentes, aunque indican un riesgo potencial, puede que no requieran una atención inmediata. Se mantienen bajo una estrecha inspección en caso de que una nueva evidencia modifique su estado. A estos incidentes se les asigna una puntuación de impacto entre 30 y 69 y se muestran en color amarillo.
Molestias	Se trata de incidentes que se consideran de riesgo bajo o nulo. Por lo general, esto corresponde a una actividad potencialmente no deseada/peligrosa que no necesariamente implica un riesgo o una vulneración en la red supervisada. Estos incidentes tienen una puntuación de impacto inferior a 30 y se muestran en azul.

- El anillo intermedio muestra la clase de amenaza junto con el número de incidentes relevantes para cada tipo de incidente. Las clases de amenazas incluyen servidores de comandos y control, descargas de archivos malintencionados, criptomineros y muchos más.
- El anillo externo representa las familias de amenazas individuales detectadas en la red. Las familias de amenazas incluyen ransomware, archivos binarios malintencionados, etc.

Al señalar el gráfico, el widget muestra el nombre de la amenaza y un recuento de hosts en los que la aplicación NSX Network Detection and Response observó la amenaza.

Al hacer clic en un elemento del gráfico, la vista se acerca y se muestran más detalles sobre el tipo de información seleccionado. Al hacer clic de nuevo en el elemento, se vuelve a alejar la vista.

Si hace clic en un tipo de incidente en el anillo interno, la vista de gráfico amplía y muestra los incidentes coincidentes en el anillo central y externo. Si hace clic en una clase de amenaza en el anillo central, la vista de gráfico se acerca y muestra las familias de amenazas coincidentes. Si hace clic en el anillo externo, la vista de gráfico se acerca y muestra detalles sobre la amenaza seleccionada.

La leyenda en el lado derecho del widget muestra un recuento de las ocurrencias de las amenazas más frecuentes detectadas. Al señalar un elemento de la leyenda, una ventana emergente proporciona más información sobre la clase de amenaza, el número de incidentes y el número de hosts afectados. Al hacer clic en el elemento, se amplía la vista de gráfico del tipo de amenaza seleccionado y se proporciona más información contextual.

Usar filtros en la página Incidentes

NSX Network Detection and Response proporciona un mecanismo de filtrado que le permitirá centrarse en la información de incidentes específica de su interés. El uso de filtros es opcional.

Procedimiento

- 1 En la página **Incidentes**, haga clic en  para expandir el widget **Filtros**.
- 2 Haga clic en cualquier lugar del cuadro de texto **Filtro en** y seleccione un elemento en el menú desplegable.

Puede seleccionar entre los siguientes filtros disponibles. Para delimitar aún más el foco de la información que se muestra, puede combinar varios filtros.

Nombre de filtro	Descripción
UUID de campaña	Restrinja las entradas mostradas por el UUID de campaña. Se trata de una cadena hexadecimal de 32 caracteres, por ejemplo, <code>7dabc0fc9b3f478a850e1089a923df3a</code> . Como alternativa, introduzca la cadena <code>null</code> para seleccionar registros que no pertenezcan a ninguna campaña.
Red de inicio	Restrinja las entradas mostradas por la configuración de la red de inicio. Seleccione Solo red de inicio o Solo redes sin identificar en el menú desplegable.
IP de host	Restrinja las entradas mostradas a una dirección IP de origen, un rango de direcciones IP o un bloque CIDR específicos. Escriba el valor en el cuadro de texto.

Nombre de filtro	Descripción
Nombre del host	Restrinja las entradas mostradas por el nombre de host. Se debe proporcionar la etiqueta o el nombre de host completos.
Prioridad	Restrinja las entradas mostradas según el estado de Prioridad. Seleccione Infecciones , Lista de inspección o Molestias en el menú desplegable.
Lectura	Restrinja las entradas mostradas por su estado de lectura. Seleccione Leído o Sin leer en el menú desplegable.
Estado	Restrinja las entradas mostradas por su estado. Seleccione Cerrado o Abierto en el menú desplegable.
Amenaza	Restrinja las entradas mostradas por una amenaza específica. Seleccione una amenaza en el menú desplegable. El menú se rellena automáticamente con una lista de amenazas catalogadas. Utilice la función de búsqueda en la parte superior del menú para encontrar rápidamente un nombre de amenaza.
Clase de amenaza	Restrinja las entradas mostradas a una clase específica de amenazas. Seleccione la clase de amenaza en el menú desplegable. El menú se rellena automáticamente con un catálogo de clases, algunos de los cuales se enumeran a continuación. Utilice la función de búsqueda en la parte superior del menú para encontrar rápidamente un nombre de clase. <ul style="list-style-type: none"> ■ adware: malware que muestra o descarga anuncios en un equipo infectado. ■ fraude de clics: el fraude de clics se centra en la publicidad en línea de pago por clic. ■ comando y control: una máquina infectada pertenece a un botnet y un atacante puede controlar la máquina de forma remota. ■ drive-by: un atacante intentó explotar una vulnerabilidad en la máquina para instalar malware adicional en el sistema de destino. ■ kit de herramientas de explotación: detección de un kit de herramientas de explotación que intentó un ataque de descarga drive-by ■ falso av: software antivirus falso u otro tipo de software de seguridad no autorizado diseñado para simular o malinformar a los usuarios. ■ C&C inactivo: el servidor de comando y control de este botnet específico está inactivo. ■ Prueba de bloqueo de VMware: el dominio block.lastline.com se utiliza para probar el bloqueo de conexiones de red y los eventos seleccionados pertenecen a esta clase. ■ Prueba de VMware: el dominio test.lastline.com se utiliza para probar la funcionalidad de la configuración y los eventos seleccionados pertenecen a esta clase. ■ Descarga de archivos malintencionados, distribución de malware y descarga de malware: la dirección IP o el dominio alojan ejecutables malintencionados. ■ sinkhole: una organización legítima opera un agujero de recepción, por lo que no representa una amenaza. Sin embargo, los hosts que intenten ponerse en contacto con ese host pueden verse afectados. ■ spyware: malware que intenta el robo de información confidencial. ■ dns sospechoso: los dominios DNS sospechosos son dominios a los que se contacta mediante malware que se ejecuta en máquinas infectadas. Nuestras técnicas patentadas pudieron identificar de forma proactiva estos dominios como malintencionados. ■ desconocido: se detectó un riesgo de seguridad desconocido.

3 Para aplicar los filtros seleccionados, haga clic en **Aplicar**.

- 4 (opcional) Para eliminar un filtro individual, haga clic en el botón **Eliminar** – junto a su entrada. Para eliminar todos los filtros seleccionados, haga clic en el icono  situado en el lado derecho del widget **Filtros**.
El widget **Filtros** se contrae al eliminar todos los filtros seleccionados.

Lista de incidentes

Un incidente representa una actividad relevante para la seguridad detectado por NSX Network Detection and Response que se ha producido en la red supervisada. Un incidente puede constar de un solo evento o de una serie de eventos que se correlacionaron automáticamente y que se determinaron como estrechamente relacionados. La lista de incidentes muestra los incidentes registrados con sus niveles de amenaza correspondientes.

Puede ver todos los incidentes notificados que se determinaron como críticos, aquellos que debe estar pendientes o aquellos que se consideran problemas en la red. Los incidentes críticos deben controlarse sin demora. No tomar ninguna acción ante un incidente crítico es muy peligroso y aumenta la probabilidad de que otros hosts de la red también se vea comprometidos.

Los incidentes que aún no ha examinado están marcados como no leídos, mientras que los que ya haya examinado se marcan como leídos. Tiene la opción de seleccionar incidentes y realizar acciones en ellos, como marcarlos como leídos o no leídos. También puede cerrar o abrir los incidentes seleccionados.

El cuadro de texto **Búsqueda rápida** sobre la lista permite hacer una búsqueda rápida mientras introduce la búsqueda. Filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier campo, que coincida con la cadena de consulta.

Utilice el menú desplegable **SELECCIONAR** para realizar una selección afinada. Sus opciones le permiten seleccionar **Todos los incidentes visibles** o **Borrar la selección**. También puede seleccionar los incidentes **Leídos (página actual)** o **No leídos (página actual)**. También puedes hacer clic en el icono **Editar** en la fila del título para seleccionar todos los mensajes visibles.

Utilice el menú desplegable **ACCIÓN** para actualizar los incidentes seleccionados: **Marca como leído**, **Marca como no leído**, **Cerrar** o **Abrir**.

Personalice el número de filas que se muestran. El valor predeterminado es 20 entradas. Utilice los iconos  y  para desplazarse por varias páginas.

Las columnas que se muestran en la lista se pueden personalizar haciendo clic en el ícono contenido adicional.

Cada fila es un resumen de un incidente. Haga clic en el ícono **Más** (o en cualquier lugar de una fila de entrada) para acceder a los detalles del incidente. Para seleccionar una fila del mensaje, haga clic en el ícono **Editar**.

La lista se ordena por Impacto e incluye las siguientes columnas.

Columna	Descripción
Host	<p>El host afectado por este incidente. Esta columna muestra la dirección IP, el nombre de host o la etiqueta del host, según la ventana emergente Ajustes de visualización actual.</p> <p>Haga clic en el icono  para ver la página Perfil de host que muestra detalles sobre el host.</p> <p>Haga clic en el icono  para ordenar la lista por información del host.</p>
Eventos de detección	<p>Número de eventos que componen este incidente. Se trata de un vínculo que muestra un recuento de eventos y el icono . Al hacer clic en este vínculo, se carga la página Eventos, filtrada para mostrar solo los eventos de este incidente.</p> <p>Haga clic en el icono  para ordenar la lista por eventos.</p>
Inicio	<p>Hora de inicio del incidente.</p> <p>Haga clic en el icono  para ordenar la lista por hora de inicio.</p>
Final	<p>Hora de finalización del incidente.</p> <p>Haga clic en el icono  para ordenar la lista por hora de finalización.</p>
Amenaza	<p>Nombre del riesgo de seguridad detectado.</p> <p>Haga clic en el icono  para ordenar la lista por amenazas.</p>
Clase de amenaza	<p>Nombre de la clase de riesgo de seguridad detectada.</p> <p>Haga clic en el icono Ordenar para ordenar la lista por clase de amenaza.</p>
Impacto	<p>El valor del impacto indica el nivel crítico de la amenaza detectada y oscila entre 1 y 100:</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas que se encuentran entre 1 y 29 se consideran benignas. <p>Si aparece el icono detener, significa que el artefacto se bloqueó.</p> <p>La lista se ordena en orden descendente de impacto (los incidentes más críticos en la parte superior). Haga clic en el icono  para ordenar la lista en orden ascendente (las incidentes menos críticos en la parte superior) y, a continuación, haga clic en el icono ángulo hacia abajo  para volver al orden predeterminado.</p>

Detalles del incidente

Al hacer clic en cualquier lugar de una fila de incidentes, la vista Detalles del incidente se expande dentro de la lista de incidentes.

Hay una serie de botones en la parte superior de los detalles del incidente:

- Haga clic en el botón  para cerrar el incidente.
- Utilice el menú desplegable **Acción** para realizar una acción en el incidente:
 - Si el incidente aún no se ha cerrado, seleccione **Cerrar incidente** . De lo contrario, seleccione **Abrir incidente**.
 - Si el incidente aún no se ha leído, seleccione **Marcar como leído**. De lo contrario, selecciona **Marcar como no leído**.

- Seleccione **Ignorar amenaza**. Los detalles de la amenaza se enumeran en el elemento de menú. Al seleccionar este elemento, se indica que la presencia de esta amenaza en particular en el host no es de interés. Por lo tanto, todos los incidentes en los que se detecta esta amenaza en este host se cerrarán automáticamente.
- Seleccione **Marcar el host <host> como limpio**. El sistema marcará el host implicado en el incidente como limpio. Como resultado, se cerrarán todos los incidentes en ese host.
- Al hacer clic en  **Ver detalles del incidente** se mostrará el contenido de la página **Perfil del incidente** en una nueva pestaña del navegador.
- Al hacer clic en **Administrar alerta** se iniciará la barra lateral **Administrar alerta**. Utilice esta función para suprimir o degradar los eventos inofensivos asociados con el incidente especificado, como los incidentes relacionados con la prueba del sistema o el bloqueo. Consulte [Trabajar con la barra lateral Administrar alerta](#) para obtener más información.
- Haga clic en  **Marcar como leído** para marcar el incidente. El botón cambia a **Marcar como no leído**, lo que le permite revertir el estado de lectura.

Resumen de incidentes

La sección superior proporciona una descripción general visual de la amenaza detectada y muestra su puntuación de impacto.

Detalles del incidente

El widget **Detalles del incidente** muestra información detallada de la red sobre el incidente. Incluye los siguientes datos.

Columna	Descripción
IP de origen	La dirección IP del origen del incidente. Haga clic en el icono  para ver la página Actividad del host . Haga clic en el icono  para ver el origen en la página Análisis de red .
Host de origen	Si está disponible, el FQDN del origen del incidente.
Eventos	El número de eventos que conforman este incidente.
Identificador de incidente	Un vínculo permanente a la página Perfil del incidente . El enlace se abrirá en una nueva pestaña/ventana del navegador.
ID de campaña	Un vínculo permanente a la página de campañas. El enlace se abre en una nueva pestaña del navegador.
Impacto	La puntuación de impacto aplicada por el sistema a este incidente.
Hora de inicio	Una marca de tiempo para el comienzo del incidente.
Hora de finalización	Una marca de tiempo para el último evento registrado del incidente.
Estado	Muestra si se ha cerrado el incidente.

Evidencia

El widget **Evidencia** cuando se expande muestra la lista de eventos detectados por NSX Network Detection and Response.

Las columnas que se muestran en la lista se pueden personalizar haciendo clic en el icono .

Cada fila es un resumen de una entrada de evidencia e incluye las siguientes columnas.

Columna	Descripción
Primera detección	Marca de tiempo desde la primera vez que se detectó este evento.
Última detección	Marca de tiempo desde la última vez que se detectó este evento.
Amenaza	Nombre del riesgo de seguridad detectado.
Clase de amenaza	Nombre de la clase de riesgo de seguridad detectada.
Impacto	La puntuación de impacto aplicada a este incidente.
Evidencia	La categoría de evidencia de este incidente. El título del bloque de detalles de la evidencia se deriva del nombre de la categoría.
Asunto	El artefacto, normalmente un archivo, que se está analizando.
Referencia	Un vínculo permanente a la página del evento. El enlace se abre en una nueva pestaña del navegador.

Detalles de la evidencia

Haga clic en el icono (o en cualquier parte de una fila de entrada de incidente) para mostrar el bloque de detalles de la evidencia.

El título del bloque de detalles de la evidencia se deriva del tipo de evidencia. Por ejemplo, la evidencia de reputación.

En esta sección, se muestra información más detallada sobre la evidencia. Incluye los siguientes datos.

Datos	Descripción
Amenaza	Nombre del riesgo de seguridad detectado.
Clase de amenaza	Nombre de la clase de riesgo de seguridad detectada.
Impacto	La puntuación de impacto aplicada a este incidente.
Detector	Si aparece, mostrará el módulo de NSX Network Detection and Response que identificó la amenaza. Haga clic en el vínculo para ver la ventana emergente Detector. Consulte Ventana emergente de documentación del detector .
Ver el evento de red	Un vínculo permanente a la página del evento. El enlace se abre en una nueva pestaña del navegador.
Ver el evento de red	Un vínculo permanente a la página del evento. El enlace se abre en una nueva pestaña del navegador.
Primera detección	Marca de tiempo desde la primera vez que se detectó este evento.
Última detección	Marca de tiempo desde la última vez que se detectó este evento.

Datos	Descripción
Gravedad	Estimación del nivel de gravedad de la amenaza detectada. Por ejemplo, una conexión a un comando y un servidor de control se suele considerar una gravedad alta, ya que la conexión podría resultar dañada.
Confianza	Indica la probabilidad de que la amenaza individual detectada sea malintencionada. Dado que el sistema utiliza heurísticas avanzadas para detectar amenazas desconocidas, en algunos casos, la amenaza detectada puede tener un valor de confianza menor si el volumen de información disponible para esa amenaza específica es limitado.
Asunto	Si está presente, muestra el artefacto, por lo general, un archivo que se está analizando.

Consulte [Acerca de la evidencia](#) para obtener más información.

Trabajar con la página de archivos descargados

La página **Archivos descargados** proporciona pestañas que contienen información sobre los archivos que se descargaron en la red de NSX-T Data Center.

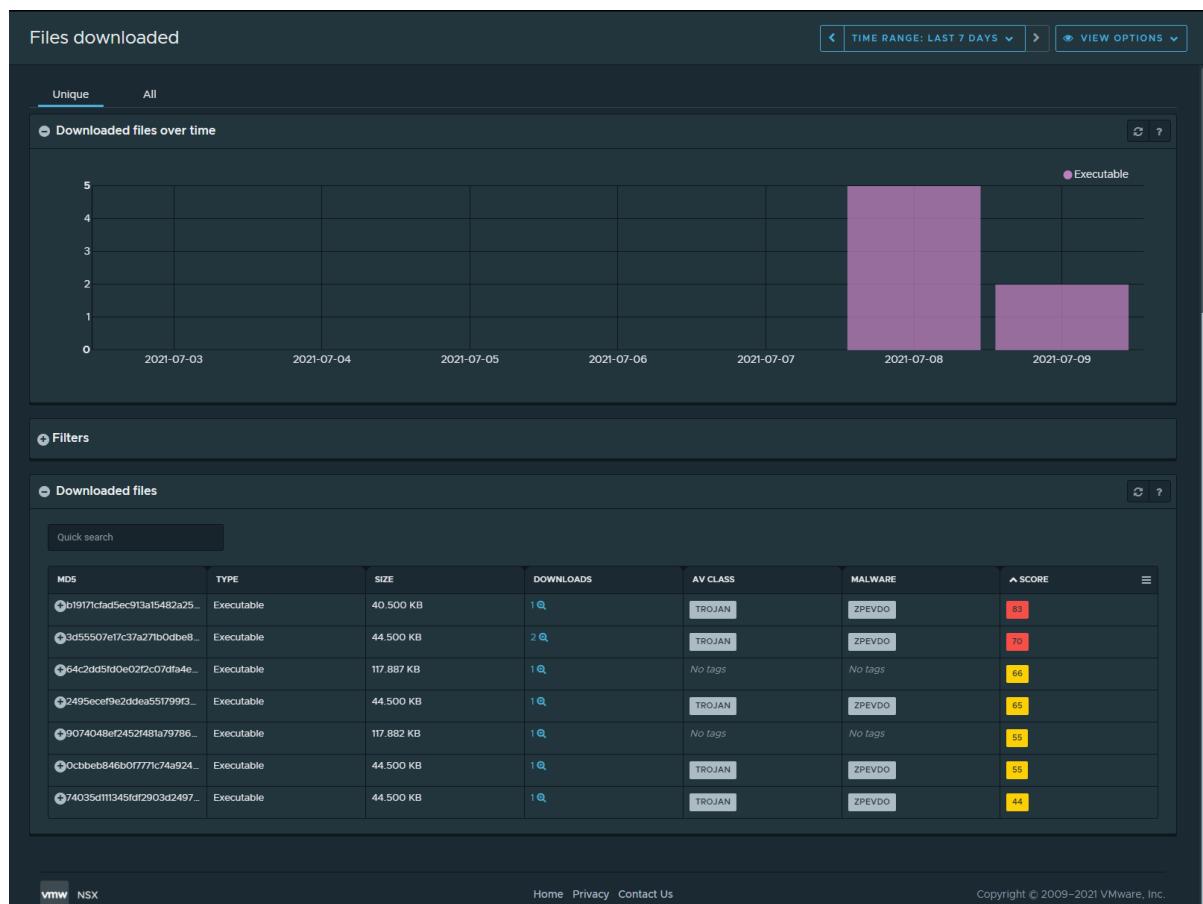
La página consta de varios widgets que se pueden administrar mediante la información incluida en [Introducción a la interfaz de usuario de NSX Network Detection and Response](#).

La página proporciona una vista de alto nivel de los números de archivos de diferentes tipos que se descargaron en la red. También le permite consultar los detalles de las descargas individuales, incluido el acceso a los informes completos del análisis realizado.

En esta página se muestran las siguientes pestañas.

- La pestaña **Único** muestra distintas descargas de archivos en la red analizada.
- La pestaña **Todo** muestra todas las instancias de descargas de archivos que NSX Network Detection and Response analizó en la red. Algunos de los archivos mostrados son repeticiones.

La siguiente imagen muestra un ejemplo de la página **Archivos descargados**.



Pestaña Único

La pestaña **Único** de la página **Archivos descargados** de NSX Network Detection and Response muestra distintas descargas de archivos en la red que se analizaron.

Archivos descargados a lo largo del tiempo

El widget **Archivos descargados** proporciona una descripción general del número de archivos que se descargaron en la red supervisada durante el intervalo de tiempo especificado. El gráfico es un histograma diario de archivos descargados, agrupados por el tipo de archivo de alto nivel.

El widget muestra solo las descargas de archivos distintas que se analizaron.

A continuación se muestran los tipos de archivo.

Tipo de archivo	Descripción
Archivo	Formatos de archivo, como ZIP o RAR.
Documento	Incluye otros tipos de documentos de Office.
Ejecutable	Formatos de aplicación binarios, como ejecutable portátil de Windows.
Java	Aplicación Java o applet.
Medio	Archivo Flash de macromedia (Adobe).

Tipo de archivo	Descripción
Otros	Otro formato de archivo reconocido.
PDF	Archivos de formato de documento portátiles.
Script	Un script ejecutable, como JavaScript, Python y otros.
Desconocido	Tipo de archivo desconocido.

Usar filtros en la página Archivos descargados

NSX Network Detection and Response proporciona un mecanismo de filtrado que le permite centrarse en información específica sobre los archivos descargados que le interesen. El uso de filtros es opcional.

Procedimiento

- 1 En la página **Archivos descargados**, haga clic en  para expandir el widget **Filtros**.
- 2 Haga clic en cualquier lugar del cuadro de texto **Filtra en** y seleccione un elemento en el menú desplegable.

Puede seleccionar entre los siguientes filtros disponibles. Para delimitar aún más el foco de la información que se muestra, puede combinar varios filtros.

Nombre de filtro	Descripción
Etiquetas de análisis	Restrinja los archivos mostrados por sus etiquetas de análisis. Se trata de etiquetas asignadas a un archivo o una URL por el análisis del sistema. Pueden identificar una amenaza o una clase de amenaza, o hacer referencia a comportamientos malintencionados específicos que se detectaron.
UUID de analista	Restrinja los archivos mostrados al UUID de análisis del sistema para el archivo descargado. Este es un identificador único interno para el análisis de un archivo.
Protocolo de aplicación	Restrinja los archivos mostrados transferidos a través de uno de los protocolos especificados. Los valores admitidos son HTTP/HTTPS, FTP y SMB.
IP contactada	Restrinja los archivos mostrados a la dirección IP desde la que se descargó el archivo. Al igual que el filtro IP de host, admite direcciones IP, bloques CIDR o rangos de direcciones IP.
Filtro de tipo de archivo	Restrinja los archivos mostrados a uno o varios tipos de archivos de alto nivel. Consulte la lista de tipos de archivo (anteriores).
Archivos	Seleccione Malintencionado para restringir los archivos mostrados a archivos malintencionados. Estos son archivos a los que el análisis del sistema les asignó una puntuación de 70 o más (de 100).
IP de host	Restrinja los archivos mostrados a la dirección IP del host en la red que descargó el archivo. Este filtro admite la selección de una o varias direcciones IP, bloques CIDR (por ejemplo, 192.168.0.0/24) o rangos de direcciones IP (por ejemplo, 192.168.1.5-192.168.1.9).
Host HTTP	Restrinja los archivos mostrados a los nombres de host desde los que se descargó el archivo. Nota Este valor se extrae del encabezado Host HTTP en la solicitud HTTP que descargó el archivo. Por lo tanto, está bajo el control del cliente y puede ser suplantado por un software malintencionado, como un archivo binario de malware que ya se ejecuta en un host infectado.

Nombre de filtro	Descripción
MD5	Restrinja los archivos mostrados al hash MD5 del archivo descargado.
Puntuación mínima	Restrinja los archivos mostrados a aquellos a los que el análisis del sistema haya asignado una puntuación mayor que el valor seleccionado (de 1 a 100).

- 3 Para aplicar los filtros seleccionados, haga clic en **Aplicar**.
- 4 (opcional) Para eliminar un filtro individual, haga clic en el botón **ELIMINAR-** junto a su entrada. Para eliminar todos los filtros seleccionados, haga clic en el icono **X** situado en el lado derecho del widget **Filtros**.

El widget **Filtros** se contrae al eliminar todos los filtros seleccionados.

Lista de archivos descargados únicos

La lista **Archivos descargados** muestra todos los archivos distintos que descargaron los hosts de la red y que procesó el servicio NSX Advanced Threat Prevention.

El cuadro de texto **Búsqueda rápida** en la esquina superior izquierda de la lista proporciona una capacidad de búsqueda rápida mientras introduce texto. Filtra las filas de la lista y muestra solo aquellas filas de cualquier columna que incluyan texto que coincide con la cadena de consulta que introdujo en el cuadro de texto de búsqueda.

Para personalizar las columnas que se muestran en la lista, haga clic en el  situado en la esquina superior derecha de la lista.

Puede personalizar el número de filas que se mostrarán. El valor predeterminado es 20 entradas. Utilice los iconos  y  para desplazarse por varias páginas.

Cada fila es un resumen de un archivo descargado. Haga clic en el icono  o en cualquier lugar de una fila de entrada para acceder a una vista detallada del archivo descargado.

La lista se ordena por puntuación e incluye las siguientes columnas.

Nombre de la columna	Descripción
MD5	El hash MD5 del archivo descargado.
Tipo	El tipo de archivo de alto nivel del archivo descargado. Los tipos admitidos actualmente son: <ul style="list-style-type: none"> ■ Archivo: formatos de archivo como ZIP o RAR ■ Documento: incluye otros tipos de documentos de Office ■ Ejecutable: formatos de aplicación binarios, como ejecutable portátil de Windows. ■ Java: aplicación Java o applet ■ Medios: archivo Flash de Macromedia (Adobe) ■ Otro: otro formato de archivo reconocido ■ PDF: archivos con formato de documento portátil ■ Script: un script ejecutable, como JavaScript, Python y otros. ■ Desconocido: tipo de archivo desconocido
Tamaño	Tamaño en bytes del archivo descargado.

Nombre de la columna	Descripción
Descargas	<p>Número de veces que los hosts de la red descargaron el archivo.</p> <p>El número mostrado y  proporcionan un vínculo a la página de descargas detallada. El vínculo pasa un filtro UUID de Analista que restringe la vista a las descargas de este archivo específico.</p>
Clase AV	<p>Etiqueta que define la clase de antivirus del archivo descargado. Si la etiqueta tiene un ícono , puede hacer clic en ese ícono para obtener una descripción en una ventana emergente.</p>
Malware	<p>Una etiqueta que define el tipo de malware del archivo descargado. Si la etiqueta tiene un ícono , puede hacer clic en ese ícono para obtener una descripción en una ventana emergente.</p>
Puntuación	<p>La puntuación asignada al archivo descargado por el análisis indica el nivel crítico de la amenaza detectada y oscila entre 0 y 100:</p> <ul style="list-style-type: none"> ■ Las amenazas con 70 o más se consideran críticas. ■ Las amenazas entre 30 y 69 se consideran de riesgo medio. ■ Las amenazas que se encuentran entre 1 y 29 se consideran benignas. <p>Para obtener más información sobre el núcleo de la malintencionaldad y la estimación de riesgo, consulte Informe de análisis: pestaña Descripción general.</p> <p>Si aparece el ícono , significa que el artefacto se bloqueó. La lista se ordena en orden descendente (las amenazas más críticas en la parte superior). Haga clic en  para ordenar la lista en orden creciente (las amenazas menos críticas en la parte superior), y haga clic en  para volver al orden predeterminado.</p>

Detalles de archivos descargados

La vista de detalles de los archivos descargados se expande dentro de la lista **Archivos descargados**.

Verá un subconjunto de los siguientes detalles disponibles, en función de la pestaña que haya seleccionado en la página **Archivos descargados**.

Nombre de detalle	Descripción
Informe de análisis	Haga clic en el vínculo o en el ícono  para ver el informe de análisis en una nueva pestaña.
Tipo de archivo	El tipo de alto nivel del archivo descargado. Consulte Archivos descargados a lo largo del tiempo para obtener la lista de tipos de archivo.
Detalles del tipo de archivo	Si está disponible, más detalles sobre el tipo de archivo. Por ejemplo, PE executable, application, 32-bit, Intel i386 O Zip archive data.
Nombre de archivo	Si está disponible, el nombre del archivo.
Descargado	<p>Por descargas únicas, la cantidad de veces que los hosts de la red descargaron el archivo.</p> <p>Haga clic en el número o en el ícono  para ver las descargas de archivos en la página de descargas. El vínculo pasa un filtro UUID de Analista que restringe la vista a las descargas del archivo específico.</p>
Descargado por	<p>Las direcciones IP de los hosts de la red que descargaron el archivo.</p> <p>Si está disponible, haga clic en  para ver la información de registro y otros datos sobre el host en Ventana emergente WHOIS.</p>

Nombre de detalle	Descripción
Dirección URL	La URL de la descarga del archivo. Esto es una cadena Unicode codificada en UTF-8.
Dirección URL	La URL sin formato de la descarga del archivo. Si hay caracteres que no son ASCII en la URL, esos caracteres, así como el propio carácter de barra diagonal inversa, tendrán codificación de barra diagonal inversa.
Protocolo	Protocolos de red utilizados para descargar el archivo. Uno de los siguientes: HTTP/HTTPS, FTP o SMB.
Descargado de	Dirección IP del host contactado. Si está disponible, haga clic en  para ver la información de registro y otros datos sobre el host en Ventana emergente WHOIS .
Host HTTP	Si está disponible, el nombre de dominio del host contactado. Este nombre puede derivarse de otros datos, incluida la dirección IP. Si está disponible, haga clic en  para ver la información de registro y otros datos sobre el host en Ventana emergente WHOIS .
Agente de usuario	La cadena del agente de usuario extraída de la solicitud HTTP/HTTPS.
Primera descarga	Para las descargas únicas, la marca de tiempo de la primera detección registrada de la descarga de archivos.
Última descarga	Para las descargas únicas, la marca de tiempo de la detección más reciente de la descarga de archivos.
Marca de tiempo	La marca de tiempo de la detección de la descarga del archivo.
Tamaño de archivo	Tamaño del archivo en bytes.
MD5	El hash MD5 del archivo descargado.
SHA1	El hash SHA1 del archivo descargado.
Estado de envío	Indica por qué el archivo descargado no se envió para un análisis completo. Por lo general, esto se debe a un filtrado previo u otros motivos. Coloque el mouse sobre el icono  para mostrar una ventana emergente con más detalles.
UUID de analista	El identificador único devuelto por el servicio NSX Advanced Threat Prevention después de procesar el archivo descargado.
Identificador de evento	Un vínculo al evento asociado para la descarga del archivo. Haga clic en el identificador o en  para ver el evento. Consulte Eventos de detección para obtener más información.

Descripción general del análisis

La sección Descripción general del análisis proporciona un resumen de los resultados del análisis de un archivo descargado por el servicio NSX Advanced Threat Prevention.

Para abrir el informe de análisis completo en una pestaña nueva, haga clic en . Consulte [Uso del informe Análisis](#).

Para descargar el archivo detectado en la máquina local, haga clic en  en el lado derecho de la pantalla. En el menú desplegable, seleccione **Descargar archivo** o **Descargar como ZIP**.

Si selecciona **Descargar como ZIP**, aparecerá la ventana emergente **Descargar archivo como zip** que le solicitará que proporcione una contraseña opcional para el archivo. Haga clic en **Descargar** para completar la descarga del archivo . ZIP.

Importante La aplicación NSX Network Detection and Response solo le permite descargar archivos detectados en determinadas condiciones.

Si el artefacto se considera de bajo riesgo, se mostrará  y podrá descargarlo en el equipo local.

Si el artefacto se considera peligroso, no se mostrará  a menos que la licencia tenga la capacidad `ALLOW_RISKY_ARTIFACT_DOWNLOADS`.

Debe tener en cuenta que el artefacto puede causar daños al abrirse.

Es posible que la interfaz NSX Network Detection and Response muestre la ventana emergente **Advertencia: descargando archivo malintencionado**. Haga clic en el botón **Acepto** para aceptar las condiciones y descargar el archivo.

En el caso de los artefactos malintencionados, encapsule el archivo en un archivo ZIP para evitar que otras soluciones que supervisan el tráfico inspeccionen automáticamente la amenaza.

Si no tiene la capacidad `ALLOW_RISKY_ARTIFACT_DOWNLOADS` y necesita poder descargar artefactos malintencionados, póngase en contacto con el servicio de soporte técnico de [VMware](#).

Haga clic en  y  para expandir y contraer las secciones de la pestaña.

La sección Descripción general del análisis proporciona un resumen de los resultados de análisis de un archivo o una URL analizados por el servicio NSX Advanced Threat Prevention. La sección muestra los siguientes datos.

- MD5: el hash MD5 del archivo. Para buscar otras instancias de este artefacto en la red, haga clic en <ícono de búsqueda>.
- SHA1: el hash SHA1 del archivo.
- SHA256 : el hash SHA256 del archivo.
- Tipo de MIME: la etiqueta utilizada para identificar el tipo de datos en el archivo.
- Envío: la marca de tiempo del envío

La sección Nivel de amenaza comienza con un resumen de los resultados del análisis: El hash md5 del archivo se determinó como malintencionado/benigno.

Después, muestra los siguientes datos:

Evaluación de riesgos

En esta sección se muestran los resultados de la evaluación de riesgos.

- Puntuación de malintencionalidad: establece una puntuación de 100.

- Estimación de riesgo: estimación del riesgo estimado por este artefacto.
 - Alto: este artefacto representa un riesgo crítico y debe abordarse con prioridad. Por lo general, estos asuntos son archivos o documentos de Internet que contienen vulnerabilidades de seguridad, lo que pone en peligro el sistema infectado. Los riesgos son múltiples: desde la pérdida de información hasta el fallo del sistema. Estos riesgos se infieren parcialmente del tipo de actividad detectada. El umbral de puntuación de esta categoría suele ser mayor que 70.
 - Medio: este artefacto representa un riesgo a largo plazo y debe supervisarse de cerca. Puede ser una página web que contiene contenido sospechoso, lo que podría provocar intentos de ataques drive-by. También pueden ser un adware o producto antivirus falso que no representa una amenaza grave inmediata, pero pueden causar problemas con el funcionamiento del sistema. El umbral de puntuación de esta categoría suele ser de 30 a 70.
 - Bajo: este artefacto se considera benigno y puede ignorarlo. El umbral de puntuación de esta categoría suele ser inferior a 30.
- Clase de antivirus: la clase de antivirus o malware a la que pertenece el artefacto. Por ejemplo, troyanos, gusanos, adware, ransomware, spyware, etc.
- Familia de antivirus: la familia de antivirus o malware a la que pertenece el artefacto. Por ejemplo, valyria, darkside, etc. Para buscar otras instancias de esta familia, haga clic en el ícono de búsqueda.

Descripción general del análisis

La información que se muestra se ordena por gravedad e incluye las siguientes propiedades:

- Gravedad: una puntuación entre 0 y 100 de la malintencionaldad de las actividades detectadas durante el análisis del artefacto. Los iconos adicionales indican los sistemas operativos que pueden ejecutar el artefacto.
- Tipo: los tipos de actividades detectados durante el análisis del artefacto. Estos tipos incluyen:
 - Inicio automático: capacidad para reiniciar después de apagar una máquina.
 - Deshabilitar: capacidad para deshabilitar componentes críticos del sistema.
 - Evasión: capacidad para evadir el entorno de análisis.
 - Archivo: actividad sospechosa en el sistema de archivos.
 - Memoria: actividad sospechosa dentro de la memoria del sistema.
 - Red: actividad sospechosa en el nivel de red.
 - Reputación: origen conocido o firmado por una organización de reputación.
 - Configuración: capacidad para alterar permanentemente los ajustes críticos del sistema.
 - Firma: identificación de asunto malintencionado.

- Robo: capacidad para acceder a información confidencial y potencialmente filtrada.
- Invisible: capacidad para permanecer inadvertido por parte de los usuarios.
- Silenciado: identificación del sujeto benigno.
- Descripción: una descripción correspondiente a cada tipo de actividad detectada durante el análisis del artefacto.
- Tácticas de ATT&CK: la etapa o etapas de un ataque ATT&CK de MITRE. Varias tácticas están separadas por comas.
- Técnicas de ATT&CK: las acciones o herramientas observadas que puede utilizar un actor malintencionado. Varias técnicas están separadas por comas.
- Vínculos: para buscar otras instancias de esta actividad, haga clic en el icono de búsqueda.

Artefactos adicionales

En esta sección se enumeran los artefactos adicionales (archivos y URL) que se observaron durante el análisis de la muestra enviada y que, a su vez, se enviaron para un análisis detallado. Esta sección incluye las siguientes propiedades:

- Descripción: Describe el artefacto adicional.
- SHA1: el hash SHA1 del artefacto adicional.
- Tipo de contenido: el tipo MIME del artefacto adicional.
- Puntuación: la puntuación de malintencionaldad del artefacto adicional. Para ver el informe de análisis asociado, haga clic en .

Argumentos de la línea de comandos descodificados

Si se ejecutó algún script de PowerShell durante el análisis, el sistema los descodifica, lo que hace que sus argumentos estén disponibles en un formato más legible.

Herramientas de terceros

Un vínculo a un informe sobre el artefacto en el portal VirusTotal.

Pestaña Todo

La pestaña **Todo** muestra todas las instancias de las descargas de archivos analizadas en su red de NSX-T Data Center.

Archivos descargados a lo largo del tiempo en la pestaña Todo

El widget **Archivos descargados** de la pestaña **Todo** proporciona una descripción general del número de archivos que se descargaron en la red supervisada durante el intervalo de tiempo especificado. El gráfico es un histograma diario de archivos descargados, agrupados por el tipo de archivo de alto nivel.

El widget muestra todas las descargas de archivos analizadas.

Consulte [Archivos descargados a lo largo del tiempo](#) para obtener la lista de tipos de archivo.

Usar filtros en la página Archivos descargados

NSX Network Detection and Response proporciona un mecanismo de filtrado que le permite centrarse en información específica sobre los archivos descargados que le interesen. El uso de filtros es opcional.

Procedimiento

- 1 En la página **Archivos descargados**, haga clic en  para expandir el widget **Filtros**.
- 2 Haga clic en cualquier lugar del cuadro de texto **Filtra en** y seleccione un elemento en el menú desplegable.

Puede seleccionar entre los siguientes filtros disponibles. Para delimitar aún más el foco de la información que se muestra, puede combinar varios filtros.

Nombre de filtro	Descripción
Etiquetas de análisis	Restrinja los archivos mostrados por sus etiquetas de análisis. Se trata de etiquetas asignadas a un archivo o una URL por el análisis del sistema. Pueden identificar una amenaza o una clase de amenaza, o hacer referencia a comportamientos malintencionados específicos que se detectaron.
UUID de analista	Restrinja los archivos mostrados al UUID de análisis del sistema para el archivo descargado. Este es un identificador único interno para el análisis de un archivo.
Protocolo de aplicación	Restrinja los archivos mostrados transferidos a través de uno de los protocolos especificados. Los valores admitidos son HTTP/HTTPS, FTP y SMB.
IP contactada	Restrinja los archivos mostrados a la dirección IP desde la que se descargó el archivo. Al igual que el filtro IP de host, admite direcciones IP, bloques CIDR o rangos de direcciones IP.
Filtro de tipo de archivo	Restrinja los archivos mostrados a uno o varios tipos de archivos de alto nivel. Consulte la lista de tipos de archivo (anteriores).
Archivos	Seleccione Malintencionado para restringir los archivos mostrados a archivos malintencionados. Estos son archivos a los que el análisis del sistema les asignó una puntuación de 70 o más (de 100).
IP de host	Restrinja los archivos mostrados a la dirección IP del host en la red que descargó el archivo. Este filtro admite la selección de una o varias direcciones IP, bloques CIDR (por ejemplo, 192.168.0.0/24) o rangos de direcciones IP (por ejemplo, 192.168.1.5-192.168.1.9).
Host HTTP	Restrinja los archivos mostrados a los nombres de host desde los que se descargó el archivo. Nota Este valor se extrae del encabezado Host HTTP en la solicitud HTTP que descargó el archivo. Por lo tanto, está bajo el control del cliente y puede ser suplantado por un software malintencionado, como un archivo binario de malware que ya se ejecuta en un host infectado.
MD5	Restrinja los archivos mostrados al hash MD5 del archivo descargado.
Puntuación mínima	Restrinja los archivos mostrados a aquellos a los que el análisis del sistema haya asignado una puntuación mayor que el valor seleccionado (de 1 a 100).

- 3 Para aplicar los filtros seleccionados, haga clic en **Aplicar**.

- 4 (opcional) Para eliminar un filtro individual, haga clic en el botón **ELIMINAR**– junto a su entrada. Para eliminar todos los filtros seleccionados, haga clic en el icono **X** situado en el lado derecho del widget **Filtros**.

El widget **Filtros** se contrae al eliminar todos los filtros seleccionados.

Lista de archivos descargados en la pestaña Todos

La lista **Archivos descargados** muestra todos los archivos que descargaron los hosts de la red y que procesó el servicio NSX Advanced Threat Prevention.

El cuadro de texto **Búsqueda rápida** en la esquina superior izquierda de la lista proporciona una capacidad de búsqueda rápida mientras introduce texto. Filtra las filas de la lista y muestra solo aquellas filas de cualquier columna que incluyan texto que coincida con la cadena de consulta que introdujo en el cuadro de texto de búsqueda.

Para personalizar las columnas que se muestran en la lista, haga clic en el  situado en la esquina superior derecha de la lista.

Puede personalizar el número de filas que se mostrarán. El valor predeterminado es 20 entradas. Utilice los iconos  y  para desplazarse por varias páginas.

Cada fila es un resumen de un archivo descargado. Haga clic en el icono  o en cualquier lugar de una fila de entrada para acceder a una vista detallada del archivo descargado.

Consulte [Detalles de archivos descargados](#) para obtener más información sobre la vista detallada del archivo descargado.

La lista se ordena por la información de marca de tiempo e incluye las siguientes columnas.

Nombre de la columna	Descripción
Marca de tiempo	La marca de tiempo de la detección de la descarga del archivo.
Host	El host que descargó el archivo.
IP contactada	Dirección IP del host contactado.
Ubicación	Para una descarga, esta es la dirección URL del archivo en el formato admitido. Por ejemplo, <code>\\\127.0.0.2\share\1128dedb.exe</code> para una descarga de SMB o <code>http://www.example.com/download/example.zip</code> para una descarga HTTP. Para una carga, se muestra "Carga".
MD5	El hash MD5 del archivo descargado.
Tipo	El tipo de alto nivel del archivo descargado. Consulte la Archivos descargados a lo largo del tiempo para obtener la lista de tipos de archivo.
Clase AV	Etiqueta que define la clase de antivirus del archivo descargado. Si la etiqueta tiene el icono  , puede hacer clic en esa etiqueta para obtener una descripción emergente.

Nombre de la columna	Descripción
Malware	Una etiqueta que define el tipo de malware del archivo descargado. Si la etiqueta tiene el icono  , puede hacer clic en esa etiqueta para obtener una descripción emergente.
Puntuación	La puntuación asignada al archivo descargado por el análisis de NSX Intelligence. Haga clic en  para ordenar la lista por puntuación. Si aparece  significa que el artefacto se bloqueó.

Uso de la página de administración de alertas

La página **Administración de alertas** muestra las reglas para administrar alertas en NSX Network Detection and Response.

NSX Network Detection and Response busca coincidencias entre los eventos y los filtros definidos por el usuario contenidos en estas reglas. Los eventos coincidentes se convierten en eventos **INFO** (Degradar) en la interfaz de usuario de NSX Network Detection and Response, se eliminan o se les asigna un valor de impacto personalizado en función de la acción seleccionada.

La lista **Reglas personalizadas** define las reglas de alerta.

El cuadro de texto de búsqueda rápida que aparece sobre la lista proporciona la función de búsqueda tal como se introduce. Filtra las filas de la lista, mostrando solo aquellas filas que tienen texto, en cualquier columna, que coincide con la cadena de consulta.

Haga clic en  en el lado derecho de la página para agregar una nueva regla de alerta. Se muestra la barra lateral **Administrar alerta**. Consulte [Trabajar con la barra lateral Administrar alerta](#) para obtener información detallada.

Puede personalizar el número de filas que se mostrarán. El valor predeterminado es 25 entradas. Para desplazarse por varias páginas, utilice los iconos de paginación.

La lista se ordena por la columna Última modificación e incluye la siguiente información.

Nombre de la columna	Descripción
Nombre de regla	El nombre de la regla de alerta. Para ordenar la lista por nombre de regla, haga clic en  en el encabezado de la lista.
Expresión	La expresión coincidente de la regla es un número de filtros que se comparan con los eventos. La expresión puede truncarse si es demasiado larga. Expanda la fila para mostrar todo el contenido de la regla haciendo clic en  o en cualquier lugar de la fila de entrada. Para ordenar la lista por expresión, haga clic en  en el encabezado de la lista.

Nombre de la columna	Descripción
Acción de regla	<p>La acción de regla define qué hacer con un evento que coincide con la expresión: <code>demote</code> el evento a <code>INFO</code>, <code>suppress</code> el evento, o asignar un valor de <code>impact</code> personalizado de 1 a 100. La acción puede truncarse si es demasiado larga. Expanda la fila para mostrar todo el contenido de la regla haciendo clic en icono (o en cualquier lugar de la fila de entrada).</p> <p>El nombre de la regla se anexa a la acción como una etiqueta personalizada, por ejemplo, <code>tag:network_event=rule_name</code>.</p> <p>Para ordenar la lista por acción de regla, haga clic en  en el encabezado de la lista.</p>
Última modificación	La fecha y la hora de la última modificación de la regla.
Acciones	<p>Para ver o editar la regla, haga clic en . La barra lateral Administrar alerta se muestra para que pueda ver o realizar cambios en la regla.</p> <p>Para eliminar la regla, haga clic en .</p>

Trabajar con la barra lateral Administrar alerta

La barra lateral **Administrar alerta** permite crear una regla que coincida con todos los eventos subsiguientes detectados por NSX Network Detection and Response. Cuando un evento coincide con una regla, se aplica la acción de la regla.

Acceder a la barra lateral

Puede acceder a la barra lateral **Administrar alerta** de una de las siguientes formas.

- En cualquier pestaña de la página **Perfil de host**, haga clic en el botón **Acciones de host** y, a continuación, seleccione Administrar alerta en el menú desplegable. A continuación, el panel de la barra lateral, se rellena automáticamente con los filtros pertinentes. Puede editar estas entradas.
- Haga clic en la pestaña **Amenazas** en la página **Perfil de host**. En una tarjeta de amenazas, haga clic en **Próximos pasos** y seleccione **Administrar alerta** en el menú desplegable.
- En la vista **Detalles del incidente**, seleccione un incidente específico y haga clic en **Administrar alerta**.
- En la página **Administración de alertas**, haga clic en  en el widget **Administración de alertas**,

La barra lateral **Administrar alerta** consta de tres paneles independientes: FILTROS, ACCIONES y REVISAR REGLA. Cada panel se muestra en función de en qué paso de Crear regla o Editar regla se encuentre actualmente.

Para cerrar la barra lateral **Administrar alerta** haga clic en la **X** situada en la esquina superior derecha. Si realizó cambios, debe confirmar el cierre de la barra lateral.

Para crear o editar una regla, debe realizar tres pasos en la barra lateral **Administrar alerta**.

Paso 1: Crear o editar filtros

La pestaña **Filtros** tiene dos modos de edición que puede utilizar al trabajar con filtros: Básico (valor predeterminado) y Avanzado. Puede crear o editar filtros en cualquiera de los modos.

- Para cambiar el modo Crear/Editar al modo Avanzado, haga clic en la pestaña **Avanzado** en la parte superior de la barra lateral.
- Para volver al modo Básico, haga clic en la pestaña **Básico** (pero consulte la [nota Importante](#)).

Para crear un filtro en modo básico, realice los siguientes pasos.

- 1 Haga clic en **Agregar un nuevo filtro+**.
- 2 Seleccione un filtro en el menú desplegable de entradas de filtro.

Los filtros se agrupan en cuatro categorías: Origen, URL, Detección y Archivo. Consulte la sección de entradas de atributos en [Sintaxis de reglas de alerta](#) para obtener más información sobre estas categorías.

- 3 Según el tipo de regla seleccionado, establezca su valor. Esto puede implicar hacer clic en una opción, introducir un valor, seleccionar un elemento de un menú desplegable u otros.

Para editar los filtros, desplácese por la lista, seleccione un filtro y modifique los valores adecuados. Elimine los filtros no deseados haciendo clic. También puede seleccionar más filtros.

Para crear filtros en modo Avanzado, rellene el cuadro de texto **Expresión coincidente** y agregue o edite un filtro con la sintaxis de las reglas de alerta. Por ejemplo,

```
(network_event.relevant_host_ip: 10.154.115.91 OR network_event.relevant_host_ip:
10.1.1.1-10.255.255.255) AND NOT
(network_event.server_port: 53 OR network_event.server_port: 65535) OR
(network_event.other_host_hostname: block.lastline.com) AND
(network_event.threat: Lastline blocking test)
```

Importante Por lo general, puede alternar entre los dos modos de edición de la barra lateral. Sin embargo, si el filtro de expresión coincidente que creó o editó no es compatible con el modo Básico, el vínculo **Básico** estará deshabilitado y la pestaña **FILTROS** se establecerá de forma predeterminada en el editor Avanzado.

Paso 2: Definir la acción

Después de definir o editar un filtro, para definir las acciones de la regla, haga clic en **Definir acciones** en la esquina inferior derecha. El panel **Acciones** tiene dos modos de edición: Acciones básicas (valor predeterminado) y Acciones avanzadas:

- Haga clic en la pestaña **Acciones avanzadas** en la parte superior de la barra lateral para cambiar el modo de creación/edición al modo Avanzado.
- Haga clic en el vínculo **Acciones básicas** para volver al modo básico.

Existen dos opciones en el panel **Acciones** en el modo de acciones básicas: **Administrador alerta** e **Impacto personalizado (1-100)**.

Suprimir acción

- 1 Haga clic en el botón de alternancia **Administrador alerta**.
- 2 Seleccione **Degradar a evento INFO** (valor predeterminado) o **Eliminar** en el menú desplegable.

La acción Degradar convierte los eventos de red subsiguientes que coincidan con la regla en eventos **INFO**. Tenga en cuenta que debe seleccionar **INFO** con el filtro Resultado del evento.

La acción Eliminar elimina los eventos coincidentes del portal del usuario.

Advertencia Ya no podrá acceder a los eventos que se eliminan.

Impacto personalizado

- 1 Haga clic en el botón de alternancia **Impacto personalizado (1-100)**.
- 2 Haga clic en los botones de opción para seleccionar **Rango definido** o **Valor único**. Si seleccionó **Rango definido**, introduzca los valores mínimo y máximo en los cuadros de texto correspondientes. Si seleccionó **Valor único**, introduzca el valor en el cuadro de texto.

También puede definir las acciones mediante el panel Acciones avanzadas.

- 1 Haga clic en la pestaña **Acciones avanzadas**.
- 2 En el cuadro de texto, agregue o edite una acción con la sintaxis de las reglas de alerta.

Por ejemplo:

```
demote:outcome=TEST
```

O

```
impact:min_impact=12,impact:max_impact=22
```

Después de seleccionar la acción, haga clic en **Revisar regla** para ir al siguiente paso.

Para corregir los filtros seleccionados, haga clic en **Filtros** para volver al panel **Filtros** anterior.

Paso 3: Revisar regla

El panel Revisar regla le permite verificar la regla de alerta.

- 1 En el cuadro de texto Nombre de regla, introduzca un nombre.
Si va a editar una regla existente, no puede cambiarle el nombre.
- 2 (Opcional) Utilice el menú desplegable para seleccionar una licencia.

Este menú desplegable estará deshabilitado si inició la barra lateral **Administrar alerta** desde la página **Administración de alertas** o si está editando una regla existente.

- 3 En la sección **Resumen de regla**, compruebe los filtros seleccionados que aparecen en la lista.

Si la pestaña **Filtros** se dejó en el modo Básico, el resumen consistirá en una lista de los filtros seleccionados. Cada filtro se muestra con su nombre y sus valores. Por ejemplo:

```
Rule summary
SERVER IP
12.6.6.6/32
RELEVANT HOST SILENCED
1
THREAT(S)
Torn rat
THREAT CLASS
Malicious file execution
```

Si la pestaña **Filtros** se dejó en modo Avanzado, el resumen mostrará la expresión coincidente. Por ejemplo:

```
Rule summary
(network_event.server_ip: 12.6.6.6/32) AND
(network_event.relevant_host_whitelisted: 1)
AND (network_event.threat: Torn RAT) AND
(network_event.threat_class: Malicious File
Execution)
```

Si la pestaña **Acciones** se dejó en modo Acciones básicas, el resumen mostrará la acción. Por ejemplo:

```
SUPPRESSION ALERT
Demote to INFO event
```

Si la pestaña **Acciones** se dejó en modo Acciones avanzadas, el resumen mostrará la acción. Por ejemplo:

```
ACTION
impact:min_impact=12,impact:max_impact=22
```

- 4 (Opcional) Para corregir los tipos de regla seleccionados, haga clic en **Editar regla** para volver a la página anterior.
- 5 Cuando haya terminado, haga clic en **Crear regla** para completar la regla o haga clic en **Actualizar regla** si va a editar una regla existente.

Sintaxis de reglas de alerta

Utilice la sintaxis de la regla de alerta para definir las acciones que debe realizar NSX Network Detection and Response cuando los eventos coinciden con un filtro.

Una regla de alerta consta de dos partes: Expresión coincidente y Acciones.

Expresión coincidente

Una combinación de cláusulas que expresan una condición en los atributos de un objeto.

Una expresión coincidente tiene el siguiente formato: `object_type . attribute_type:`

`[relation]value`

La expresión coincidente consta de las cuatro partes siguientes.

Nombre de la parte	Descripción
object_type	El tipo de objeto que debe coincidir. Se admite el siguiente tipo de registro: ■ network_event El tipo de objeto y su atributo están separados por un punto (.).
attribute_type	El atributo que debe coincidir (consulte Entradas de atributos). object_type.attribute_type se separa de [relation] y el valor con dos puntos (:).
[relation]	La relación entre el objeto y su atributo y el valor para el que debe coincidir. Si no se especifica ninguna relación, la igualdad será la predeterminada. Los tipos de relación admitidos son: ■ Igualdad (:) ■ Mayor o igual que (>, >=) ■ Menor o igual que (<, <=)
value	El valor que debe coincidir con object_type.attribute_type de los eventos entrantes.

Las expresiones coincidentes múltiples se separan por los operadores lógicos AND, OR y NOT.

Acciones

Una o varias modificaciones que se realizarán en el objeto.

Una acción tiene el siguiente formato: `action : target = value`

La acción consta de tres partes:

Nombre de la parte	Descripción
action	La acción que se realizará (consulte Acciones admitidas). La acción y su target se separan con dos puntos (:).
target	El destino admitido.
value	El valor opcional que se aplica al destino.

Las acciones múltiples están separadas por una coma (,) y se aplican en el mismo orden en que fueron definidas.

Entradas de atributos

En la siguiente lista se describen las diferentes entradas de atributos que puede utilizar al crear o actualizar nuevos filtros. Los atributos se agrupan en las siguientes cinco categorías.

ORIGEN

Atributo de origen	Descripción
client_ip	Coincide con una dirección IP o un rango de direcciones IP. El valor de la dirección debe ser una coincidencia exacta. (network_event.client_ip: 142.42.1.6/24)
other_host_hostname	Coincide con el nombre de host del otro host asociado al evento. Se admiten comparaciones con comodines: * para caracteres múltiples, ? para caracteres simples. Debe aplicar escape (\) a los caracteres comodín para que coincidan con un * o un ? literal. (network_event.other_host_hostname: host.example.com)
other_host_in_homenet	Si es true, coincide si la dirección IP del otro host asociado con el evento se encuentra en la red de inicio. Espera un valor booleano. (network_event.other_host_in_homenet: false)
other_host_ip	Coincide con una dirección IP o un rango de direcciones IP. El valor de la dirección debe ser una coincidencia exacta. (network_event.other_host_ip: 10.10.4.2)
other_host_tag	Coincide con una etiqueta de host. Seleccione una etiqueta de host existente. (network_event.other_host_tag: tag)
relevant_host_in_homenet	Si es true, coincide si la dirección IP del host relevante asociado con el evento se encuentra en la red de inicio. Espera un valor booleano. (network_event.relevant_host_in_homenet: true)
relevant_host_ip	Coincide con una dirección IP o un rango de direcciones IP. El valor de la dirección debe ser una coincidencia exacta. (network_event.relevant_host_ip: 42.6.7.0/16)
relevant_host_tag	Coincide con una etiqueta de host. Seleccione una etiqueta de host existente. (network_event.relevant_host_tag: tag)
relevant_host_whitelisted	Coincide con la dirección IP de origen silenciada. Espera un valor booleano. (network_event.relevant_host_whitelisted: true)
server_ip	Coincide con una dirección IP o un rango de direcciones IP. El valor de la dirección debe ser una coincidencia exacta. (network_event.server_ip: 12.6.6.6)
server_port	Coincide con un número de puerto. Se realizan comparaciones de enteros: equality, inequality, greater-than, less-than, etc. (network_event.server_port: 7777)
transport_protocol	Coincide con "TCP" o "UDP". (network_event.transport_protocol: UDP)

Dirección URL

Atributo de URL	Descripción
full_url	Coincide con al menos una URL en el evento. Se admiten comparaciones con comodines: * para caracteres múltiples, ? para caracteres simples. Debe aplicar escape (\) a los caracteres comodín para que coincidan con un * o un ? literal. Por ejemplo, el carácter de cadena de consulta ? debe tener carácter de escape (\?): (network_event.full_url: https://www.example.com/resource/path\?r=start&v=cK5G8fPmWeA)
normalized_url	Coincide con al menos una URL normalizada (una URL sin la cadena de consulta) en el evento. Se admiten comparaciones con comodines: * para caracteres múltiples, ? para caracteres simples. Debe aplicar escape (\) a los caracteres comodín para que coincidan con un * o un ? literal. (network_event.normalized_url: https://www.example.com/resource/path/)
resource_path	Coincide con al menos una ruta de recurso de URL en el evento. Se admiten comparaciones con comodines: * para caracteres múltiples, ? para caracteres simples. Debe aplicar escape (\) a los caracteres comodín para que coincidan con un * o un ? literal.

DETECTION

Atributo de detección	Descripción
custom_ids_rule_id	Coincide con un identificador de una regla de IDS. El valor numérico debe ser una coincidencia exacta. (network_event.custom_ids_rule_id: 987654321)
detector	Coincide con el nombre o el identificador único del módulo que detectó el evento. El valor de la cadena debe ser una coincidencia exacta. (network_event.detector: llrules:1532130206460)
event_outcome	Coincide con "DETECTION" o "INFO". (network_event.event_outcome: DETECTION)
event_type	Coincide con uno de los siguientes elementos: "BINARYDOWNLOAD", "DNS", "DNSANOMALY", "DYNAMICIP", "HTTPPANOMALY", "IDS", "IP", "LLANTARULE", "NETFLOW", "NETFLOWANOMALY", "NETWORK", "TLSANOMALY" o "URL". (network_event.event_type: IDS)
llanta_rule_uuid	Coincide con el UUID de una regla del sistema. El valor numérico debe ser una coincidencia exacta. (network_event.llanta_rule_uuid: b579caec719415cb04f925f8f187cb0)
operation	Coincide con una de las opciones "BLOCK", "INFO", "LOG" o "TEST". (network_event.operation: BLOCK)
threat	Coincide con una cadena válida que define una amenaza. Se admiten comparaciones con comodines: * para caracteres múltiples, ? para caracteres simples. Debe aplicar escape (\) a los caracteres comodín para que coincidan con un * o un ? literal. (network_event.threat: Torn RAT)
threat_class	Coincide con una clase de amenaza. El valor de la cadena debe ser una coincidencia exacta. (network_event.threat_class: Malicious File Execution)

FILE

Atributo de archivo	Descripción
av_class	Coincide con al menos una etiqueta de análisis av_class. El valor de la cadena debe ser una coincidencia exacta. (network_event.av_class: exploit)
file_category	Coincide con una de las categorías compatibles de archivos. El valor de la cadena debe ser una coincidencia exacta. (network_event.file_category: Java)
file_md5	Coincide con una suma MD5 válida. (network_event.file_md5: bb4f64ddfb8704d2bf69b0216be7f837)
file_sha1	Coincide con una suma de SHA1 válida. (network_event.file_sha1: c3e266ede7f6fec7a021a4ae0edf248848d5ae06)
file_size	Coincide con un tamaño de archivo en bytes. Debe ser un entero válido. Se realizan comparaciones de enteros: equality, inequality, greater-than, less-than, etc. (network_event.file_size: > 1042249837)
file_type	Coincide con una cadena válida que define un tipo de archivo. Se admiten comparaciones con comodines: * para caracteres múltiples, ? para caracteres simples. Debe aplicar escape (\) a los caracteres comodín para que coincidan con un * o un ? literal. (network_event.file_type: ?xecutable)
malware	Coincide con al menos una etiqueta de análisis av_family o lastline_malware. El valor de la cadena debe ser una coincidencia exacta. (network_event.malware: emotet)
malware_activity	Coincide con al menos una etiqueta de análisis de actividad. El valor de la cadena debe ser una coincidencia exacta. (network_event.malware_activity: Execution: Spawning Powershell with too many parameters)

OTRO

Nombre de otro atributo	Descripción
custom_tag	Coincide con una etiqueta definida por el usuario asignada a eventos. El valor de la cadena debe ser una coincidencia exacta. (network_event.custom_tag: tagged_event)

Acciones admitidas

Las siguientes son las acciones que puede utilizar al definir reglas.

Nombre de acción	Descripción
demote	Degrada el resultado del evento coincidente a un modo diferente. Destinos admitidos: <code>outcome</code> . Valores permitidos: "INFO" o "TEST".
impact	Establezca un límite inferior o superior sobre el impacto de un evento. Destinos admitidos: <ul style="list-style-type: none">■ <code>impact</code>: establece el límite inferior y superior en el mismo valor.■ <code>max_impact</code>: establece el límite superior en <code>impact</code>. Menor o igual al valor.■ <code>min_impact</code>: establece el límite inferior en <code>impact</code>. Mayor o igual que el valor. Valores permitidos: un número entero entre 1 y 100.
suppress	Suprime todas las amenazas en el evento coincidente. Esto hace que se puntúe como un falso positivo con un impacto de cero (0), lo que elimina el evento de forma efectiva. Destinos admitidos: <code>network_event</code> . Valores permitidos: ninguno.
tag	Asigne una etiqueta definida por el usuario al evento coincidente. Destinos admitidos: <code>network_event</code> . Valores permitidos: una cadena válida.

Uso del informe Análisis

El informe de análisis producido por NSX Network Detection and Response contiene los resultados detallados de un análisis realizado por el servicio NSX Advanced Threat Prevention en un archivo enviado.

Además de la puntuación de malintencionaldad, el informe también contiene información importante sobre la actividad del asunto del análisis. La actividad descrita constituye la base de la evaluación y la puntuación de amenazas de NSX Network Detection and Response.

El informe de análisis se inicia en la pestaña **Descripción general**.

Informe de análisis: pestaña Descripción general

La pestaña **Descripción general** de la página **Informe del análisis** de la interfaz de usuario de NSX Network Detection and Response proporciona un resumen de los resultados del análisis del archivo analizado por el servicio NSX Advanced Threat Prevention.

Para descargar el archivo detectado en la máquina local, haga clic en  en el lado derecho de la pantalla. En el menú desplegable, seleccione **Descargar archivo** o **Descargar como ZIP**.

Si selecciona **Descargar como ZIP**, aparecerá la ventana emergente **Descargar archivo como zip** que le solicitará que proporcione una contraseña opcional para el archivo. Haga clic en **Descargar** para completar la descarga del archivo . ZIP.

Importante La aplicación NSX Network Detection and Response solo le permite descargar archivos detectados en determinadas condiciones.

Si el artefacto se considera de bajo riesgo, se mostrará  y podrá descargarlo en el equipo local.

Si el artefacto se considera peligroso, no se mostrará  a menos que la licencia tenga la capacidad `ALLOW_RISKY_ARTIFACT_DOWNLOADS`.

Debe tener en cuenta que el artefacto puede causar daños al abrirse.

Es posible que la interfaz NSX Network Detection and Response muestre la ventana emergente **Advertencia: descargando archivo malintencionado**. Haga clic en el botón **Acepto** para aceptar las condiciones y descargar el archivo.

En el caso de los artefactos malintencionados, encapsule el archivo en un archivo ZIP para evitar que otras soluciones que supervisan el tráfico inspeccionen automáticamente la amenaza.

Si no tiene la capacidad `ALLOW_RISKY_ARTIFACT_DOWNLOADS` y necesita poder descargar artefactos malintencionados, póngase en contacto con el servicio de soporte técnico de [VMware](#).

Sección Descripción general del análisis

Nota Si el servicio NSX Advanced Threat Prevention encontró errores durante el análisis del archivo, se mostrará un bloque resaltado. Contiene una lista de los errores detectados.

La sección Descripción general del análisis proporciona un resumen de los resultados de análisis de un archivo o una URL analizados por el servicio NSX Advanced Threat Prevention. La sección muestra los siguientes datos.

- MD5: el hash MD5 del archivo. Para buscar otras instancias de este artefacto en la red, haga clic en <ícono de búsqueda>.
- SHA1: el hash SHA1 del archivo.
- SHA256 : el hash SHA256 del archivo.
- Tipo de MIME: la etiqueta utilizada para identificar el tipo de datos en el archivo.
- Envío: la marca de tiempo del envío

Sección de nivel de amenaza

La sección Nivel de amenaza comienza con un resumen de los resultados del análisis: El hash md5 del archivo se determinó como malintencionado/benigno.

Después, muestra los siguientes datos:

Evaluación de riesgos

En esta sección se muestran los resultados de la evaluación de riesgos.

- Puntuación de malintencionalidad: establece una puntuación de 100.
- Estimación de riesgo: estimación del riesgo estimado por este artefacto.
 - Alto: este artefacto representa un riesgo crítico y debe abordarse con prioridad. Por lo general, estos asuntos son archivos o documentos de Internet que contienen vulnerabilidades de seguridad, lo que pone en peligro el sistema infectado. Los riesgos son múltiples: desde la pérdida de información hasta el fallo del sistema. Estos riesgos se infieren parcialmente del tipo de actividad detectada. El umbral de puntuación de esta categoría suele ser mayor que 70.
 - Medio: este artefacto representa un riesgo a largo plazo y debe supervisarse de cerca. Puede ser una página web que contiene contenido sospechoso, lo que podría provocar intentos de ataques drive-by. También pueden ser un adware o producto antivirus falso que no representa una amenaza grave inmediata, pero pueden causar problemas con el funcionamiento del sistema. El umbral de puntuación de esta categoría suele ser de 30 a 70.
 - Bajo: este artefacto se considera benigno y puede ignorarlo. El umbral de puntuación de esta categoría suele ser inferior a 30.
- Clase de antivirus: la clase de antivirus o malware a la que pertenece el artefacto. Por ejemplo, troyanos, gusanos, adware, ransomware, spyware, etc.
- Familia de antivirus: la familia de antivirus o malware a la que pertenece el artefacto. Por ejemplo, valyria, darkside, etc. Para buscar otras instancias de esta familia, haga clic en el ícono de búsqueda.

Descripción general del análisis

La información que se muestra se ordena por gravedad e incluye las siguientes propiedades:

- Gravedad: una puntuación entre 0 y 100 de la malintencionalidad de las actividades detectadas durante el análisis del artefacto. Los iconos adicionales indican los sistemas operativos que pueden ejecutar el artefacto.
- Tipo: los tipos de actividades detectados durante el análisis del artefacto. Estos tipos incluyen:
 - Inicio automático: capacidad para reiniciar después de apagar una máquina.
 - Deshabilitar: capacidad para deshabilitar componentes críticos del sistema.
 - Evasión: capacidad para evadir el entorno de análisis.
 - Archivo: actividad sospechosa en el sistema de archivos.
 - Memoria: actividad sospechosa dentro de la memoria del sistema.
 - Red: actividad sospechosa en el nivel de red.
 - Reputación: origen conocido o firmado por una organización de reputación.

- Configuración: capacidad para alterar permanentemente los ajustes críticos del sistema.
- Firma: identificación de asunto malintencionado.
- Robo: capacidad para acceder a información confidencial y potencialmente filtrada.
- Invisible: capacidad para permanecer inadvertido por parte de los usuarios.
- Silenciado: identificación del sujeto benigno.
- Descripción: una descripción correspondiente a cada tipo de actividad detectada durante el análisis del artefacto.
- Tácticas de ATT&CK: la etapa o etapas de un ataque ATT&CK de MITRE. Varias tácticas están separadas por comas.
- Técnicas de ATT&CK: las acciones o herramientas observadas que puede utilizar un actor malintencionado. Varias técnicas están separadas por comas.
- Vínculos: para buscar otras instancias de esta actividad, haga clic en el icono de búsqueda.

Artefactos adicionales

En esta sección se enumeran los artefactos adicionales (archivos y URL) que se observaron durante el análisis de la muestra enviada y que, a su vez, se enviaron para un análisis detallado. Esta sección incluye las siguientes propiedades:

- Descripción: Describe el artefacto adicional.
- SHA1: el hash SHA1 del artefacto adicional.
- Tipo de contenido: el tipo MIME del artefacto adicional.
- Puntuación: la puntuación de malintencionalidad del artefacto adicional. Para ver el informe de análisis asociado, haga clic en .

Argumentos de la línea de comandos descodificados

Si se ejecutó algún script de PowerShell durante el análisis, el sistema los descodifica, lo que hace que sus argumentos estén disponibles en un formato más legible.

Herramientas de terceros

Un vínculo a un informe sobre el artefacto en el portal VirusTotal.

Informe de análisis: pestaña Informe

La información que se muestra en la pestaña **Informe** cambia en función del tipo de archivo analizado por NSX Network Detection and Response.

Para ver un informe, haga clic en la flecha hacia abajo de la pestaña **Informe** y seleccione uno de los informes disponibles.

Haga clic en  y  para expandir y contraer las secciones de la pestaña.

Sección de información de análisis

La sección **Información de análisis** contiene información clave sobre el análisis al que hace referencia el informe actual:

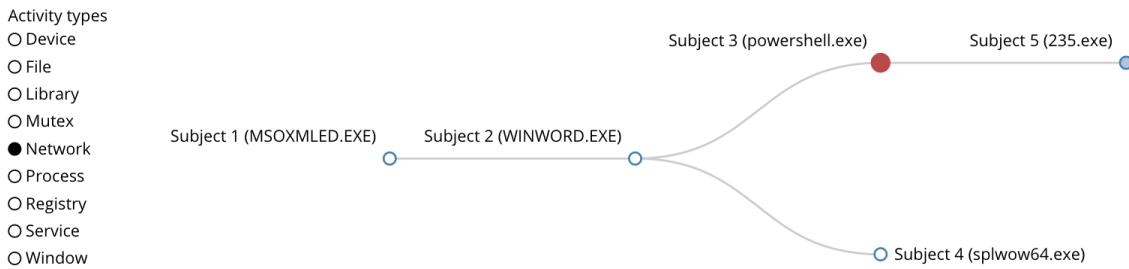
- Asunto de análisis: el hash MD5 del archivo.
- Tipo de análisis: tipo de análisis realizado:
 - Análisis dinámico en Microsoft Windows 10: el servicio de NSX Advanced Threat Prevention ejecutó el asunto de análisis en un entorno simulado de Windows 10 mediante el espacio aislado NSX Network Detection and Response. El sistema supervisa el comportamiento de los archivos y sus interacciones con el sistema operativo en busca de indicadores sospechosos o malintencionados.
 - Análisis dinámico en Microsoft Windows 7: el servicio de NSX Advanced Threat Prevention ejecutó el asunto de análisis en un entorno simulado de Windows 7 mediante el espacio aislado NSX Network Detection and Response. El sistema supervisa el comportamiento de los archivos y sus interacciones con el sistema operativo en busca de indicadores sospechosos o malintencionados.
 - Análisis dinámico en el navegador Chrome instrumentado: el servicio de NSX Advanced Threat Prevention inspeccionó el asunto del análisis (como un archivo HTML o una URL) mediante el navegador instrumentado, que está basado en Google Chrome. El navegador instrumentado reproduce de forma intencionada el comportamiento del navegador real y, por lo tanto, el contenido malintencionado no le permite tomar huellas digitales fácilmente.
 - Análisis dinámico en navegador emulado: el servicio de NSX Advanced Threat Prevention inspeccionó el asunto de análisis (como un archivo HTML o una URL) mediante el navegador emulado. El navegador emulado puede emular dinámicamente diferentes "personalidades" del navegador (por ejemplo, cambiar su `user-agent` o modificar las API que expone). Esta capacidad es útil cuando se analiza contenido malintencionado dirigido a tipos o versiones de exploradores específicos. La desventaja de este tipo de análisis es que este navegador es menos realista y es posible que el contenido malintencionado pueda tomar huellas digitales.
 - Análisis dinámico en visor de archivos simulado: el servicio NSX Advanced Threat Prevention inspeccione el asunto del análisis (como un archivo PDF) mediante el visor de archivos simulado. El visor puede detectar contenidos y vínculos integrados.
 - Inflación de archivo: el servicio NSX Advanced Threat Prevention expandió el asunto de análisis (un archivo), extrajo su contenido y envió el contenido para su análisis si son del tipo apropiado.
- Contraseña utilizada: si está disponible, se proporciona la contraseña que el servicio NSX Advanced Threat Prevention utilizó para descifrar la muestra correctamente.

Widget Relaciones del análisis

Un solo análisis puede requerir que el servicio NSX Advanced Threat Prevention supervise varios asuntos.

Por ejemplo, durante un análisis de archivo, es posible que la aplicación original inicie varios procesos. De forma similar, durante un análisis de URL, es posible que se recuperen más URL y se haga referencia a ellas.

En este caso, NSX Network Detection and Response generará el widget **Descripción general de los asuntos del análisis**, que proporciona una representación gráfica de la relación de cada asunto de análisis que supervisó el servicio NSX Advanced Threat Prevention durante el análisis.



El widget muestra un nodo para cada asunto de análisis. Una instancia de Edge vincula dos nodos si se detectó que los asuntos de análisis correspondientes interactúan durante el análisis (por ejemplo, si un proceso inició otro proceso).

A la izquierda del widget se encuentra una leyenda de las actividades que se observaron durante el análisis. Haga clic en el botón de opción junto al nombre de una actividad para resaltar los asuntos de análisis que mostraron esa actividad específica. También puede seleccionar un conjunto de actividades.

Haga clic en un nodo para contraer los nodos relacionados subsiguientes.

Al hacer doble clic en un nodo, accederá a la sección del informe que proporciona información detallada sobre el asunto de análisis correspondiente.

Informe de archivos de análisis

Las secciones **Asunto del análisis** muestran información detallada sobre el archivo o los archivos que contenía o a los que accedió la muestra cuando el servicio NSX Advanced Threat Prevention la procesó.

Para expandir la sección, haga clic en el ícono

Para un archivo ejecutable, se muestran los siguientes datos:

- Nombre: el nombre del ejecutable, si está disponible.
- MD5: el hash MD5 del archivo.
- SHA1: el hash SHA1 del archivo.
- Tipo de archivo: el tipo de archivo ejecutable (por ejemplo, PE executable, application, 32-bit, Intel i386).
- Tamaño del archivo: el tamaño del archivo.

- Línea de comandos: la línea de comandos completa, incluidos los argumentos o las opciones. Por ejemplo, C:\Users\ExampleUser\AppData\Local\Temp\exe_malware.exe.
- Contexto de ejecución: el nivel de privilegio invocado por el ejecutable.
- Arquitectura: la arquitectura del archivo ejecutable.
- Motivo del análisis: por qué se inició el procesamiento del archivo.

Actividades de archivo de análisis

Las secciones **Asunto del análisis** muestran la actividad real de la muestra, tal como la recopila el servicio NSX Advanced Threat Prevention.

Las secciones incluyen el asunto original que se está analizando y otros asuntos del entorno de análisis, ya sea porque los generó el asunto original o porque el asunto original alteró su memoria.

Nota No todas estas actividades están presentes para una muestra específica.

Haga clic en el icono  para expandir cada una de las siguientes secciones.

Nombre de la sección	Descripción
E/S de consola	Datos escritos en los identificadores de la consola (descriptores de archivos de entrada y de salida estándar).
Argumentos de la línea de comandos descodificados	Los argumentos de scripts malintencionados de PowerShell a menudo se codifican u ofuscan. Si se ejecutó un script durante el análisis, el back-end de VMware lo decodifica, lo que hace que sus argumentos estén disponibles en un formato más legible.
E/S de dispositivo	Lista de E/S de dispositivos de operaciones de E/S intentadas por el asunto durante el tiempo de ejecución. Para cada operación, se registran el dispositivo de destino y el código de control.
Actividad del controlador	Lista de controladores a los que accede el asunto durante el tiempo de ejecución. Se registran las siguientes operaciones: carga y descarga.
Excepciones	Lista de scripts ejecutados por el asunto durante el tiempo de ejecución. Para cada fila, hay una entrada para Nombre, TIPO e INTÉRPRETE. Puede ordenar la lista por cualquier columna.
Scripts ejecutados	Lista de scripts ejecutados por el asunto durante el tiempo de ejecución. Para cada fila, hay una entrada para Nombre, TIPO e INTÉRPRETE. Puede ordenar la lista por cualquier columna.
Actividad del sistema de archivos	Lista de archivos a los que accede el asunto durante el tiempo de ejecución. Se registran las siguientes operaciones: lectura, escritura, cambio de nombre y eliminación. Para los archivos escritos, se registra el nuevo tamaño y el hash MD5 del archivo.
Bibliotecas	Lista de archivos de biblioteca cargados por el asunto durante el tiempo de ejecución.
Contenido de la memoria	Se encontraron datos destacados en la memoria del programa. El sistema extrae, por ejemplo, direcciones IP, dominios y URL durante el análisis.
Actividad de Mutex	Lista de bloqueos de exclusión mutua a los que accede el asunto durante el tiempo de ejecución. Se registran las siguientes operaciones: creación y apertura.
Actividad de red	Lista de conversaciones de red relacionadas con el asunto durante el tiempo de ejecución. Se registran los siguientes tipos de conversaciones: comunicaciones a través de FTP, HTTP, IRC, SMTP y otros tipos de protocolos UDP/TCP. También se registran las solicitudes de DNS y las descargas de archivos remotos.

Nombre de la sección	Descripción
Interacciones del proceso	Lista de interacciones de procesos intentadas por el asunto durante el tiempo de ejecución. Se registran las siguientes operaciones: creación de procesos, creación de subprocesos, lectura y escritura de memoria.
Actividad del registro	Lista de valores y claves de registro a los que accede el asunto durante el tiempo de ejecución. Se registran las siguientes operaciones: lectura, escritura, eliminación y supervisión.
Actividad de servicio	Lista de servicios a los que accede el asunto durante el tiempo de ejecución. Se registran las siguientes operaciones: iniciar, detener y modificar parámetros.
Actividad de Windows	Lista de ventanas abiertas por el asunto durante el tiempo de ejecución.

Artefactos de archivo de análisis

La sección **Informe de eventos** muestra artefactos adicionales que el servicio NSX Advanced Threat Prevention recopila mientras procesa la muestra.

Estos artefactos se incluyen en el informe para que pueda verlos.

Captura de paquetes

Si el asunto generó tráfico de red, este tráfico se recopila y se muestra en el widget tráfico capturado.

Archivos extraídos

Para un archivo expandido, se muestra una lista del contenido. Cada fila muestra el tipo mime, la etiqueta (indica el tipo de análisis), la descripción, el nombre de archivo (si está disponible en el archivo) y la puntuación del artefacto. Solo se proporciona una puntuación si se analiza el artefacto. En este caso, también se proporciona un vínculo a su informe.

Si el servicio NSX Advanced Threat Prevention encontró un error al desempaquetar un archivo, mostrará una alerta que indica la condición de error. Los errores incluyen el límite máximo de archivos superado, el límite de profundidad máximo superado y el límite máximo de tareas secundarias superado.

Archivos generados

Durante el análisis, la muestra puede generar varios archivos. Estos archivos se muestran en una lista ordenada por RUTA.

- RUTA: la ruta del artefacto en el sistema de archivos.
- TIPO: el tipo de archivo determinado. Para ordenar la lista por tipo de archivo, haga clic en **TIPO**.

Haga clic en el icono  para expandir una fila. Se muestran los datos de MD5, SHA1, Tamaño (bytes), Empaquetadores y Firmas. Es posible que los datos no estén disponibles para todos los campos.

Argumentos de la línea de comandos descodificados

Los argumentos de scripts malintencionados de PowerShell a menudo se codifican u ofuscan. Si se ejecutó un script durante el análisis, el servicio NSX Advanced Threat Prevention lo descodifica, lo que hace que sus argumentos estén disponibles en un formato más legible. Estos argumentos se muestran en una lista que muestra el asunto del análisis y el script descodificado.

Informe de URL de análisis

La sección **Detalles de análisis** muestra las actividades reales del asunto del análisis, tal como lo recopila el servicio NSX Advanced Threat Prevention. Una actividad se utiliza para determinar una evaluación de su tipo.

Las siguientes actividades se muestran en esta sección **Detalles de análisis**.

Tipo de actividad	Descripción
Actividad de red	Enumera todas las URL visitadas durante el análisis, así como el contenido web adicional solicitado o el contenido por asunto. Cada URL adicional se registra junto con su tipo de contenido, el código de estado del servidor, la dirección IP del servidor, los hashes de contenido de respuesta (MD5 y SHA1), la longitud del contenido de la respuesta y el tiempo de la solicitud (hora de inicio, hora de finalización y duración en milisegundos).
Recursos	Enumera los recursos locales a los que se accedió durante el análisis de URL a través del protocolo res . A veces, las páginas web malintencionadas acceden a los recursos locales para sondear el entorno de ejecución; por ejemplo, para determinar si hay determinados programas instalados. Esta sección solo se muestra si se detectaron eventos de recursos durante el análisis.
Actividad de ejecución de código	Muestra el código que se ejecutó durante el análisis. En particular, muestra código interesante que se incluyó estáticamente en un recurso (mediante una etiqueta <code><script></code>) y todos los códigos que se generaron y ejecutaron dinámicamente durante el análisis de URL. A menudo, se genera código malintencionado en tiempo de ejecución para omitir firmas estáticas y hacer que su análisis sea más complicado. <ul style="list-style-type: none"> ■ Código JavaScript estático: se muestra solo si se detectaron eventos relevantes durante el análisis. ■ Código de JavaScript dinámico: el informe indica si no se encontraron eventos durante el análisis. ■ Código HTML: código que se agregó al documento dinámicamente a través de funciones como <code>document.write()</code>. El informe indica lo contrario si no se encontró ningún evento durante el análisis.
iFrames ocultos	Muestra las etiquetas HTML ocultas, como <code>iframe</code> , que se detectaron durante la navegación. Los elementos ocultos a veces se utilizan en páginas comprometidas para introducir código malintencionado de sitios web de terceros. Esta sección solo se muestra si se encontraron etiquetas ocultas durante el análisis.
Contenido de la memoria	Enumera las cadenas que se encontraron durante el análisis. Esta sección solo se muestra si se detectaron cadenas durante el análisis.
Contenido textual	Muestra el contenido textual extraído de un documento. Esta sección solo se muestra si se detectó texto durante el análisis, solo análisis de PDF.
Vínculos en documentos	Muestra los vínculos que se encontraron en los documentos analizados. Esta sección solo se muestra si se encontraron vínculos durante el análisis.

Tipo de actividad	Descripción
Complementos	Enumera cualquier uso de complementos de navegador comunes. Las llamadas a estos complementos se registran y el informe contiene los detalles sobre los métodos invocados y los argumentos pasados.
Applets	Muestra los applets Java que se descargaron durante el análisis de URL. Esta sección solo se muestra si se encontraron applets durante el análisis.
Explotaciones	El entorno de análisis tiene la capacidad de detectar el código de shell contenido en los asuntos de análisis. El código de shell detectado se extrae e incluye en el informe en formato hexadecimal.
Shellcode	El entorno de análisis tiene la capacidad de detectar el código de shell contenido en los asuntos de análisis. El código de shell detectado se extrae e incluye en el informe en formato hexadecimal.
Procesos	Enumera los procesos que se generaron durante el análisis de URL. Esta sección solo se muestra si se encontraron procesos generados durante el análisis.
Archivos descartados	Enumera los archivos que se almacenaron en el disco duro del sistema durante el análisis de URL. Esta sección solo se muestra si se detectaron operaciones de archivo durante el análisis.

Administración y operaciones de NSX Intelligence

6

Dispone de herramientas para realizar operaciones que le ayudarán a administrar la función NSX Intelligence en su entorno de NSX-T.

Los siguientes temas le ayudarán a administrar el acceso a la función NSX Intelligence, a supervisar el estado de la aplicación NSX Intelligence o a encontrar información sobre objetos de NSX Intelligence.

Este capítulo incluye los siguientes temas:

- [Control de acceso basado en funciones en NSX Intelligence](#)
- [Recopilar paquetes de soporte de NSX Intelligence](#)
- [Búsqueda de entidades de NSX Intelligence](#)
- [Administrar la configuración de NSX Intelligence](#)
- [Administrar los rangos de IP privadas para NSX Intelligence](#)

Control de acceso basado en funciones en NSX Intelligence

El control de acceso basado en funciones (RBAC) ayuda a restringir el acceso a las funcionalidades de NSX Intelligence solo a determinados usuarios autorizados.

Como a las funciones de NSX Intelligence se accede mediante la interfaz de usuario de NSX Manager, se usan las mismas funciones integradas en NSX-T Data Center que se asignan a los usuarios para el RBAC de NSX Intelligence, y cada función tiene permisos específicos. Para obtener información sobre cómo asignar funciones a los usuarios, consulte la *Guía de administración de NSX-T Data Center*.

Para ver las funciones integradas de NSX-T Data Center, desplácese hasta **Sistema > Administración de usuarios > Funciones**.

Funciones y permisos

A continuación se muestran los tipos de permisos aplicados en la función NSX Intelligence. En la lista se incluyen las abreviaturas de los permisos que se utilizan en la tabla [Tabla 6-1. Funciones y permisos de NSX Intelligence](#).

- Acceso completo (FA): para obtener recomendaciones, el acceso completo incluye la capacidad de leer, iniciar, volver a ejecutar, actualizar, eliminar y publicar recomendaciones.

- Ejecución (E)
- Lectura (R)
- Ninguno

La función NSX Intelligence reconoce las siguientes funciones integradas. No se puede agregar ninguna función nueva porque las funciones RBAC personalizadas no admiten funciones de NSX Intelligence. En la lista también se incluyen las abreviaturas de las funciones que se utilizan en la tabla [Tabla 6-1. Funciones y permisos de NSX Intelligence](#).

- Auditor (A)
- Usuario admin de organización (EA)
- Usuario admin de socios de GI (Guest Introspection) (GIA)
- Usuario admin de LB (equilibrador de carga) (LBA)
- Operador de LB (LBO)
- Usuario admin de socios de NETX (introspección de red) (NIA)
- Usuario admin de red (NA)
- Operador de red (NO)
- Usuario admin de seguridad (SA)
- Operador de seguridad (SO)
- Recopilador de paquetes de soporte computación basada en servidor (SBC)
- Usuario admin de VPN (VPNA)

En la siguiente tabla se muestran los permisos que tiene cada función integrada para las diferentes operaciones de NSX Intelligence.

Tabla 6-1. Funciones y permisos de NSX Intelligence

Operación	E												VP
	A	A	SA	SO	NA	NO	SBC	GIA	NIA	LBA	LBO	NA	
Activar la función NSX Intelligence en NSX Application Platform.	F A	R A	R FA	R R	Nin gun o								
Configurar la recopilación de datos de NSX Intelligence en hosts o clústeres de hosts mediante Sistema > NSX Intelligence	F A	R A	FA o	R o	Nin gun o								
Trabajar con el panel de control Seguridad > Tráfico sospechoso > Eventos de detección.	F A	R A	FA o	R o	Nin gun o								
Configurar los detectores en Seguridad > Tráfico sospechoso > Definiciones de detector.	F A	R A	FA o	R o	Nin gun o								

Tabla 6-1. Funciones y permisos de NSX Intelligence (continuación)

Operación	E												VP
	A	A	SA	SO	NA	NO	SBC	GIA	NIA	LBA	LBO	NA	
Visualice los flujos de tráfico mediante Planificar y solucionar problemas > Detectar y realizar acción.	F A	R	R	R	R	R	Nin gun o						
Trabaje con recomendaciones de NSX mediante Planificar y solucionar problemas > Recomendaciones.	F A	R	FA	R	Nin gun o								
Genere un paquete de soporte mediante Sistema > Paquete de soporte.	F A	R	Nin gun o	Nin gun o	Nin gun o	Nin gun o	FA	Nin gun a	Nin gun o	Nin gun o	Nin gun o	Nin gun o	Nin gun o
Actualizar la función NSX Intelligence mediante NSX Application Platform.	F A	R	Nin gun o										
Busque flujos mediante la barra de búsqueda.	F A	R	R	R	R	R	Nin gun o						
Busque recomendaciones mediante la barra de búsqueda.	F A	R	R	R	Nin gun o								

Recopilar paquetes de soporte de NSX Intelligence

Puede recopilar paquetes de soporte de la función NSX Intelligence mediante la interfaz de usuario de NSX Manager. Puede descargar el paquete en su sistema local o cargarlo en un servidor de archivos remoto.

El contenido del archivo del paquete de soporte no incluye datos de flujo de tráfico de red ni datos de recomendaciones.

Procedimiento

- En un navegador, inicie sesión con privilegios de administrador empresarial en una instancia de NSX Manager desde <https://<dirección-ip-nsx-manager>>.
- Seleccione **Sistema > Paquete de soporte**.
- En la página **Solicitar paquete**, seleccione **NSX Application Platform** en el menú desplegable **Tipo**.
- En el panel **Disponible**, seleccione el servicio para el que se va a recopilar el paquete de soporte.
- Para mover los servicios seleccionados al panel **Seleccionado**, haga clic en el icono >.

- 6 En el cuadro de texto **Antigüedad del registro (días)**, mantenga el valor predeterminado **Todo** o introduzca el número específico de días de los registros que desea incluir en el paquete de soporte.
- 7 Para especificar que desea que los archivos básicos y de registro de audit se incluyan en el paquete de soporte, haga clic en el botón de **Incluir archivos básicos y registros de audit** para establecerlo en **Sí**.
Asegúrese de que lee y comprende la información que aparece debajo de esta opción al incluir o excluir los archivos básicos y los registros de audit.
- 8 (opcional) Active la casilla de verificación **Cargar paquete al servidor de archivos remoto** si desea cargar el paquete de soporte en un servidor de archivos remoto.
 - a Proporcione la dirección IP o el nombre de host del servidor de archivos remoto, el puerto y el protocolo que se utilizará.
 - b Introduzca el nombre de usuario y la contraseña del servidor de archivos remoto.
 - c Introduzca la ruta se destino absoluta en la que se va a cargar el paquete en el servidor remoto.
 - d Si desea que NSX Manager realice la carga del paquete, active la opción **Carga de administrador**.

9 Haga clic en **Iniciar recopilación de paquetes**.

10 Supervise el estado del procedimiento de recopilación del paquete.

La página **Estado** muestra el progreso de la recopilación del paquete de soporte. Cuando la recopilación se haya completado correctamente, el tamaño del paquete se mostrará junto a **Paquete de soporte**. En la tabla **Detalles**, se muestra la información sobre todos los paquetes de soporte que se generaron correctamente o que no se pudieron completar.

11 Para almacenar el paquete de soporte en una carpeta local, haga clic en **Descargar**. Si seleccionó la casilla de verificación **Cargar paquete al servidor de archivos remoto**, el paquete de soporte se cargará en el servidor de archivos especificado.

Búsqueda de entidades de NSX Intelligence

La capacidad de búsqueda global en NSX-T Data Center reconoce palabras clave de NSX Intelligence.

Puede utilizar la interfaz de búsqueda de NSX Manager para buscar entidades relacionadas con NSX Intelligence. Debe tener activado NSX Intelligence en NSX-T Data Center 3.0 o una versión posterior para que la función de búsqueda global de NSX Intelligence se pueda utilizar.

Los resultados de la búsqueda se basan en el estado actual de la configuración de NSX-T Data Center y no exponen datos históricos de NSX Intelligence.

En función de los criterios de búsqueda, los resultados de la búsqueda pueden mostrar información sobre las entidades relacionadas con NSX Intelligence, como grupos, máquinas virtuales, flujos y recomendaciones. Puede filtrar estos resultados en función de una o varias propiedades relacionadas de las entidades. Los vínculos de navegación se incluyen en los resultados de la búsqueda y le permiten ver una entidad de resultados seleccionada en el lienzo de visualización de NSX Intelligence.

En la siguiente tabla, se enumeran los tipos de recursos de NSX Intelligence admitidos y sus propiedades.

Tipo de recurso admitido	Propiedades
recommendations	<ul style="list-style-type: none"> ■ context group path ■ context physical server display name ■ context physical server id ■ context vm display name ■ context vm external id ■ display name ■ effective physical server display name ■ effecive physical server id ■ effective vm display name ■ effective vm id ■ status <ul style="list-style-type: none"> ■ ANALYSIS_IN_PROGRESS ■ FAILED ■ PUBLISHED ■ READY_TO_PUBLISH ■ WAITING <p>Ejemplo de consulta de búsqueda:</p> <pre>recommendation where status = READY_TO_PUBLISH and context group display name = 'Linux'</pre>
flows	<ul style="list-style-type: none"> ■ active only ■ destination group display name ■ destination physical server display name ■ destination physical server id ■ destination vm display name ■ destination vm external id ■ flow type <ul style="list-style-type: none"> ■ ALLOWED ■ BLOCKED ■ UNPROTECTED ■ source group display name ■ source physical server display name ■ source physical server id ■ source vm display name ■ source vm external id <p>Ejemplo de consulta de búsqueda:</p> <pre>flows where source vm display name = 'Win10' and destination vm display name = 'AD Server'</pre>

Buscar entidades de NSX Intelligence

Puede buscar entidades de NSX Intelligence, como grupos, máquinas virtuales, servidores físicos, flujos y recomendaciones, utilizando varios criterios admitidos.

La tabla muestra los resultados de búsqueda ordenados por relevancia. Puede filtrar los resultados proporcionando más criterios de búsqueda en la consulta.

Nota Si tiene caracteres especiales en la consulta de búsqueda que también actúen como operadores, debe agregar una barra diagonal inversa inicial, \, antes de cada carácter especial. Los caracteres que funcionan como los operadores son: +, -, =, &&, ||, <, >, !, (,), {, }, [,], ^, ", ~, ?, :, / y \.

Requisitos previos

Debe tener la función NSX Intelligence 3.2 o una versión posterior implementada en NSX-T Data Center 3.2 o una versión posterior.

Procedimiento

- 1 En un navegador, inicie sesión con privilegios de usuario admin empresarial en NSX Manager desde <https://<dirección-ip-nsx-manager>>.
- 2 En la página **Inicio**, introduzca un criterio de búsqueda para una entidad de NSX Intelligence.

A medida que introduce el criterio de búsqueda, la función de búsqueda global ofrece asistencia mostrando las palabras clave aplicables.

Los resultados se muestran en una tabla similar a la siguiente imagen.

The screenshot shows the NSX-T Data Center interface with the title bar "vm NSX-T". The main area displays a search result for flows. The search query is "Q. flows where flow type = UNPROTECTED and source vm external id = '501b1e8c-2a74-4ee9-8179-c9ccc2148f4f'". The results table has columns: Origen (Cómputo, Grupo), Destino (Cómputo, Grupo), Servicios, Último flujo (Contra la última directiva), and Ver en el gráfico. Two rows are shown:

Origen	Destino	Servicios	Último flujo (Contra la última directiva)	Ver en el gráfico
rhelvm2 RHELVM2_Group	rhelvm4 RHELVM4_Group	SSH... +2 More	● Allowed	[graph icon]
rhelvm2 Group-1 (REC 211109 10:2)	rhelvm4 RHELVM4_Group	SSH... +2 More	● Allowed	[graph icon]

At the bottom left is an "Actualizar" button, and at the bottom right is a status bar showing "1 - 2 of 2 Flow(s)".

Puede expandir cada fila para ver más detalles de cada resultado de búsqueda específico. También puede hacer clic en los vínculos proporcionados para mostrar información adicional sobre ese atributo específico. Al hacer clic en el ícono de gráfico y un vínculo en la ventana emergente, puede ver información más detallada en el lienzo de visualización de NSX Intelligence.

- 3 (opcional) Para guardar los criterios de búsqueda perfeccionados, haga clic en el ícono Guardar .

- 4 En la barra de búsqueda, haz clic en el icono de búsqueda avanzada  para ver las consultas de búsqueda guardadas y recientes.
- 5 Para ver la lista de los criterios de consulta de búsqueda recientes, haga clic en **Reciente**.
Al hacer clic en los criterios de búsqueda, los resultados se mostrarán en el panel de resultados.
- 6 Para ver cualquier criterio de búsqueda guardado, haga clic en **Guardado**.
- 7 (opcional) Para restablecer los criterios de búsqueda avanzada, haga clic en **Borrar todo**.

Administrar la configuración de NSX Intelligence

Después de activar la función NSX Intelligence, de forma predeterminada, comienza a recopilar datos de tráfico de red en todos los hosts independientes y el clúster de hosts. Si es necesario, también podrá detener la recopilación de datos de un host independiente o un clúster de hosts.

La sección **Host independiente** de la pestaña **Recopilación de datos** en la interfaz de usuario **Configuración del sistema > NSX Intelligence** solo muestra los hosts que no pertenecen a un clúster y no están administrados por un administrador de equipos. La sección **Clúster** enumera todos los clústeres del entorno de NSX-T.

No se puede desactivar ni activar la recopilación de datos para un único host que pertenece a un clúster. Solo puede desactivar o activar la recopilación de datos en todo el clúster al que pertenece ese host. Cuando la recopilación de datos está desactivada para un clúster, la aplicación **NSX Intelligence** deja de recopilar datos en todos los hosts que pertenecen a ese clúster. De forma similar, si el modo de recopilación de datos está activado en un clúster, la aplicación **NSX Intelligence** comienza a recopilar datos en todos los hosts que pertenecen a ese clúster.

Si el modo de recopilación de datos está desactivado para un host independiente, y ese host se agrega a un clúster cuya recopilación de datos está activada, la aplicación **NSX Intelligence** comenzará a recopilar datos en ese host después de que se una a ese clúster. De forma contraria, si un host independiente tiene activado el modo de recopilación de datos y se agrega a un clúster cuya recopilación de datos está desactivada, la aplicación **NSX Intelligence** detendrá la recopilación de datos en ese host después de unirse a ese clúster.

Requisitos previos

- La función NSX Intelligence debe activarse en NSX Application Platform. Consulte *Activar y actualizar VMware NSX Intelligence* para obtener información detallada.
- Debe tener privilegios de usuario de administrador empresarial de NSX-T Data Center.
- Al menos una licencia válida de la edición NSX Data Center Enterprise Plus está vigente para la sesión de NSX Manager.

Procedimiento

- 1 En un navegador, inicie sesión con privilegios de administrador empresarial en un dispositivo de NSX Manager desde <https://<dirección-ip-nsx-manager>>.
- 2 En la interfaz de usuario de NSX Manager, seleccione **Sistema** y, en la sección Ajustes, seleccione **NSX Intelligence**.
- 3 Para administrar la recopilación de datos de tráfico para uno o varios hosts, realice uno de los siguientes pasos.
 - a Para detener la recopilación de datos de tráfico, seleccione el host o los hosts en la sección **Host independiente**, haga clic en **Desactivar** y, a continuación, haga clic en **Confirmar** cuando se le pida que confirme.
 - b Para iniciar la recopilación de datos de tráfico, seleccione el host o los hosts, haga clic en **Activar** y, a continuación, haga clic en **Confirmar** cuando se le pida que confirme.

El sistema actualizará el valor de **Estado de recopilación** para cada host afectado a Desactivado o Activado, en función del modo de recopilación de datos que haya establecido.

- 4 Para administrar la recopilación de datos de tráfico para uno o varios clústeres de hosts, realice uno de los siguientes pasos.
 - a Para detener la recopilación de datos de uno o varios clústeres, seleccione el clúster o los clústeres en la sección **Clúster**, haga clic en **Desactivar** y, a continuación, haga clic en **Confirmar** cuando se le pida que confirme.
 - b Para iniciar la recopilación de datos de tráfico, seleccione el clúster o los clústeres, haga clic en **Activar** y, a continuación, haga clic en **Confirmar** cuando se le pida que confirme.

El sistema actualizará el valor de **Estado de recopilación** para cada clúster afectado a Desactivado o Activado, en función del modo de recopilación de datos que haya establecido.

Administrar los rangos de IP privadas para NSX Intelligence

Los rangos de IP privadas se utilizan para aislar datos de tráfico sospechoso dentro de segmentos de red controlados.

Puede administrar los rangos de IP privadas mediante la pestaña **Rangos de IP privados** en la interfaz de usuario de **Configuración general de seguridad**. Estos rangos de IP privadas se pueden utilizar en las funciones NSX Intelligence y NSX Network Detection and Response al activar cualquiera de ellas.

Si activa la función NSX Network Detection and Response, el sistema cargará la información de los rangos de IP privadas en la función NSX Network Detection and Response, información que usan algunas de las reglas de correlación de intrusiones.

- Para introducir un rango de direcciones IP IPv4, haga clic dentro del cuadro de texto Rango de IP IPv4 e introduzca los valores con el formato de notación CIDR de IP IPv4 que se muestra debajo del cuadro. Presione Intro para cada entrada y haga clic en **Guardar** cuando haya terminado.
- Para introducir un rango de direcciones IP IPv6, haga clic dentro del cuadro de texto Rango de IP IPv6 e introduzca los valores con el formato de notación CIDR de IP IPv6 que se muestra debajo del cuadro. Presione Intro para cada entrada y haga clic en **Guardar** cuando haya terminado.

La función NSX Intelligence clasifica una dirección IP que pertenece a una de las anotaciones CIDR que se especifican en el cuadro de diálogo como una dirección IP privada. Cualquier dirección IP que no pertenezca a ninguna de estas notaciones CIDR se clasificará como una dirección IP pública. Si la dirección IP de la máquina virtual o el servidor físico no se encuentra en una de estas notaciones CIDR, puede agregar la notación CIDR mediante esta interfaz de usuario **Rangos de IP privados**.

Solucionar problemas relacionados con el uso de NSX Intelligence

7

Si la función NSX Intelligence deja de responder, o si necesita más detalles sobre un mensaje de error que recibió al utilizar la función NSX Intelligence, puede ejecutar comandos específicos para obtener el estado de los servicios de NSX Intelligence.

También puede recopilar paquetes de soporte para ayudar al personal de soporte de VMware en los problemas de depuración que haya podido tener.

Este capítulo incluye los siguientes temas:

- [Comprobar el estado de la función NSX Intelligence](#)
- [Hay servicios degradados después de una activación correcta de NSX Intelligence](#)
- [Incoherencias en los informes de topología incremental](#)
- [La información de flujo de FTP aún se muestra después de que se detenga la sesión de FTP](#)
- [La vista Grupos no se actualiza con los datos de flujo de tráfico](#)

Comprobar el estado de la función NSX Intelligence

Si la función NSX Intelligence deja de responder, compruebe el estado de los servicios de NSX Application Platform.

Problema

La función NSX Intelligence dejó de responder o se recibió un mensaje de error indicando que no funciona según lo esperado.

Causa

Es posible que uno o varios de los servicios subyacentes de NSX Application Platform se hayan detenido o que no estén en buen estado. La función NSX Intelligence se aloja en NSX Application Platform y, por lo tanto, si alguno de los servicios de la plataforma no está en buen estado, la función NSX Intelligence puede verse afectada.

Solución

Compruebe el estado de NSX Intelligence mediante la llamada API `health`. En el resultado JSON, compruebe las entradas `services` en la clave `intelligence`. Consulte el

documento de <http://developers.eng.vmware.com/apis/nsx-intelligence-&-application-platform/cluster/latest/napp/api/v1/platform/monitor/feature/health/get/> para obtener más información.

Hay servicios degradados después de una activación correcta de NSX Intelligence

La función NSX Intelligence se activó correctamente, pero hay algunos servicios degradados.

Problema

La función NSX Intelligence se activó correctamente, pero su estado aparece como PARCIALMENTE ACTIVO o INACTIVO. Este estado Degradado aparece inmediatamente después de implementar la función NSX Intelligence o en una etapa posterior de su ciclo de vida.

Causa

El motivo puede ser cualquiera de los siguientes.

- 1 No se puede acceder al registro de Docker desde el TKC o el nodo de trabajo de Kubernetes ascendente.
- 2 El pod de la aplicación NSX Intelligence no pudo alcanzar el estado En ejecución.

Solución

Trabaje con el administrador de la infraestructura de Kubernetes para intentar solucionar el problema. Use las siguientes soluciones que se corresponden con los problemas incluidos en la sección anterior Problemas.

- 1 Compruebe si todos los pods deseados pueden iniciarse. El inicio de los pods depende de que se pueda acceder al registro de Docker. En caso de que no se pueda acceder al registro de Docker o se produzca un error en la acción de descarga debido a motivos de autenticación o autorización, es posible que el nodo de trabajo de Kubernetes no pueda descargar la imagen de contenedor de Docker necesaria para ejecutar las cargas de trabajo. Solucione el problema de conectividad del registro de Docker, elimine la función NSX Intelligence e intente activarla de nuevo.
- 2 Compruebe que todos los pods tienen el estado En ejecución y que todos los trabajos se hayan completado correctamente. Una vez que se descarga la imagen de contenedor de Docker, los pods deben poder iniciarse y ejecutarse. Para los pods que no se encuentran en estado En ejecución, compruebe los eventos mediante el siguiente comando describe.

```
napp-k describe pod <pod-name>
```

Para los trabajos que no se hayan completado correctamente, compruebe los registros mediante el siguiente comando.

```
napp-k logs <pod-name>
```

En el caso de que ninguna de las soluciones proporcionadas funcione, póngase en contacto con el servicio de soporte técnico de VMware para obtener más ayuda.

Incoherencias en los informes de topología incremental

Es posible que existan incoherencias en la cantidad de máquinas virtuales, servidores físicos, grupos o flujos que se muestran en la vista Grupos o Recursos informáticos si deja la página de la interfaz de usuario de visualización de NSX Intelligence durante mucho tiempo.

Problema

Si abre la vista Grupos o la vista Recursos informáticos y deja abierta la página de la interfaz de usuario de visualización de NSX Intelligence durante un tiempo prolongado, los nuevos eventos se enviarán de forma incremental y se combinarán en la vista. Es posible que haya algunas incoherencias en los recuentos de grupos, máquinas virtuales o servidores físicos durante la combinación y los informes incrementales. Por ejemplo, si se cambia la configuración, como cambios en el grupo al que pertenece la máquina virtual que se activaron durante el informe incremental, es posible que observe incoherencias en las visualizaciones que se muestran. Es posible que los nuevos flujos generados a partir de las entidades informáticas recién agregadas tampoco se incluyan en la vista actual.

Puede que observe las siguientes incoherencias en las visualizaciones que se muestran.

- 1 Un nodo de grupo sin clasificar muestra un recuento incorrecto de máquinas virtuales.
 - El recuento de máquinas virtuales que se muestra para un grupo sin clasificar es diferente y, por lo general, mayor que el recuento de máquinas virtuales que aparece cuando se muestra una vista de grupos nueva.
 - El recuento de máquinas virtuales que se muestra para un grupo Sin categorizar es diferente y, por lo general, mayor que el recuento de máquinas virtuales que se muestra al hacer clic con el botón derecho en el nodo de un grupo y se selecciona **Máquina virtual**.
- 2 Un grupo sin clasificar en una vista de grupos de análisis profundo muestra un número incoherente de máquinas virtuales.
 - El grupo Sin clasificar que se muestra en una vista de grupos de análisis profundo puede mostrar más máquinas virtuales de las que se muestran en una vista de grupos de análisis profundo que se acaba de abrir.
 - El grupo Sin clasificar en una vista de grupos de análisis profundo puede mostrar más máquinas virtuales de las que se muestran al hacer clic con el botón derecho en el nodo del grupo Sin clasificar y se selecciona **Máquina virtual**.
 - Es posible que una máquina virtual reciba una actualización activa en el grupo Sin clasificar, incluso después de que ya se haya agregado a otro grupo.

- 3 Es posible que se muestre una máquina virtual sin nombre en las vistas Grupos y Recursos informáticos.
 - Por lo general, este problema se observa en las máquinas virtuales que pertenecen al grupo Desconocido o Sin categorizar. También existe una pequeña posibilidad de que aparezca en un grupo normal.
- 4 Cuando la aplicación NSX Intelligence está recopilando flujos de tráfico con una tasa de alta velocidad de carga cuando se muestra la vista Grupos o Recursos informáticos, es posible que se retrasen las actualizaciones de visualización incremental en la vista.

Causa

Actualmente, los informes de datos en tiempo real tienen algunas incoherencias conocidas que se producen durante los informes incrementales.

Solución

Para borrar las incoherencias, vuelva a cargar todo el lienzo de visualización de NSX Intelligence actualizando el navegador web.

La información de flujo de FTP aún se muestra después de que se detenga la sesión de FTP

Después de detener repentinamente una sesión de FTP, la información de flujo de FTP para esa sesión se muestra en la página de la interfaz de usuario de visualización de NSX Intelligence.

Problema

Si inicia una sesión de FTP y, en mitad de la sesión, presiona Ctrl+C o Ctrl+Z, se detendrá la sesión de FTP. Sin embargo, la información sobre ese flujo de FTP permanece en la pantalla durante un largo periodo de tiempo en la pestaña **Flujos activos** de la tabla Detalles de flujo del grupo.

Causa

Debido a que la sesión de TCP no se detuvo correctamente, el tiempo de espera de inactividad de TCP aún está en vigor. El tiempo de espera se establece en 12 o 24 horas de forma predeterminada.

Solución

Para asegurarse de que la información de los flujos de tráfico de FTP no continúe mostrándose en la pestaña **Flujos activos** después de que la sesión de FTP se detenga de forma abrupta, establezca un perfil de temporizador de sesión con un valor de tiempo de espera más corto. Establezca el perfil en los grupos correspondientes. Consulte el tema "Crear un temporizador de sesión" en la *Guía de administración de NSX-T Data Center* para obtener más información.

La vista Grupos no se actualiza con los datos de flujo de tráfico

Después de migrar correctamente de NSX Intelligence 1.2.x a NSX Intelligence 3.2 o versiones posteriores, los datos de flujo de tráfico que se muestran en la vista Grupos no se actualizan.

Problema

La vista Grupos no muestra los datos de flujo de tráfico más recientes.

Causa

Existe un problema de red en la red de clústeres de Kubernetes en la que se ejecuta NSX Intelligence.

Solución

Después de estabilizar la red del clúster de Kubernetes, realice uno de los siguientes pasos para ver todos los datos de flujo de tráfico actualizados que podrían haberse perdido durante la inestabilidad de la red.

- 1 Espere a que las actualizaciones de los datos de flujo de tráfico se reflejen en el lienzo NSX Intelligence.

Una vez que la red del clúster de Kubernetes se vuelva estable, NSX Intelligence sincronizará todos los datos de flujo de tráfico con NSX Manager y mostrará la información de flujo de tráfico de los grupos actualizados en el lienzo NSX Intelligence.
- 2 Si desea forzar una sincronización de datos inmediatamente, póngase en contacto con el administrador de la infraestructura de Kubernetes para reiniciar el pod `nsx-config`. Una vez que el pod de `nsx-config` se reinicie y se encuentre en un estado de ejecución estable, se activará una sincronización de los datos de flujo de tráfico y la vista Grupos se actualizará en el lienzo NSX Intelligence.